УДК 004.056.53

І. О. Бондаренко
А. Р. Магденко
Д. О. Пінчук

ЕТИКА ХАКЕРСТВА: ЧИ МОЖУТЬ «БІЛІ ХАКЕРИ» БУТИ КОРИСНИМИ?

Вінницький національний технічний університет

Анотація

У тезах розглядається феномен етичного хакерства як складова сучасної кібербезпеки. Зокрема, аналізується роль так званих «білих хакерів» у виявленні вразливостей, захисті інформаційних систем та запобіганні кібератакам. Також досліджуються морально-етичні та правові аспекти їхньої діяльності. У роботі використано порівняльний аналіз міжнародного досвіду регулювання етичного хакерства та наведено приклади ефективної співпраці білих хакерів з державними й приватними структурами.

Ключові слова: етичне хакерство, білі хакери, кібербезпека, соціальна інженерія, етика, кіберзлочинність.

Abstract

The thesis discusses the phenomenon of ethical hacking as a component of modern cybersecurity. In particular, the role of the so-called "white hackers" in identifying vulnerabilities, protecting information systems and preventing cyberattacks is analyzed. The moral, ethical, and legal aspects of their activities are also studied. The paper uses a comparative analysis of international experience in regulating ethical hacking and provides examples of effective cooperation between white hackers and public and private entities.

Keywords: ethical hacking, white hackers, cybersecurity, social engineering, ethics, cybercrime.

Вступ

У XXI столітті технологічна революція зробила цифровий простір невід'ємною частиною людського життя. Сучасне суспільство дедалі більше залежить від інформаційних технологій у всіх сферах: від економіки й охорони здоров'я до освіти, безпеки та побуту. Разом із цим зростає і кількість кіберзагроз – зловмисники використовують високотехнологічні засоби для крадіжки даних, вимагання, шантажу, саботажу, підриву критичної інфраструктури тощо.

У цих умовах з'являється нове явище – етичне хакерство. Це цілеспрямована діяльність, метою якої є виявлення слабких місць у системах до того, як їх використають зловмисники. Етичні хакери, або «білі хакери» (white hat hackers), на відміну від чорних хакерів (black hat), працюють з дозволу власників системи і спрямовують свої зусилля на зміцнення кіберзахисту.

Попри зростаюче визнання ролі білих хакерів, досі не існує однозначної відповіді на питання: чи є їхня діяльність етично прийнятною, соціально корисною і юридично безпечною? Багато країн не мають чіткого правового регулювання такого типу роботи, а етичні межі хакерства залишаються суперечливими. Сам факт «втручання» у систему може сприйматися як загроза, навіть якщо це робиться з добрими намірами [1].

Результати дослідження

Етичні хакери, або так звані «білі хакери», є фахівцями, які використовують ті самі інструменти, техніки та знання, що й злочинні хакери (black hat), але з єдиною різницею – їхня діяльність спрямована на захист, а не на атаку. Основним завданням білих хакерів є виявлення вразливостей в інформаційних системах до того, як ними скористаються зловмисники. Така практика відома як penetration testing (пентест) – цілеспрямоване моделювання атак з метою виявлення слабких місць у мережі, програмному забезпеченні чи апаратних засобах.

Білі хакери часто працюють на аутсорсі або в межах внутрішніх команд безпеки компаній. Їх також активно залучають до внутрішнього аудиту інформаційної безпеки, підготовки до сертифікацій (наприклад, ISO/IEC 27001), а також під час розробки нових продуктів, де потрібно оцінити надійність архітектури безпеки.

Існують численні приклади, коли завдяки роботі білих хакерів було попереджено масові витоки даних або блокування критичних систем. Наприклад, у 2021 році етичний хакер знайденого критичну вразливість у платформі Twitter API, яка могла дозволити несанкціонований доступ до особистих даних мільйонів користувачів. Зловмисники могли б використати це для фішингових атак або масових спроб викрадення акаунтів.

Також важливою сферою участі білих хакерів є програми винагород за баги (Bug Bounty). Багато міжнародних компаній, як-от Google, Facebook, Microsoft, Apple, Uber тощо, мають постійно діючі програми, у межах яких будь-хто (але за чіткими умовами) може тестувати безпеку їхніх систем і отримати за це грошову винагороду. Наприклад, Google у 2022 році виплатив понад 10 мільйонів доларів у межах програми Google Vulnerability Reward Program (VRP). Це яскраво свідчить про ефективність залучення зовнішніх експертів до виявлення проблем [2].

Один з найскладніших аспектів діяльності білих хакерів – етичне та правове регулювання їхньої роботи. Хоча їхня діяльність зазвичай узгоджується з компанією або структурою, яку вони перевіряють, межа між легітимним тестуванням і потенційним правопорушенням дуже тонка (рис.1).

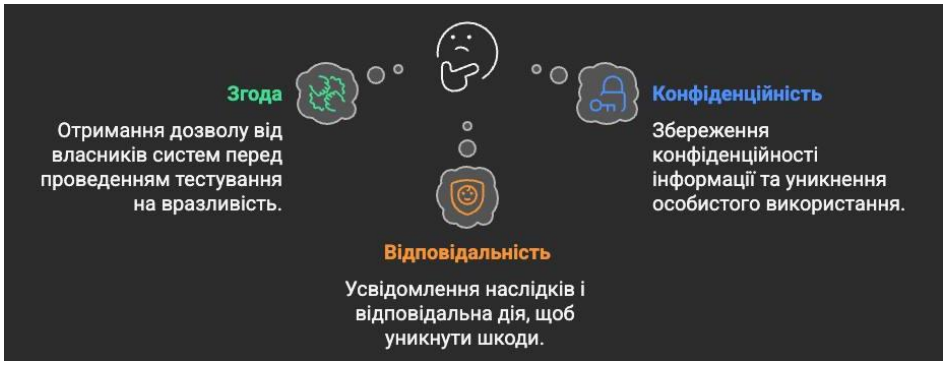

Рисунок 1 – Етичні аспекти білих хакерів

Зокрема, якщо хакер не отримав прямий дозвіл (ліцензію або контракт) на перевірку, навіть добросовісне виявлення вразливості може вважатися порушенням закону. Наприклад, у США відповідно до Computer Fraud and Abuse Act (CFAA) будь-яке несанкціоноване проникнення в комп'ютерну систему – навіть без злого наміру – розглядається як злочин. Це створює правову колізію, коли хакер діє в інтересах безпеки, але може бути притягнутий до відповідальності за сам факт доступу [3].

З іншого боку, деякі країни та організації поступово адаптують законодавство до нових реалій. Так, у ЄС активно просувається ідея десятого принципу "Responsible Disclosure", за яким етичні хакери повинні мати можливість повідомити про вразливість без ризику переслідування. У 2021 році Нідерланди ухвалили рекомендації, які офіційно закликають до співпраці з хакерами, що діють етично.

Також важливе місце займає етика взаємодії хакера з організацією. Хакер не має права шантажувати компанію, вимагати гроші за нерозголошення вразливостей або створювати навмисні ушкодження системи навіть у межах тестування. Етичний кодекс професійного хакера має передбачати повну прозорість, добросовісність, відповідальність та дотримання умов договору [4].

Отже, етичне хакерство потребує не лише технічної, а й глибокої морально-правової підготовки. Формування чітких юридичних рамок та професійної етики – ключ до легітимізації цієї професії.

Діяльність білих хакерів має не лише технічний, а й соціальний вимір. У часи цифровізації практично всіх аспектів нашого життя – від банкінгу до охорони здоров'я – захист персональних даних, приватності, критичної інфраструктури стає справою загального значення. І саме етичні хакери часто є першими, хто звертає увагу на потенційні небезпеки.

Наприклад, у 2017 році білі хакери виявили вразливість у мобільному додатку для управління пацієнтськими даними в одній із найбільших клінічних мереж США. Проблема дозволяла доступ до медичних карток понад 150 тисяч осіб. Завдяки повідомленню білих хакерів проблему було усунуто протягом 72 годин, і не відбулося жодного витоку.

Інший приклад – ініціатива Hack the Pentagon, запущена Міністерством оборони США у 2016 році. У рамках програми сотні етичних хакерів отримали змогу перевірити безпеку урядових сайтів та

сервісів. Усього за кілька тижнів було виявлено понад 1200 вразливостей, і багато з них були визнані критичними.

Також етичні хакери часто виконують роль просвітників і наставників, проводячи воркшопи, тренінги, участь у змаганнях типу Capture the Flag (CTF), де молодь навчається основам безпеки в ігровому форматі. Це створює культуру інформаційної безпеки серед нових поколінь фахівців, формуючи відповідальне ставлення до технологій.

Окрім того, співпраця компаній із білими хакерами сприяє підвищенню довіри користувачів, демонструючи відкритість та готовність працювати над покращенням безпеки. Це стає конкурентною перевагою на ринку, особливо в галузях, де захист даних є критично важливим (банки, медичні установи, технологічні компанії) [5].

В Україні етичне хакерство розвивалося ще до 2022 року, але саме війна стала каталізатором зростання цієї сфери. З початком повномасштабного вторгнення з'явилася ініціатива IT-армії України – об'єднання добровольців, які за згодою та в межах узгоджених дій здійснюють атаки на російські пропагандистські ресурси, державні сервіси та фінансові системи. Це створило безпрецедентний прецедент, коли хакерська діяльність стала частиною державної оборони – в межах міжнародного гуманітарного права та загальних принципів кіберетики.

Паралельно з цим зросла активність білих хакерів у сфері захисту українських цифрових сервісів. Наприклад, програма багбаунті "Дія", запущена Міністерством цифрової трансформації у партнерстві з Ukrainian Cybersecurity Cluster, дозволила етичним хакерам легально тестувати платформу на наявність вразливостей. Участь у програмі брали як українські, так і міжнародні фахівці. Держава не лише заохочувала таку участь, а й виплачувала винагороди за виявлені баги, що стало прикладом конструктивної співпраці з хакерською спільнотою [6].

В Україні поки що відсутнє чітке правове регулювання діяльності етичних хакерів. Відповідно до чинного законодавства, несанкціонований доступ до комп'ютерної системи (навіть якщо він був зроблений "на благо") може кваліфікуватися як злочин, передбачений статтями 361–363 Кримінального кодексу України. Таким чином, етичні хакери можуть потрапити під кримінальну відповідальність, якщо не мають офіційного дозволу на свою діяльність або не діють у межах державних ініціатив [7].

Велике значення у формуванні культури етичного хакерства в Україні відіграє система освіти та просвітницькі ініціативи. Громадські організації, такі як Ukrainian Cyber Alliance**,** CyberHub Ukraine**,** Hackerspace Ukraine активно проводять хакатони, тренінги, Capture The Flag-змагання, воркшопи з етичного зламу, зокрема для школярів, студентів і молодих IT-фахівців. Завдяки таким заходам в Україні формується нове покоління свідомих кіберспеціалістів**,** які розуміють, що етика і технології мають йти поруч [8].

Висновки

У результаті проведеного аналізу було встановлено, що діяльність етичних хакерів має суттєве значення для забезпечення безпеки цифрового простору. Вони є не просто технічними консультантами, а ключовими гравцями в екосистемі кіберзахисту, здатними ефективно ідентифікувати потенційні загрози до того, як ці загрози перетворяться на масштабні інциденти. Їхня участь у процесах тестування, аудиту, прогнозування атак, розробки захисних механізмів є надзвичайно цінною як для приватного бізнесу, так і для державного сектору.

Етичні хакери довели свою ефективність через практичні кейси, серед яких – запобігання витокам особистих даних, виявлення критичних вразливостей у програмному забезпеченні, а також участь у програмах Bug Bounty, які стали популярним та ефективним інструментом взаємодії між хакерами та компаніями. Водночас етична сторона питання залишається складною: порушення приватності, недовіра з боку держави, правова невизначеність – усе це створює ризики як для самих хакерів, так і для структур, що співпрацюють із ними.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is ethical hacking? IBM – Україна. URL: https://www.ibm.com/topics/ethical-hacking (дата звернення: 29.03.2025).

2. Етичні хакери – захисники цифрового світу. Національний координаційний центр кібербезпеки при РНБО України. URL: https://ncscc.gov.ua/news/etychni-hakery-zahysnyky-tsyfrovoho-svitu (дата звернення: 31.03.2025).

3. Кримінальна відповідальність за несанкціоноване втручання в комп'ютерні системи: аналіз закону США (CFAA). U.S. Department of Justice. URL: https://www.justice.gov/criminal-ccips/computer-fraud-and-abuse-act (дата звернення: 31.03.2025).

4. Хакери з етикою: як в Україні формують культуру кібербезпеки. Мінцифра України. URL: https://thedigital.gov.ua/news/kiberbezpeka-v-ukraini-etichni-khakery-ta-novi-initsiatyvy (дата звернення: 01.04.2025).

5. Hack the Pentagon – перша урядова Bug Bounty програма. Міністерство оборони США. URL: https://www.defense.gov/News/News-Stories/Article/Article/684018/dod-launches-hack-the-pentagon/ (дата звернення: 03.04.2025).

6. Багбаунті Дії: челендж для етичних хакерів. Дія. URL: https://diia.gov.ua/news/bagbaunti-diyi-chelendzh-dlya-etichnih-hakeriv (дата звернення: 03.04.2025).

7. Кримінальний кодекс України. Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 15.04.2025).

8. Ukrainian Cyber Alliance. URL: https://en.wikipedia.org/wiki/Ukrainian_Cyber_Alliance (дата звернення: 17.04.2025).

Магденко Анастасія Романівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anastasiiamahdenko@gmail.com

Пінчук Дар'я Олександрівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Науковий керівник: ***Бондаренко Ірина Олексіївна*** **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Mahdenko Anastasiia R. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anastasiiamahdenko@gmail.com

Pinchuk Daria O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Supervisor*:* ***Bondarenko Iryna O.*** **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua