Борко Надія Олександрівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ ТА СВІТІ: ЕКЗИСТЕНЦІЙНИЙ АНАЛІЗ, МЕТОДОЛОГІЯ АТАК І СТРАТЕГІЇ ПРОТИДІЇ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Сучасна цивілізація перебуває на етапі цифрової трансформації, де інформаційно-комунікаційні технології (ІКТ) виступають критичним каталізатором для функціонування усіх сфер життєдіяльності – від електронного урядування та e-commerce до управління критичними інфраструктурами [1]. Ця технологічна інтеграція забезпечує безпрецедентну ефективність, але водночас формує ефект гіперзалежності від цифрового простору, роблячи будь-яку мережеву систему потенційним об'єктом атаки. У цьому контексті кіберзлочинність перестала бути виключно технічною проблемою, перетворившись на системну загрозу XXI століття, що зачіпає національну безпеку, економічну стійкість та фундаментальні права людини на конфіденційність [2].

Кіберзлочинність охоплює незаконні дії, які здійснюються за допомогою ІКТ або спрямовані проти них. Концептуальна основа цього явища, закріплена у міжнародних документах, таких як Конвенція Ради Європи про кіберзлочинність, стосується порушення тріади цілісності, конфіденційності та доступності комп'ютерних даних і систем (CIA Triad). До основних видів кіберзлочинів належать: несанкціоноване заволодіння коштами, кібершпигунство, шантаж,

розповсюдження шкідливого програмного забезпечення та атаки на державні й комерційні системи. Їх транскордонний та анонімний характер ускладнює ефективну протидію, оскільки агресор може діяти з будь-якої точки світу, мінімізуючи юридичну відповідальність [3].

Методологія кіберзлочинності відзначається високою технологічною складністю, що підтверджують численні інциденти. Наприклад, атака на критичну інфраструктуру Західної України у 2015 році, здійснена угрупованням «Sandworm» із використанням шкідливого ПЗ BlackEnergy 3, призвела до відключення електропостачання понад 225 тисяч споживачів [4]. Цей кейс став прецедентом у світі і показав, як кіберзлочини можуть слугувати інструментом гібридної війни.

Фінансовий сектор також часто стає об'єктом кібератак. Група Carbanak викрала понад $1 млрд, маніпулюючи внутрішніми банківськими системами, використовуючи фішинг та банківські трояни, замасковані під легітимні оновлення [5]. Крім того, порушення доступності систем через DoS/DDoS-атаки, які часто здійснюють ботнети – централізовано керовані мережі заражених пристроїв, призводять до економічних втрат і підриву довіри до державних та комерційних порталів. Прикладом є серія атак на українські урядові сервіси у 2020 році [6].

Викрадення даних і застосування програм-вимагачів (ransomware) – ще одна загроза. Наприклад, DarkSide зашифрувала дані Colonial Pipeline у США в 2021 році, що спричинило дефіцит пального і підкреслило залежність фізичної інфраструктури від цифрової безпеки [7].

Зростання кіберзлочинності визначається кількома ключовими детермінантами. По-перше, технологічна експансія та зростання кількості пристроїв Інтернету речей (IoT) створюють величезну кількість точок вразливості [8]. По-друге, низький рівень цифрової грамотності та нехтування кібергігієною серед користувачів забезпечує успіх атак із застосуванням соціальної інженерії [9]. По-третє, професіоналізація та комерціалізація кіберзлочинності на чорному ринку знизили поріг входу для потенційних злочинців [10].

Комплексний підхід до кібербезпеки передбачає дії на різних рівнях. На корпоративному та індивідуальному рівні необхідне суворе дотримання кібергігієни: багатофакторна автентифікація, регулярне оновлення програмного забезпечення,

резервне копіювання даних. На державному рівні потрібне вдосконалення законодавства, наприклад, через реалізацію Закону України «Про основні засади забезпечення кібербезпеки України», та зміцнення інституцій, таких як Департамент кіберполіції, для ефективного розкриття транскордонних злочинів.

Лише узгоджена стратегія, що поєднує технологічну стійкість, юридичну відповідальність та високий рівень обізнаності користувачів, здатна забезпечити надійний захист цифрового середовища та зберегти стабільність суспільства перед обличчям кіберзагроз.

Список використаних джерел

1. Laudon, K., & Laudon, J. (2020). *Management Information Systems: Managing the Digital Firm*. Pearson.
2. Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
3. Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
4. Zetter, K. (2016). *Inside the Cyberattack that Shocked the US and Ukraine*. Wired.
5. Symantec Security Response. (2018). *Carbanak Gang Analysis Report*.
6. CERT-UA. (2020). *Annual Report on DDoS Attacks Against Ukrainian Government Services*.
7. FBI & CISA. (2021). *Colonial Pipeline Ransomware Incident Report*.
8. Rose, S., et al. (2019). *Zero Trust Architecture*. NIST Special Publication 800-207.
9. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.
10. Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA)*.