Co-funded by the Erasmus+ Programme of the European Union

КІБЕРЗАГРОЗИ ЯК СКЛАДОВА ГІБРИДНИХ КОНФЛІКТІВ: СУЧАСНІ ТЕНДЕНЦІЇ ТА ЗАХИСТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Норік Лариса,
к. е. н, доцент, доцент кафедри економіко-математичного моделювання
Харківський національний економічний університет імені Семена Кузнеця,
доцент кафедри вищої математики фізичного факультету
Харківський національний університет ім. В. Н. Каразіна,
м. Харків, Україна,
ORCID: https://orcid.org/0000-0002-7077-1260

В епоху глобалізації та цифровізації однією з ключових загроз у сучасному світі стають гібридні конфлікти, які є комбінацією військових, політичних, економічних, інформаційних та кіберзасобів для досягнення стратегічних цілей. Кіберзагрози стали невід'ємною частиною гібридних конфліктів, поєднуючи в собі використання інформаційних технологій для підриву стабільності держав та їхніх інституцій. Цифровізація, яка має сприяти розвитку суспільства та економіки, стає інструментом у руках зловмисників, які прагнуть використати вразливості в кіберпросторі для досягнення своїх політичних і військових цілей. В умовах сучасної гібридної війни Україна стикається з новими викликами, де кібербезпека відіграє вирішальну роль у захисті національних інтересів. У цьому контексті надзвичайно важливо розглянути сучасні тенденції кіберзагроз та заходи захисту національної безпеки України в умовах гібридних конфліктів.

За даними [1] 97% світових організацій спостерігали зростання кіберзагроз з початку російсько-української війни у 2022 році, що демонструє вплив геополітичної напруженості на кібербезпеку. Україна також неодноразово ставала об’єктом масштабних кібернападів, які намагалися паралізувати роботу критичних інфраструктурних об’єктів – від банківської системи до енергетичних установ. Водночас Україна стикається з викликами у сфері інформаційної безпеки, коли використовуються контрольовані медіа та соціальні мережі для поширення дезінформації, пропаганди та маніпуляцій громадською думкою.

Останнім часом виникають нові форми кіберзагроз, що ставлять під загрозу функціонування багатьох компаній у світі та Україні. Так, за інформацією [2] у 2023 році особливо виділилися такі: *фішинг*- та *смішинг*-атаки, за допомогою яких злочинці обманюють користувачів, щоб отримати доступ до конфіденційної інформації (фішинг визначений як основний вектор зараження в 41 % випадків кібербезпеки [1]); *зловмисне програмне забезпечення* – шкідливі програми, які викрадають дані, досліджують локальні мережі або надсилають спам із зараженого пристрою (у 2023 році в усьому світі було

виявлено 6,06 млрд атак зловмисного програмного забезпечення, більшість з яких припадає на Азіатсько-Тихоокеанський регіон [3]); *програми-вимагачі*, які блокують систему та позбавляють доступу до критично важливих даних, водночас вимагають викуп за відновлення контролю над своїми системами (у 2023 році 72,7 % усіх організацій стали жертвами атаки програм-вимагачів, найбільше постраждали від кібервимагань великі підприємства – 40%, за ними йдуть малі організації – 25% і середні підприємства – 23% [1]); *компрометація корпоративної електронної пошти* завдяки злому злочинцями бізнес-систем з метою отримання доступу до інформації про платіжні системи (малі підприємства мають найвищий рівень цільової шкідливої електронної пошти – 1 з 323 [1]); *внутрішні загрози* – витоки або навмисні дії співробітників, які мають доступ до конфіденційних даних; *розвідка та атаки на хмарні сервіси,* щоб отримати доступ до даних і використовувати їх (середня глобальна вартість витоку даних у 2023 році становила 4,45 млн дол, що підкреслює зростаючий фінансовий тягар для організацій [1]); *атака нульового дня*, коли використовують раніше невідомі вразливості в системі кібербезпеки на макрорівні ще до того, як розробники дізнаються про існування проблеми; *соціальна інженерія* – маніпуляції людьми для отримання доступу до системи шляхом підроблених запитів, спрямованих на керівників безпеки або співробітників (74% усіх порушень пов’язані частково з людською помилкою, неправильним використанням привілеїв, використанням викрадених облікових даних [1]); *кібершпигунство, витік даних та крадіжка інтелектуальної власності* – це серйозна загроза для інноваційних компаній, особливо в контексті гібридних конфліктів, коли іноземні агенти можуть намагатися викрасти важливі технології (крадіжка даних була причиною 19% усіх інцидентів [1]).

Сучасні наукові дослідження зосереджені на вивченні кіберзагроз та шляхів їх нейтралізації. Науковці активно працюють над розробкою нових підходів до захисту інформаційних систем і вдосконаленням стратегій кібербезпеки, спрямованих на запобігання потенційним загрозам. Так, в роботі [4] подано аналіз глобальних трендів розвитку Інтернету речей та кібербезпеки за 2004 – 2024 роки та доведено важливість прийняття цілісного підходу до кібербезпеки, який поєднує технологічні рішення з освітою, обізнаністю та міжнародним співробітництвом. У дослідженні [5] також підкреслюється важливість інформаційної безпеки для захисту цифрових активів і конфіденційної інформації, забезпечення координації зацікавлених сторін у транскордонних сценаріях прийняття рішень. Автори роботи [6] системно проаналізували потреби у сфері кібербезпеки на основі штучного інтелекту та виявили найбільш критичні проблеми, а саме: обмежений обмін розвідувальною інформацією про загрози та недостатність автоматизації реагування на інциденти та нормативні перешкоди, пов’язані із законами про захист даних і розвитком законодавства про кібербезпеку. У статті [7] подано

результати ґрунтовного дослідження, у якому проаналізовано різні верифіковані кібератаки, які здійснені проти критичної інфраструктури за останні роки,та розроблено архітектуру і структуру критичної інфраструктури із використовуваними технологіями та криптографічними примітивами.

Протидія гібридним загрозам вимагає комплексного підходу, що включає зміцнення політичної стійкості, розвиток оборонних можливостей та активну міжнародну співпрацю. Україна намагається зміцнити свої можливості щодо безпеки, зокрема шляхом посилення кібербезпеки, створення стратегії боротьби з дезінформацією та посилення національної системи протидії новим загрозам. НАТО і його індо-тихоокеанські партнери Австралія, Японія, Нова Зеландія та Південна Корея планують запустити чотири нові спільні проєкти, пов'язані з допомогою Україні, штучним інтелектом, кібербезпекою та протидією дезінформації. Наукова асоціація кібербезпеки ISCAУкраїни розробляє та впроваджує проекти, спрямовані на підвищення загального рівня кібербезпеки українського суспільства за рахунок здійснення наукової, науково-технічної та освітньої діяльності в галузі кібербезпеки і суміжних галузях. Україна також може скористатися досвідом світових країн у сфері кібербезпеки через впровадження низки стратегічних і технологічних рішень. Успіх у цьому протистоянні визначатиме не тільки майбутнє України, але й глобальну стабільність у світі.

Список використаних джерел:

1. Найпопулярніші статистичні дані з кібербезпеки за 2024 рік. URL: https://www.cobalt.io/blog/cybersecurity-statistics-2024 (дата звернення 16.09.2024).

2. ТОП 10 загроз кібербезпеці бізнесу у 2023 році. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023 (дата звернення 12.09.2024).

3. State of malware worldwide Statistics & Facts. URL: https://www.statista.com/topics/8338/malware/#topicOverview (дата звернення 20.09.2024).

4. Гайдук О., Звєрєв В. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. №3(23). С. 225–236.https://doi.org/10.28925/2663-4023.2024.23.225236

5. Pestana G., Sofou S. Data Governance to Counter Hybrid Threats against Critical Infrastructures. *Smart Cities*. 2024. No. 7(4). P. 1857–1877. https://doi.org/10.3390/smartcities7040072

6. Katrakazas P., Papastergiou S. A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience. *Businesses*. 2024. No. 4(2). P. 225–240. https://doi.org/10.3390/businesses4020015

7. Tsantikidou K., Sklavos N. Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures. *Cryptography*. 2024. No. 8(1): article 7. https://doi.org/10.3390/cryptography8010007