https://www.researchgate.net/publication/369110221_Classification_of_BATSE_Swift_and_Fermi_Gamma-Ray_Bursts_from_Prompt_Emission_Alone

7. *Power BI vs. Tableau: Which is The Better Business Intelligence Tool in 2025?* (2024, November 25). DataCamp. https://www.datacamp.com/blog/power-bi-vs-tableau-which-one-should-you-choose?

8. *Which one is better: Bokeh or Plotly?* (2024, August 5). GeeksforGeeks. https://www.geeksforgeeks.org/which-one-is-better-bokeh-or-plotly/

Борусевич В.В.,
здобувачка першого (бакалаврського) рівня вищої освіти,
Ріппа С.П.,
д.е.н., професор,
Київський національний економічний університет імені Вадима Гетьмана

ВПЛИВ КІБЕРЗЛОЧИННОСТІ НА ГЛОБАЛЬНУ СТАБІЛЬНІСТЬ: НОВІ ВИКЛИКИ ЦИФРОВОЇ ЕПОХИ

У 21 столітті цифрові технології стали невід’ємною частиною нашого життя. Від щоденного спілкування в соціальних мережах до онлайн-банкінгу, від хмарних сховищ даних до "розумних" міст — інтернет і комп’ютерні системи об’єднали світ, зробивши його швидким та зручним. Однак разом із цими перевагами з’явилися й нові загрози.

Кіберзлочинність сьогодні — це не просто віруси, які можуть знищити файли на домашньому комп’ютері. Це складні, часто державно-спонсоровані атаки, спрямовані на крадіжку конфіденційних даних (особистих, фінансових, корпоративних), дестабілізацію критичної інфраструктури (енергосистем, лікарень, транспортних мереж), маніпулювання громадською думкою через фейкові новини та соціальні мережі.

Ще 10–15 років тому кібербезпека була проблемою переважно IT-фахівців. Сьогодні ж уразливим може бути будь-хто: звичайні користувачі — через витоки

паролів, фішинг або шахрайство в месенджерах; бізнес — через атаки на сервери або шантаж вірусами-шифрувальниками; держави — через кібершпигунство або саботаж. За даними дослідників Cybersecurity Ventures [1], до 2025 року збитки від кіберзлочинності вже досягли 10,5 трлн доларів на рік. Такі інциденти, як масова атака вірусом WannaCry у 2017 році [2] або кібератаки під час російсько-української війни, показали, що кіберпростір став новим полем битви — не менш важливим, ніж традиційні військові дії.

Сучасний цифровий світ стикається з широким спектром кіберзагроз, які стають все більш витонченими та небезпечними. Однією з найпоширеніших і найефективніших залишається соціальна інженерія, зокрема фішинг – коли зловмисники надсилають підроблені листи або створюють сайти, що імітують офіційні ресурси банків, соцмереж чи державних установ. Ці атаки часто починаються з нібито невинного повідомлення про блокування картки чи необхідність підтвердити облікові дані, але насправді ведуть до викрадення конфіденційної інформації. Окремо варто згадати вішинг, коли шахраї телефонують жертвам під виглядом співробітників банків, і претекстинг, де зловмисники видають себе за технічну підтримку, щоб отримати доступ до пристроїв.

Шкідливе програмне забезпечення залишається серйозною загрозою, особливо віруси-шифрувальники (Ransomware) [3], які блокують файли та вимагають викуп за їх розшифрування. Такі атаки можуть паралізувати роботу цілих компаній і призводять до мільйонних збитків. Троянські програми, які маскуються під корисні додатки, та кейлоггери, що фіксують натискання клавіш для крадіжки паролів, також становлять значну небезпеку.

Мережева інфраструктура постійно піддається атакам, серед яких найбільш руйнівними є DDoS-атаки, коли сервери "завалюються" під навалом мільйонів запитів. Такі атаки часто використовуються проти урядових ресурсів під час політичних конфліктів. Не менш небезпечні атаки типу "Людина посередині", коли зловмисники перехоплюють дані через незахищені Wi-Fi-мережі, або SQL-ін'єкції, що дозволяють отримати доступ до баз даних вебсайтів.

З розвитком технологій Інтернету речей (IoT) з'явилися нові загрози – наприклад, ботнети з "розумних" пристроїв, які використовуються для масованих кібератак. Камери спостереження, термостати, wifi-кавоварки та навіть онлайн-телевізори можуть стати частиною мережі заражених пристроїв, як це сталося з ботнетом Mirai, який об'єднав сотні тисяч девайсів. Особливо небезпечні атаки на промислові системи, оскільки вони можуть призвести до зупинки або катастрофічних наслідків для цілих виробництв або енергетичних об'єктів. Нескладно уявити рівень небезпеки для суспільства, коли об'єктами масованих кібератак становляться атомні електростанції, хімічні виробництва, медичні заклади тощо. В цих умовах загрози можливих катастрофічних наслідків набувають глобальних масштабів, які можна прирівняти до руйнувань від ядерної зброї чи космічних катаклізмів.

Окрему загрозу в останні часи становлять технології штучного інтелекту (ШІ) як інструмент кіберзлочинності, зокрема deepfake, які дозволяють створювати реалістичні аудіо- та відеопідробки для шахрайства. Наприклад, зловмисники можуть згенерувати голос керівника компанії, щоб вимагати переказ коштів. Криптовалютна сфера також не залишається поза межами атак кіберзлочинців: зловмисники використовують чуже обладнання для майнінгу (криптоджекінг) або проводять складні атаки на блокчейн-протоколи, викрадаючи криптовалюту в астрономічних сумах. У той же час ШІ активно використовується для виявлення шахрайства на крипторинках. Типовим зразком подібних технологій є ізраїльська платформа Alterya, яка значно пришвидшує виявлення криптовалютних зловмисників. Згідно з повідомленням компанії Chainalysis [4] ця платформа забезпечує захист платежів у реальному часі та ефективніше виявляє шахрайство під час перевірки клієнтів (KYC) для біткоїн-бірж, блокчейнів та постачальників крипто-гаманців. За оцінками експертів, технології Alterya вже допомогли провідним біткоїн-біржам скоротити шахрайства на 60%, зменшити кількість суперечок, пов’язаних із шахрайством, та підвищити ефективність роботи в сфері кібербезпеки.

Державні кіберзагрози набувають все більшого масштабу – це і цілеспрямовані APT-атаки, які проводяться спецслужбами, і кібершпигунство, спрямоване на викрадення технологій чи державних таємниць. У світі все частіше говорять про кібервійну, коли атаки на критичну інфраструктуру стають частиною гібридних конфліктів.

Статистика свідчить, що кібератаки відбуваються кожні 39 секунд, причому 94% вірусів надходять саме через електронну пошту. Втрати від кіберзлочинності щороку зростають на 15%, а 60% малих бізнесів закриваються вже через півроку після серйозного кіберінциденту.

Сучасні загрози постійно еволюціонують, і методи захисту, які працювали вчора, можуть виявитися неефективними сьогодні. Тому кібербезпека – це не просто набір технічних заходів, а безперервний процес адаптації до нових викликів цифрової епохи.

У підсумку, кіберзлочинність у цифрову епоху впевнено можна віднести до глобального виклику, що охоплює усі сфери життя — від особистої безпеки до національної стабільності. З розвитком технологій зростає не лише кількість, а й складність кібератак, які дедалі частіше використовують інструменти штучного інтелекту, що свідчить про новий рівень глобальних загроз. Водночас, як показує практика, ШІ може бути й потужним союзником у боротьбі з кіберзлочинністю і підвищенні ефективності виявлення шахрайства і забезпечення інформаційного захисту. У цих умовах кібербезпека має стати пріоритетом не лише для ІТ-фахівців, а й для суспільства загалом. Лише завдяки поєднанню технологічних інновацій, правового регулювання та міжнародної співпраці можливо забезпечити стабільність і безпеку у світі, де розмежування між віртуальним і реальним світами все швидше зникає.

Список використаних джерел

1. Cybercrime To Cost The World 8 Trillion Annually In 2023. (2023). Research. Cybercrime Magazine, Отримано травень 20, 2025, https://cybersecurityventures. com/cybercrime-to-cost-the-world-8-trillion-annually-in -2023/

2. Вірус WannaCry пошкодив комп'ютери у 99 країнах світу. (2017, травень 13). *Головне.* BBC News Україна, Отримано травень 20, 2025, https://www.bbc.com/ ukrainian/features-39907984

3. Програми-вимагачі: вектор атак на підприємства. (2025). *Підтримка*. Eset, Отримано травень 20, 2025, https://www.eset.com/ua/support/information/ entsy klopediya-zahroz/ataka-prohram-vymahachiv-na-pidpryyemstvo/

4. Грищенко В. (2025, січень 14). Chainalysis придбав ШІ-платформу з виявлення шахрайства. *Бізнес*. Bitcoin Magazine, Отримано травень 20, 2025, https://bit coinmagazine.ua/technologies/1734956506-adam-bek-peven-shcho-kvantovi-obchi slen nya

Валькова Н.В.,
к.е.н., доцент,
Хмельницький національний університет

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБЛІКОВОЇ ІНФОРМАЦІЇ

У сучасних умовах функціонування економіки, що характеризуються високим рівнем цифровізації, поширенням кіберзагроз та загостренням конкурентної боротьби, безпека облікової інформації підприємств набуває критичного значення. Облікова інформація є основою для формування управлінської, фінансової, податкової, статистичної звітності, а також звітності зі сталого розвитку. Усі перелічені види звітності є інформаційною основою для аналітичного забезпечення прийняття управлінських рішень економічних систем різного рівня. Крім того, облікова інформація має виключне значення для здійснення контролю за діяльністю підприємств та забезпечення їх фінансової прозорості. Саме від її достовірності, повноти, своєчасності та захищеності залежить не лише ефективність управління, а й фінансова стабільність та репутація суб’єкта господарювання.