Ходимчак І.С.
студентка гр-НБ-11
юридичного факультету,
Західноукраїнський національний університет

Муравська Ю.Є.
к. ек. наук, доцент, завідувач кафедри безпеки та правоохоронної діяльності
Західноукраїнський національний університет

КІБЕРБЕЗПЕКА ЯК НОВИЙ ВИКЛИК ДЛЯ ДЕРЖАВИ

У сучасних умовах кібербезпека посідає важливе місце у системі національної безпеки держави. Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» кібербезпека є складовою національної безпеки України та спрямована на захист життєво важливих інтересів людини і громадянина, суспільства і держави у кіберпросторі[1]. Це говорить про те, що функціонування держави більше залежить від цифрового середовища й інформаційних технологій.

У Державній службі спеціального зв'язку та захисту інформації України зазначають: «Кількість кіберінцидентів в Україні щороку зростає, що свідчить про підвищення рівня кіберзагроз»[2]. Прикладом є сучасні кібератаки на державні органи України, які спрямовані на викрадення персональних даних громадян, знищення державних реєстрів та блокування доступу до критичних сервісів, наприклад, платформа «Дія». Як зазначено на сайті Держспецзв'язку, що у 2024-2025 роках інтенсивність зросла до 70%, причому хакери, підконтрольні спецслужбам РФ, дедалі частіше використовують методи багатоетапного фішингу. Ці диверсії синхронізувалися з ракетними ударами по енергетиці, супроводжувалися

масованими хвилями дезінформації для посилення паніки. Розглядаючи та аналізуючи ці виклики, ми розуміємо, якими методами користується агресор за для досягнення своїх цілей.

Одним із масштабних прикладів кібератак на Україну стала атака вірусу Not Petya у 2017 році. Вона була унікальною за масштабом, складністю та наміром, створюючи серйозні виклики для експертів з кібербезпеки та викликаючи серйозні занепокоєння щодо вразливості нашої взаємопов'язаної цифрової інфраструктури[7]. Як зазначається в матеріалах, оприлюднених із посиланням на видання *Wired*:

« Під час атаки небезпечного вірусу голова компанії Олексій Ясинський отримав дзвінок, в якому повідомляли про кібератаку на державний банк «Ощадбанк». Коли він прибув в офіс банку, то помітив, що робітники місцевого ІТ відділу не мали чіткого плану дій для боротьби з NotPetya. 90% машин були паралізовані вірусом. Далі на телефон Ясинського обрушилась лава дзвінків зі всієї України. Всі повідомляли про атаку злісного комп’ютерного вірусу. NotPetya встановив рекорд, обійшовши всі антивірусні бар’єри захисту протягом 45 секунд. Великий транспортний хаб «поляг» протягом 16 секунд»[8]. Саме ця атака завдала значних економічних збитків як Україні, так і іншим державам, а також продемонструвала вразливість критичної інфраструктури до кіберзагроз.

Після повномасштабного вторгнення Росії у 2022 році кількість кібератак проти України збільшилась та набрали системного характеру. Вони спрямовувалися на державні органи, об’єкти критичної інфраструктури та інформаційні ресурси з метою дестабілізації ситуації в країні. У день вторгнення було здійснено масштабну кібератаку на супутникову мережу Viasat, унаслідок якої тисячі модемів були виведені з ладу, що призвело до серйозних перебоїв у зв’язку та вплинуло на військові й державні комунікації [9].

У Стратегії кібербезпеки України зазначено, що: «зростання кількості та складності кібератак становить реальну загрозу національній безпеці»[3]. Це вказує на те, що вони мають значний дескрутивний вплив на функціонування державних інституцій та об'єктів критичної інфраструктури[4]. Але реалізація на 2021-2025 роки під координацією РНБО забезпечила високий рівень стійкості цифрових систем, причому станом на початок 2026 р. виконання профільних заходів сягнуло 86%.

Кіберзагрози дуже пов'язані із явищем гібридної війни. У документах НАТО підкреслює, що кіберпростір визнається окремою сферою ведення операцій. А також, що: «поєднання кібероперацій та інформаційного впливу є характерною ознакою сучасних конфліктів» [5]. Тому кібербезпека є невід'ємною складовою сучасної системи національної безпеки.

Кіберзагрози не обмежуються однією державою, тому важливе місце відіграє міжнародне співробітництво. У Будапештській конвенції наголошується: «Держави повинні забезпечувати взаємодію у сфері обміну інформацією щодо кіберзагроз»[6]. Це дозволяє підвищувати ефективність реагування на загрози, як на національному так і на міжнародному рівнях.

Забезпечення кібербезпеки ускладнюється різноманітними проблемами та викликами. Однією із найкритичніших проблем, як зазначає у звітах Європейський Союз є: «дефіцит кваліфікованих кадрів у сфері кібербезпеки»[4]. Сукупність цих факторів накладаються на недостатнє фінансування, яке не дозволяє вчасно оновлювати програмне забезпечення.

Для подолання кіберзагроз потрібно вдосконалювати стратегію кібербезпеки. Насамперед потрібно реформувати кіберосвіту. Як вказано у Стратегії кібербезпеки України: «розвиток кіберосвіти та підготовка фахівців є необхідною умовою підвищення рівня кібербезпеки»[3]. Критично важливим є інвестування в технології, зокрема впровадження штучного інтелекту(ШІ) для проактивного виявлення вразливостей та

перехід на захищенні хмарні рішення. Масова кібергігієна є надійним бар'єром проти соціальної інженерії та фітингу, тому окрему увагу слід приділити і цифровій грамотності населення. Фундаментом цих змін має стати посилення законодавства, яке поєднає українські норми зі стандартами ЄС і НАТО.

Отже, згідно зі Стратегією кібербезпеки України: «кібербезпека є ключовим фактором забезпечення державного суверенітету в умовах цифровізації»[3]. З поширенням новітніх технологій та ускладненням загроз її значення зростає. Ефективна протидія кіберзагрозам можлива лише тоді, коли комплексний підхід буде поєднувати державну політику, міжнародне співробітництво й розвиток суспільства.

Список використаних джерел

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-viii#Text (дата звернення: 04.05.2026)
2. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua (дата звернення: 04.05.2026)
3. Указ Президента України «Про Стратегію кібербезпеки України» від 26 серпня 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 04.05.2026).
4. Європейський Союз (ENISA). Cybersecurity Skills Development in the EU // ENISA Report. – 2022. – С. 12–18. URL: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union (дата звернення: 04.05.2026)
5. НАТО. Cyber Defence Policy and Concept // NATO Official Documents. – Brussels, 2020. – С. 3–7. URL: https://www.nato.int/en/about-

us/official-texts-and-resources/official-texts/2010/05/17/nato-2020-assured-security-dynamic-engagement?selectedLocale=uk (дата звернення: 04.05.2026)

6. Конвенція про кіберзлочинність від 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 04.05.2026).

7. Suhail M. NotPetya Cyber Attack: Unmasking a Destructive Wake-Up Call for Cybersecurity // LinkedIn. URL: https://ua.linkedin.com/pulse/notpetya-cyber-attack-unmasking-destructive-wake-up-call-suhail-m- (дата звернення: 04.05.2026)

8. NotPetya: наймасштабніша кібератака в історії України // Imena.ua. – URL: https://www.imena.ua/blog/notpetya-cyberattack/ (дата звернення: 04.05.2026)

9. Viasat KA-SAT cyberattack case study // CyberPeace Institute. URL: https://cyberconflicts.cyberpeaceinstitute.org (дата звернення: 04.05.2026)