УДК 338.245:338.656

З.П. Двуліт[1],
С.А. Завербний[1]
М.Т. Гладун[1],

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВІЙНИ

[1] Національний університет «Львівська політехніка»

Анотація: *У статті проаналізовано сучасні проблеми та перспективи розвитку кібербезпеки в Україні в умовах війни. Охарактеризовано види загроз та можливі шляхи для їх запобігання в критичних умовах.*
Ключові слова: інформація, діджиталізування, кібератаки, кіберзлочини, російська агресія, критична інфраструктура.

Abstract: *The article analyzes the current problems and prospects for the development of cybersecurity in Ukraine in the context of war. The types of threats and possible ways to prevent them in critical conditions are characterized.*
Key words: information, digitalization, cyberattacks, cybercrime, Russian aggression, critical infrastructure.

Розпочинаючи дослідження потрібно констатувати, що в Україні протягом останніх десятиріч спостерігається високий рівень діджиталізування різних сфер життя [1, 2, 6, 10]. Ретроспективно аналізуючи проблеми та кіберзагрози для України, її економіки, суб'єктів підприємництва тощо потрібно констатувати, що ще до повномасштабного вторгнення росії критична інфраструктура вже зазнавала масштабних кібератак (найбільше напередодні – січень-лютий 2022р.). А вже під час загарбницької війни, коли восени 2022 р. російські ракетні удари по українській енергосистемі викликали проблеми у роботі критичної інфраструктури. Через це, можливо, саме питання кібербезпеки відійшло дещо на другий план [6]. Тобто, ще задовго до повномасштабного вторгнення росія суттєво посилила кібератаки на українські держоргани, оборонно-промисловий комплекс, інфраструктурні об'єкти, ІТ-мережі, ЗМІ тощо [7]. Зрозуміло, що вітчизняний бізнес перебував під серйозною загрозою кібератак вже від початку отримання незалежності. Просто із повномасштабним російським вторгненням кібератаки набувають все значніших масштабів. Через це кожен вітчизняний суб'єкт підприємництва має свідомо, систематично оцінювати рівень своєї вразливості (діяльності, персоналу тощо) щодо інцидентів кібербезпеки, технологічних збоїв. Вказані загрози можуть виникати як через кібератаки на системи, інфраструктуру тощо, так і можуть бути наслідками безпосередніх військових дій [7]. На основі огляду літературних джерел можна констатувати, що сутність поняття «кіберзагроза» полягає у «протиправних карних діях суб'єктів інформаційних правовідносин (і, як показує дослідження, не тільки їх), які створюють небезпеку життєво важливим інтересам людини, суспільства, держави, реалізування яких залежить від належного функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, та відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації» [1, с. 99].

Кібератаки є одним із найнебезпечніших ризиків для бізнесу. Їх кількість постійно зростає (McKinsey спрогнозував, що до 2025 р. кіберзлочини щорічно спричинятимуть збитки на 10,5 трлн. дол. США, що втричі перевищуватиме величину 2015 р. [1].

Проаналізуємо наймасштабніші глобальні кібератаки цього десятиріччя (табл. 1) та оцінимо їх фінансові наслідки [1, 7].

Найцікавіше, що ключові фактори (табл. 1) про гучні кібератаки були систематизовані ПрАТ «Київстар» у вересні 2023 року, а вже 12 грудня 2023 року саме дана компанія зазнала наймасштабнішої з кібератак в Україні [1]. Через 10 днів було повністю відновлено телекомуеікаційну інфраструктуру підприємства.

Таблиця 1

Загальна характеристика основних глобальних кібератак протягом 2010-2023 рр.

Назви/об'єкти атак	Описи	Роки	Наслідки
Масштабний витік даних, Yahoo	Витік даних мінімум із 3 млрд акаунтів (викрадення особистих даних)	2013-2014	Втрата ринкової капіталізації – 1,3 млрд. дол. США, Yahoo виплатила 85 млн дол. США для врегулювання позовів, отримання штрафу у 35 млн дол. США за введення громадськості в оману щодо кіберпорушень
Найпотужніша DDoS-атака, GitHub	Лавиноподібне збільшення трафіку за допомогою технології кешування даних	2018	GitHub був недоступний всього 10 хвилин, дані користувачів не постраждали завдяки навяності потужних інструментів протидії DDoS-атакам
Удар по репутації, Marriott International	Злам бази даних бронювання (383 млн записів клієнтів)	2018	Мережа Marriott отримала колективні судові позови, штраф у майже 24 млн дол. США і витрати на заміну паспортів клієнтів, які стали жертвами витоку даних
Кількатижневий збій системи, Sony PlayStation Network	Злам онлайн-сервісів і отримання доступу до даних 77 млн акаунтів	2011	Вартість збою, як наслідок, припинення роботи сервісів оцінили у 171 млн дол. США. Для постраждалих клієнтів надали доступ до контенту PlayStation, 30 безкоштовних днів підписки на PlayStation Plus
Найбільший злом в історії криптовалют, Mt.Gox	Зловмисники вивели з біржі 650 000 BTC	2011-2013	Збитки становили близько 440 млн. дол. США. У 2014 р. Mt.Gox оголосила своє закриття
Найдорожча кібератака в історії, NotPetya	Блокування доступу до жорстких дисків, зупинка роботи окремих комп'ютерів, мереж, паралізуючи роботу сотень компаній	2016-2017	Глобальний збиток від атаки приблизно оцінили в 10 млрд. дол. США.
Найбільша хакерська атака на телеком-інфраструктуру, ПрАТ «Київстар»	У 24 млн. абонентів зник мобільний зв'язок та інтернет	2023	ІТ-інфраструктура компанії була частково зруйнована, компанія «Київстар» заявила, що персональні дані абонентів не скомпрометовані

Джерело: систематизовно авторами на основі [1, 7]

Хакери завдають фінансової, репутаційної шкоди (див. табл. 1). Саме тому бізнесу необхідно діяти на випередження, використовуючи дієві управлінські рішення задля посилення рівня власної кібербезпеки [1, 7]. Зокрема, вважаємо, вчасно прийнятим Закон «Про основні засади забезпечення кібербезпеки України» [5]. Ним визначаються правові, організаційні засади щодо забезпечення захисту життєво важливих інтересів людини, суспільства, держави, національних інтересів у кіберпросторі. Законом задекларовано ключові цілі, принципи державної політики саме у кібербезпеці. Важливим також є регламентування координування діяльності із забезпечення кібербезпеки державних органів, підприємств, організацій, громадян [5].

Як висновок, потрібно констатувати, що задля захисту від кібератак підприємства, організації мають розробляти і запроваджувати комплексні заходи безпеки (постійне, регулярне оновлення власного програмного забезпечення, систематичне застосування мережевих, системних заходів захисту, навчання персоналу щодо формування захисту, кібербезпеки, розроблення і реалізування

стратегій, тактик (деталізування їх у правилах) задля реагування на кіберінциденти тощо [3]. На макро рівні ж задля розроблення дієвого механізму для протидії кіберзагрозам Україні доцільно запозичити наявні досвід і практику зарубіжних країн, міжнародної спільноти, адаптувавши їх українським реаліям.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 6 гучних кібератак на бізнес: кейси Yahoo, GitHub і Marriott. URL: https://hub.kyivstar.ua/articles/6-guchnyh-kiberatak-na-biznes-kejsy-yahoo-github-i-marriott
2. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. Науковий вісник НЛТУ України. 2016. Вип. 26.8. С. 327-337.
3. Давиденко Є. Корпоративна безпека на українських підприємствах в умовах війни. Економіка та суспільство. 58. 2023. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3310
4. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. Підприємнцтво, господарство і право. 4. 2017. С. 99-107.
5. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами від 28.07.2022 р. № 2470-IX
6. Зануда А. Атака на Київстар. Які небезпеки вона несе, окрім відсутності зв'язку. 2023. URL: https://www.bbc.com/ukrainian/articles/cglp7kz0rjmo
7. Кириченко А. Кібербезпека в Україні: шляхи розвитку та можливості. Укрінформ. 2023. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html
8. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/ cybersecurity-uncertainty-state.html.
9. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. Економіка та суспільство. 44. 2022. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1790
10. Пешко М., Завербний А. Діджиталізація української економіки в умовах євроінтеграції. Економіка та суспільство. 47. 2023. URL: https://www.economyandsociety.in.ua/index.php/journal/article/view/2136

Двуліт Зоряна Петрівна, доктор економічних наук, професор, професор кафедри зовнішньоекономічної та митної діяльності, Національний університет «Львівська політехніка», Львів, e-mail: zoriana.p.dvulit@lpnu.ua

Dvulit Zoriana P. – doctor of economics, Professor, Head of the Department of Foreign Trade and Customs, Lviv Polytechnic National University, Lviv, e-mail: zoriana.p.dvulit@lpnu.ua

Завербний Сергій Андрійович, студент кафедри систем автоматизованого проектування, Національний університет «Львівська політехніка», Львів, e-mail: serhii.zaverbnyi.mnknm.2023@lpnu.ua

Zaverbnyi Serhii A. – student of the Department of Automated Control Systems, Lviv Polytechnic National University, Lviv, e-mail: serhii.zaverbnyi.mnknm.2023@lpnu.ua

Гладун Мар'ян Тарасович, студент кафедри захисту інформації, Національний університет «Львівська політехніка», Львів, e-mail: marian.hladun.kb.2019@lpnu.ua

Hladun Marian T. – student of the Department of Information Security, Lviv Polytechnic National University, Lviv, e-mail: marian.hladun.kb.2019@lpnu.ua