

ВПЛИВ КІБЕРХАКАТОНІВ НА НАВЧАННЯ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

Наталія Черняшук, Катерина Гаврилюк

THE IMPACT OF CYBER HACKATHONS ON THE TRAINING OF CYBERSECURITY AND COMPUTER NETWORK SPECIALISTS

Nataliia Cherniashchuk, Kateryna Havryliuk

Abstract. *This article explores the role of cyber hackathons in training specialists in cybersecurity and computer networks. It analyzes their impact on the development of practical skills in comparison with traditional teaching methods and examines international practices of organizing such events. Based on data from hackathons such as DEF CON CTF, Pwn2Own, and Hack The Box, the study demonstrates that interactive competitions are an effective tool for building professional competencies. The results show that hackathon participants grasp complex concepts 30–50% faster than students in conventional courses.*

У сучасному цифровому світі кібербезпека та комп'ютерні мережі є двома взаємопов'язаними галузями, які відіграють ключову роль у забезпеченні стабільного та безпечного функціонування інформаційних систем. З розвитком технологій зростає кількість кіберзагроз, які стають дедалі складнішими та витонченішими, що вимагає від фахівців не лише глибоких теоретичних знань, а й високого рівня практичних навичок для ефективного протидіяння атакам, аналізу вразливостей та швидкого реагування на потенційні загрози. Традиційні методи навчання, такі як лекції, семінари та лабораторні роботи, безумовно, забезпечують міцну фундаментальну базу для підготовки майбутніх спеціалістів.

Однак вони часто не здатні в повній мірі передати досвід роботи у реальних умовах, де загрози постійно змінюються, а швидкість реагування має вирішальне значення. Теоретичні знання важливі, але без практичного застосування вони можуть виявитися недостатніми у критичних ситуаціях. Саме тому сучасні методи навчання повинні включати інтерактивні підходи, які дозволяють студентам та фахівцям застосовувати отримані знання у реальних сценаріях.

Одним із найефективніших способів практичного навчання у сфері кібербезпеки є *кіберхакатони* – інтенсивні командні змагання, що імітують реальні сценарії кібератак та захисту. Вони дозволяють учасникам випробувати свої навички у різноманітних аспектах, таких як аналіз загроз, етичний хакинг, криптографія, пошук та усунення вразливостей, цифрова криміналістика та реагування на інциденти. Завдяки такому підходу учасники отримують безцінний досвід роботи у стресових умовах, що максимально наближені до реальних атак, а також розвивають критичне мислення, командну взаємодію та вміння швидко ухвалювати рішення.

Метою роботи є аналіз та оцінка ефективності хакатонів як навчального інструменту, порівняння їх із традиційними методами та визначення оптимальних підходів для підготовки фахівців насамперед із кібербезпеки та комп'ютерних мереж.

Кіберхакатони відіграють ключову роль у підготовці фахівців з комп'ютерних мереж, оскільки забезпечують моделювання реальних інцидентів і створюють умови, наближені до тих, з якими спеціалісти стикаються у професійному середовищі. Учасники мають можливість працювати з відновленням роботи мереж після атак, налаштовувати маршрутизатори в умовах обмеженого часу та оперативно приймати рішення для забезпечення стабільної роботи інфраструктури [4].

Окрім цього, хакатони допомагають розвивати навички автоматизації, що є важливою складовою сучасної кібербезпеки. Використання мов програмування, таких як Python, дозволяє учасникам створювати скрипти для моніторингу трафіку, аналізу логів та автоматизації мережевих процесів.

Це значно підвищує ефективність управління інфраструктурою та дає змогу швидше реагувати на потенційні загрози [9].

Ще одним важливим аспектом, який розкривається під час хакатонів, є розуміння концепцій програмно-визначених мереж (SDN). Деякі змагання включають завдання, що передбачають програмування мережевих контролерів, що дає змогу учасникам краще зрозуміти сучасні підходи до управління трафіком і безпекою в корпоративних мережах [11].

Прикладом такого підходу є хакатон Network Security Challenge, де учасникам пропонують знайти вразливості у віртуальній корпоративній мережі. Для цього потрібно застосовувати знання про VLAN, списки контролю доступу (ACL), а також системи виявлення та запобігання вторгненням (IDS/IPS).

Подібні завдання не лише перевіряють технічну підготовку, а й навчають працювати у реальних умовах кіберзагроз, що робить кіберхакатони незамінним елементом у підготовці висококваліфікованих мережевих спеціалістів [5].

Дослідивши та проаналізувавши популярні форуми з опитуваннями вдалося з'ясувати, що багато учасників (близько 80% із опитаних) відзначили зростання професійних зв'язків, а 54% знайшли роботу через хакатони (переважно в Palo Alto Networks, Cisco і компаніях, які були спонсорами та партнерами проведення).

Загалом усі статистики та дослідження вказують на те, що учасники кіберхакатонів мають більше шансів на вдале працевлаштування, підвищення заробітної плати, кар'єрний ріст тощо (рис. 1).

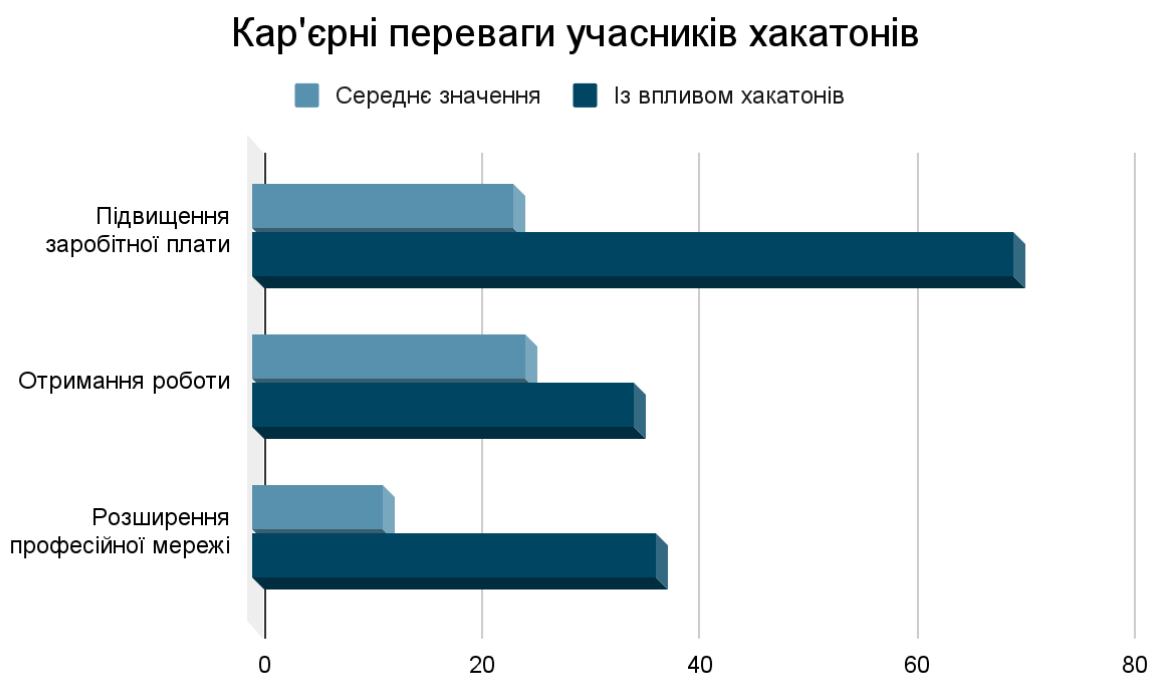


Рис.

1. Гістограма “Кар’єрні переваги учасників хакатонів”

На основі даних з міжнародних змагань за останні роки було виявлено певні тенденції щодо різних форматів хакатонів (табл. 2). На сьогоднішній день, за даними CTFtime.org, формат CTF залишається найпопулярнішим серед міжнародних змагань (близько 62% усіх змагань), що підтверджується статистикою участі та кількості подій [7].

Це пояснюється стандартизованою структурою завдань і низьким бар'єром входження для новачків (рис. 2). Також було помічено, що віртуальні лабораторії демонструють найшвидше зростання аудиторії (+17% у 2024 році).

Таблиця 2 – Характеристики основних форматів кіберхакатонів

Формат	Тривалість	Середня кількість команд	Найпопулярніші навички	Переваги над іншими
CTF	24-48 год	85±12	Криптографія, реверс-інжиніринг	Висока доступність
Attack-Defence	48-72 год	40±8	Мережева безпека, експлуатація	Реалістичні сценарії
Віртуальні	Без обмежень	200+	Веб-експлуатація, пантест	Гнучкість участі

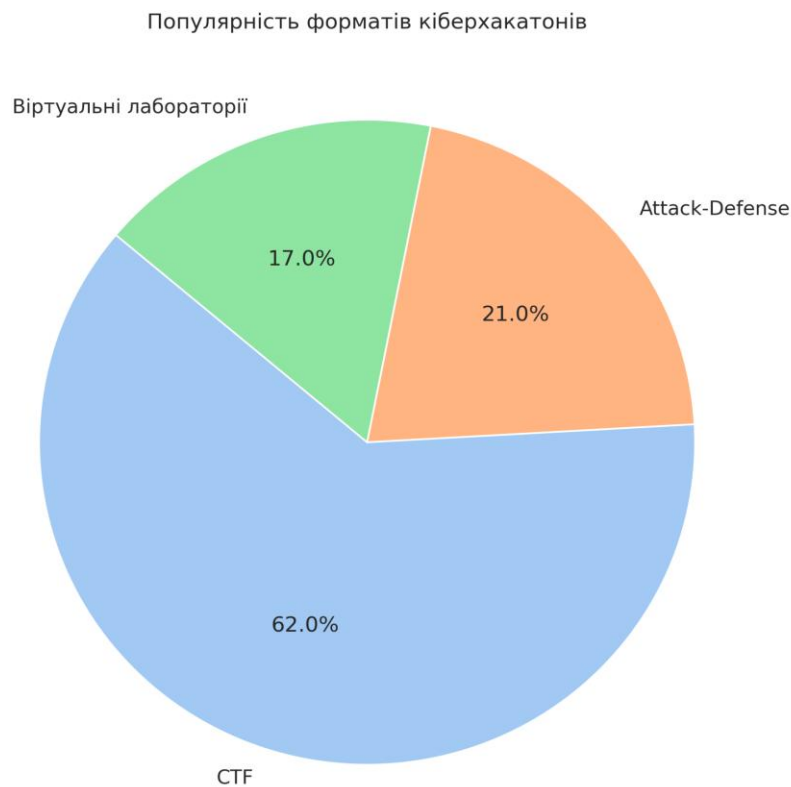


Рис. 2 – Кругова діаграма “Популярність форматів кіберхакатонів”

Кіберхакатони стали потужним інструментом для навчання фахівців з кібербезпеки та комп'ютерних мереж. Вони не лише доповнюють традиційну освіту, але й надають учасникам можливість застосувати теоретичні знання на практиці у реальних умовах.

Через інтерактивний формат та змагальний дух хакатони розвивають критичне мислення, командну роботу та вміння швидко реагувати на загрози, що є критично важливим у сучасному цифровому світі.

Україна, незважаючи на складні умови війни, активно використовує хакатони для підготовки фахівців та протидії кібератакам. Заходи, такі як Cyber Unity Hackathon та IT Army Hackathon, демонструють, як хакатони можуть стати інструментом не лише для навчання, але й для реального захисту країни.

Співпраця з міжнародними організаціями, такими як НАТО та ЄС, дозволяє Україні інтегруватися у глобальну спільноту кібербезпеки та отримувати доступ до новітніх технологій.

Бібліографія

1. Міністерство цифрової трансформації України. Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua/> (дата звернення: 25.03.2025).
2. ACM digital library: integrating hackathons into an online cybersecurity course. ACM Digital Library. URL: <https://doi.org/10.1145/3510456.3514151> (date of access: 11.04.2025).
3. Black hat. Black Hat | Home. URL: <https://www.blackhat.com/> (date of access: 11.04.2025).
4. CISA probationary reinstatements. America's Cyber Defense Agency. URL: <https://www.cisa.gov/> (дата звернення: 12.04.2025).
5. Cisco live. Cisco. URL: <https://www.ciscolive.com/> (date of access: 25.03.2025).
6. Codegate. CODEGATE. URL: <https://ctf.codegate.org/> (date of access: 28.03.2025).
7. CTFtime.org / CTF teams. CTFtime.org / All about CTF (Capture The Flag). URL: <https://ctftime.org/stats/2024/> (date of access: 11.04.2025).
8. DEF CON® hacking conference - capture the flag archive. DEF CON® Hacking Conference Home. URL: <https://defcon.org/html/links/dc-ctf.html> (date of access: 13.04.2025).
9. Hack-A-Sat. Hackasat. URL: <https://hackasat.com> (date of access: 03.04.2025).