УДК 330.341

С.Д. Лучик, В.Є. Лучик[1]

ЦИФРОВА ТА КІБЕРБЕЗПЕКА УКРАЇНСЬКОГО БІЗНЕСУ В УМОВАХ ВІЙНИ

[1]Харківський національний університет внутрішніх справ

Анотація: *У статті досліджено стан цифрової та кібербезпеки українського бізнесу в умовах війни та запропоновано заходи, покликані сприяти підвищенню ефективності кіберзахисту комп'ютерних систем і мереж компаній та цифрової безпеки персоналу.*

Ключові слова: *кібербезпека, цифрова безпека, кіберінцидент, кібератака, кіберзагроза, кіберзахист*

Abstract: *The article analyzes the state of digital and cybersecurity of Ukrainian business in the context of war and proposes measures aimed at improving the effectiveness of cybersecurity of computer systems and networks of companies and digital security of personnel.*

Keywords: *cybersecurity, digital security, cyber incident, cyber attack, cyber threat, cyber defense*

Невід'ємною частиною повномасштабної війни Росії проти України є кібервійна. Під час активної фази війни в Україні з січня 2022 року до кінця серпня 2023 року загалом трапилося 11 922 кіберінциденти за різними тактиками, цільовими секторами та техніками. Це свідчить про високий рівень кіберзагроз, що збігаються з фізичним конфліктом. Більшість інцидентів пов'язана зі зловмисним кодом (1320), за ними йдуть збір інформації (843) і вторгнення (802) [1]. Найбільшими об'єктами кібератак були і залишаються урядові організації (578 інцидентів) та IT-сектор (434 інциденти). Ворог намагається зруйнувати критичну інфраструктуру нашої країни. Проте бізнес, який сьогодні активно використовує інформаційні та цифрові технології, також є мішенню для кібернападів і потребує кіберзахисту. Зокрема, у фінансовому секторі та комерційних організаціях за цей же період мали місце відповідно 243 і 218 кіберінценденти. Кібератаки завдають як фінансової, так і репутаційної шкоди компаніям.

Цифровізація економіки передбачає впровадження цифрових технологій в усі сфери економічної діяльності та повинна супроводжуватися підвищенням рівня довіри і безпеки. Це інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій [2].

Закон України «Про основні засади забезпечення кібербезпеки України» визначає кібербезпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [3]. Завдання кібербезпеки спрямовані на захист комп'ютерних систем і мереж від кібератак, при цьому застосовуються різноманітні методи і заходи – від керування паролями до інструментів комп'ютерної безпеки на основі технологій машинного навчання.

Термін «цифровий» узгоджується з такими виразами, як цифрова економіка, цифрова трансформація та цифрові технології. Фахівці визначають цифрову безпеку як набір передових методів і інструментів, які використовуються для захисту інформації в Інтернеті, даних та інших активів. Ці інструменти включають веб-сервіси, антивірусне програмне забезпечення, SIM-карти смартфонів, біометричні дані та захищені персональні пристрої [4]. Організація економічного співробітництва та розвитку опублікувала звіт «Основи політики ОЕСР у галузі цифрової безпеки: кібербезпека для процвітання» [5, с. 12-13], в якому визначила, що інциденти цифрової безпеки – це події, які порушують доступність, цілісність та/або конфіденційність (тріаду AIC) даних, програмного забезпечення, обладнання та мереж і, як наслідок, негативно впливають на економічну та соціальну діяльність, яка залежить від цих активів.

Цифрова безпека та кібербезпека можуть використовуватися як взаємозамінні терміни, але вони мають дещо різні значення та застосування. Так, згідно рамкової політики ОЕСР щодо цифрової безпеки ризик цифрової безпеки є економічним і соціальним. В свою чергу, економічний і соціальний ризики є результатом технічного ризику. Вони пов'язані, але не однакові. Технічні ризики

обмежуються можливими порушеннями принципів конфіденційності, цілісності, доступності даних та проблемами, пов'язаними з експлуатацією інформаційно-комунікаційних технологій, зокрема, системні збої, простої, неавторизований доступ, втрата цифрових активів тощо. На відміну від цього, економічні та соціальні наслідки таких порушень можуть включати фінансові втрати, втрата можливостей, шкода репутації, крадіжка інтелектуальної власності, шкода конфіденційності та безпеці людини. Отже, технічні ризики є об'єктом кібербезпеки, а економічний та соціальний ризики – цифрової безпеки.

Україна імплементувала в національне законодавство норми європейського законодавства шляхом ухвалення Закону України «Про цифровий контент та цифрові послуги» (2023). При цьому даний закон визначає, що предметом врегульованих операцій є комп'ютерні програми, застосунки, відеофайли, аудіофайли, музичні файли, цифрові ігри та електронні книги.

В Україні складено Перелік категорій кіберінцидентів, розроблений на основі Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України, який відповідає рекомендації Європейської агенції з кібербезпеки (ENISA Reference Incident Classification Taxonomy, січень 2018 року), а також спільному документу ENISA та Європейського центру боротьби з кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network of CSIRTs). Саме кіберінцидент, за результатами дослідження страхової компанії Allianz Risk Barometer (Барометр ризиків Allianz), є головним світовим бізнес-ризиком у 2024 році. Виділяють такі категорії кіберінцинденів як шкідливий (образливий) вміст (Abusive content), шкідливий програмний код (Malicious Code), збір інформації зловмисником (Information Gathering), спроби втручання (Intrusion Attempts), втручання (Intrusion), порушення доступності (Availability), порушення властивостей інформації (Information Content Security), шахрайство (Fraud), відома вразливість (Vulnerable) та Інше (Other) [6]. За даними Державної служби спецзвязку та захисту інформації за 2023 рік українські аналітики безпеки зафіксували та обробили 1105 кіберінцидентів, що на 62,5% більше, ніж у 2022 році. Серед автономних систем, які найчастіше використовувалися для цих атак, були Google, Hurricane, Google-Cloud-Platform, Cloudflarenet та DigitalOcean-ASN [7].

Кіберзагрози бізнес-структурам, як правило, поділяють на внутрішні та зовнішні. Внутрішні кіберзагрози провокує, як правило, діяльність співробітників, які мають справу з конфіденційною інформацією. 25% витоків даних відбуваються через внутрішні загрози. Більшість внутрішніх загроз мотивуються фінансовою вигодою, хоча існують і інші причини для такої поведінки. Для зменшення впливу внутрішніх загроз, фахівці з цифрової та кібербезпеки [8] радять вживати заходи з цифрової безпеки, щоб захистити власні активи та дані клієнтів. Насамперед, забезпечити доступ до баз даних компаній лише тим співробітникам, які потребують його згідно їх посадових обов'язків. Використовувати спеціальне програмне забезпечення для запобігання витоку інформації та моніторингу активності, яке надає кілька рішень для боротьби з ненавмисним розповсюдженням інформації і дозволяє організаціям контролювати свої дані та будь-які пов'язані з ними ризики. Щоразу, коли працівник звільняється з компанії, потрібно вжити належних заходів, щоб якнайшвидше скасувати його доступ до конфіденційних даних. Також відстежувати поведінку працівників, використовуючи аналітику поведінки та машинне навчання, що забезпечить розуміння сукупності загальних дій у відношенні до даних в організації і легше буде відслідкувати незвичні активності.

До найбільш поширених зовнішніх кіберзагроз слід віднести шкідливе програмне забезпечення, DDoS-атаки, фішингові атаки, втрата пристроїв зі збереженими паролями, проникнення у мережу. Найчастіше кіберзлочинці використовували шкідливі програми сімейств SmokeLoader, Agent Tesla, Snake Keylogger, Remcos та Formbook.

2023 рік став ще рекордним роком для програм-вимагачів. Їхня оприлюднена кількість зросла на 49% у порівнянні з 2022 роком. У той самий час, невідомо, скільки існує нерозкритих атак або тих, які з певних причин не розголошуються [9]. Застосунок програм-вимагачів до комп'ютерних систем компаній веде до витоку даних, причому кіберзлочинці обирають компанії з великими обсягами критично важливих даних. Наслідками таких кібератак є не лише витік даних, а й знищення або пошкодження резервних копій даних. Компанії змушені будуть виплатити викуп власникам застосунків-здирників за нерозголошення інциденту та збереження репутації.

До слабких місць цифрової безпеки компаній фахівців відносять також:

досить високу залежність від іноземних виробників програмного забезпечення. В тому числі, з недружніх країн, таких як росія та білорусь;

неналежний контроль за виконанням заходів із забезпечення кіберзахисту та інформаційної безпеки;

вразливість цифрової інфраструктури підприємств через розосередження співробітників — віддалений формат роботи та передача задач на аутсорсінг;

недосконале законодавство у сфері кібербезпеки та повільне переймання відповідного досвіду ЄС та впровадження нормативних актів інших країн [10].

Отже, питання забезпечення цифрової та кібербезпеки для українських компаній є надзвичайно важливими. Російський агресор веде боротьбу як на військовому, так і на цифровому фронті. Кількість кібератак постійно збільшується і вони стають більш витонченими. Це, в свою чергу, вимагає посилювати та удосконалювати захист даних від них. Значну увагу слід приділити побудові ефективної системи кібербезпеки на підприємствах із використанням новітніх технічних та технологічних рішень. Серед передових постачальників рішень для кібербезпеки відзначають такі компанії, як Microsoft, Barracuda, Fortinet, Commvault, Cisco, Palo Alto, CloudFlare, Ciber Future Foundation, Dell Technologies.

Цифрова безпека стосується економічних і соціальних аспектів кібербезпеки. Для зменшення фінансових збитків від кіберінцидентів важливо приділяти увагу навчанню персоналу основам цифрової гігієни та кіберграмотності. Співробітники повинні дотримуватись суворих правил щодо роботи з конфіденційною інформацією, вміти розпізнавати підозрілу активність та володіти інформацію щодо протидії кіберзлочинам.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A Decade in the Trenches of Cyberwarfare: Ukraine’s Story of Resilience. *Kyiv International Cyber Resilience Forum 2024. Resilience at The Cyber War*. URL: https://cyberforumkyiv.org/en/ (дата звернення: 22.02.2024).
2. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 22.02.2024).
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 23.02.2024).
4. What is Digital Security: Overview, Types, and Applications Explained. *Simplilearn*. URL: https://www.simplilearn.com/what-is-digital-security-article (дата звернення: 23.02.2024).
5. OECD Policy Framework on Digital Security. Cybersecurity for Prosperity. OECD Publishing, Paris, 2022. URL: https://doi.org/10.1787/a69df866-en (дата звернення: 24.02.2024).
6. Перелік категорій кіберінцидентів. Державна служба спеціального зв’язку та захисту інформації України. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv (дата звернення: 24.02.2024).
7. Олійник В. Кількість кібератак в Україні зросла на 62% у 2023 році. *AiN*. URL: https://ain.ua/2024/01/12/kilkist-kiberatak-v-ukrayini-zrosla/ (дата звернення: 24.02.2024).
8. Баренков А. ТОП 10 загроз кібербезпеці бізнесу у 2023 році. *BDO Україна*. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023 (дата звернення: 25.02.2024).
9. Кібератаки 2022-2023: огляд найбільших інцидентів, та що нас чекає у 2024 році. H-X. URL: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua (дата звернення: 25.02.2024).
10. Український кіберфронт. *Мінфін*. URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny (дата звернення: 25.02.2024).

Лучик Світлана Дмитрівна, доктор економічних наук, професор, професор кафедри протидії кіберзлочинності, Харківський національний університет внутрішніх справ, Харків, e-mail: luchiksvitlana@gmail.com

Лучик Василь Єфрімович, доктор економічних наук, професор, професор кафедри протидії кіберзлочинності, Харківський національний університет внутрішніх справ, Харків, e-mail: luchik-vasil@gmail.com

Luchyk Svitlana D. – Doctor of economics, Professor, Professor of the Department of Combating Cybercrime, Kharkiv National University of Internal Affairs, Kharkiv, e-mail: luchiksvitlana@gmail.com

Luchyk Vasil E. – Doctor of economics, Professor, Professor of the Department of Combating Cybercrime, Kharkiv National University of Internal Affairs, Kharkiv, e-mail: luchik-vasil@gmail.com