ВПЛИВ КІБЕРАТАК НА ЦИФРОВУ ЕКОНОМІКУ УКРАЇНИ

Синявіна Ю.В., канд. екон. наук, доц.
Проценко Н.М., канд. екон. наук, доц.
Сирий В.М.
Державний біотехнологічний університет

Цифрова трансформація стала одним із основних факторів розвитку сучасного суспільства та бізнесу, оскільки вона включає не лише технологічні зміни, але й суттєві зміни в управлінських підходах, комунікаціях і процесах ухвалення рішень. Інформаційні технології (ІТ) відіграють ключову роль у цьому процесі, дозволяючи автоматизувати робочі процеси, аналізувати великі обсяги даних і впроваджувати інноваційні моделі ведення бізнесу.

Програма цифрової трансформації, запроваджена українським урядом, передбачає інтеграцію цифрових технологій у різні сектори економіки, включаючи електронне урядування, освіту та охорону здоров'я.

Водночас із цим зростають ризики, пов'язані з кібератаками, які стають дедалі частішими та складнішими. Україна, з огляду на постійні кібератаки, особливо у контексті війни та гібридних загроз, постійно стикається з новими викликами в кібербезпеці, що значно впливає на її цифрову економіку. За час повномасштабної війни Україна зазнала більш як 600 кібератак на цифровий простір України – це п'ята частина від усіх кібератак у світі [1].

Кібератаки також можуть мати негативний вплив на економіку країни в цілому, оскільки в кіберпросторі відбувається багато взаємопов'язаних процесів. Крім того, атаки на критично важливу інфраструктуру, будь то банківська чи енергетична, завжди мають прямий негативний вплив на бізнес-процеси [2].

Економічні втрати, спричинені кібератаками, мають глибокий і довготривалий вплив на різні сектори цифрової економіки. Вплив кібератак на цифрову економіку може бути масштабним і серйозно впливати на економічну активність як у короткостроковій, так і в довгостроковій перспективі. Постійні кібератаки змушують компанії вкладати значні кошти в кіберзахист, що підвищує операційні витрати та знижує конкурентоспроможність на міжнародному ринку. Крім того, зростання рівня кібератак може сповільнювати темпи цифровізації в Україні, оскільки компанії та споживачі можуть ставати більш обережними у використанні нових цифрових послуг через загрози для кібербезпеки.

Прямі фінансові втрати є одним із найбільш очевидних і значущих наслідків кібератак. Вони включають усі витрати, які компанії, організації або державні установи змушені понести в результаті кібератак, безпосередньо через порушення їх діяльності, втрату даних або викуп. Основні компоненти прямих фінансових втрат :

- виплати викупу через програми-вимагачі (ransomware), які блокують доступ до критичних даних чи систем і вимагають викупу за їх відновлення;
- втрати доходів через призупинення операцій, бізнес-процесів або збоїв у постачанні послуг;

- штрафи за витік даних, порушення законодавства щодо захисту персональних даних у разі кібератак, які призвели до витоків конфіденційної інформації.

Непрямі економічні втрати від кібератак стосуються довгострокових наслідків, які компанії, державні установи та економіка в цілому зазнають після кібератак. Ці втрати часто не є очевидними на перший погляд, але їхній вплив може бути більш руйнівним у довгостроковій перспективі, ніж прямі фінансові витрати.

Непрямі економічні втрати включають витрати, які організації зазнають внаслідок наслідків атак, а саме:

- втрата репутації та довіри;
- зниження продуктивності та ефективності;
- втрати через скорочення обсягів продажів;
- витрати на підвищення рівня безпеки;
- витрати на юридичні та регуляторні наслідки;
- зниження інвестиційної привабливості;
- вплив на інновації та розвиток.

Одним із найсерйозніших прикладів кібератак, що вплинула на цифрову економіку України, стала атака вірусу NotPetya у 2017 році. Сімейство шкідливих програм Petya (NotPetya) вразило комп'ютери, що працюють на операційній системі Windows. Зараження вірусом відбувалося через фішингове повідомлення (файл Петя.арх) або оновлення програми для бухгалтерської звітності M.E.Doc. Як наслідок, у 2017 році постраждали аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця, а також зараженню піддалися інформаційні системи НБУ, Міністерства інфраструктури, Кабміну, кіберполіції та Служби спецзв'язку України. Вірус паралізував роботу урядових та комерційних організацій, завдавши загальних збитків у розмірі понад 10 мільярдів доларів по всьому світу. Атака призвела до втрати даних, блокування важливих систем та порушення операцій у різних секторах.

На початку 2022 року, перед початком активної фази повномасштабного вторгнення Росії в Україну, було здійснено серію DDoS (Distributed Denial of Service) атак на українські урядові веб-сайти та банківські установи. Кібератаки були спрямовані на міністерства, державні агентства та найбільші банки України, зокрема на ПриватБанк і Ощадбанк. Як наслідки – тимчасове відключення сайтів Міністерства оборони, Міністерства внутрішніх справ та інших державних установ; збій у роботі онлайн-банкінгу, що призвело до тимчасової недоступності банківських сервісів для клієнтів.

Відповідно до звіту Cybersecurity Ventures, очікується, що глобальні збитки, спричинені кіберзлочинною діяльністю зростатимуть на 15% на рік з 2021 до 2025 року та можуть досягти 10,5 трильйонів доларів щорічно [3]. Причинами такого зростання є значний ріст активності груп кіберзлочинців та зловмисників, діяльність яких спонсорується. У той же час кількість атак зростає внаслідок процесів цифрової трансформації.

Незважаючи на певні зусилля, Україна досі не має достатньо комплексної системи захисту від кібератак. Багато державних та приватних організацій не

мають ефективних механізмів для своєчасного виявлення загроз і реагування на них. Це дозволяє зловмисникам безперешкодно здійснювати атаки на вразливі системи.

Багато державних та приватних організацій не мають ефективних механізмів для своєчасного виявлення загроз і реагування на них. Це дозволяє зловмисникам безперешкодно здійснювати атаки на вразливі системи.

Потреба у висококваліфікованих фахівцях з кібербезпеки є однією з головних проблем не тільки в Україні. Багато держав працюють над зменшенням цього дефіциту, а великі компанії, такі як Google, Microsoft або IBM, запроваджують різні ініціативи, спрямовані на навчання та підвищення кваліфікації людей у сфері кібербезпеки. Згідно з дослідженням (ISC)2 Cybersecurity Workforce Study, глобальна нестача кадрів у сфері кібербезпеки становить 3,4 мільйона, при цьому 70% організацій мають незакриті вакансії [4].

Виклики кібербезпеки для цифрової економіки України мають багатоплановий характер, охоплюючи як технічні, так і організаційні аспекти. Зростання складності кібератак, використання застарілої інфраструктури, брак спеціалістів і низький рівень обізнаності користувачів є ключовими проблемами, які потребують системних рішень. Для успішної протидії загрозам Україна має посилити кіберзахист критичних секторів економіки, розвивати кадровий потенціал у сфері кібербезпеки та удосконалювати законодавчу базу, що регулює захист інформаційних систем.

Кібербезпека є одним з найважливіших викликів для розвитку цифрової економіки України. Для ефективного протистояння кіберзагрозам необхідно вживати комплексних заходів, спрямованих на підвищення рівня кібергігієни населення, підготовку кваліфікованих кадрів, модернізацію ІТ-інфраструктури та розробку ефективної державної стратегії кібербезпеки. Лише спільними зусиллями держави, бізнесу та громадянського суспільства можна забезпечити безпеку цифрового простору України.

Інформаційні джерела:

1. Українське національне інформаційне агентство «Укрінформ» URL: https://www.ukrinform.ua/rubric-society/3901744-ukraina-pid-cas-povnomasstabnoi-vijni-zaznala-bils-ak-600-kiberatak.html

2. Стендер, С. В., Фротер, О. С., & Снітко, Ю. М. (2023). Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. *Академічні візії*, (26). URL: https://academy-vision.org/index.php/av/article/view/799

3. Cybersecurity Ventures. URL: https://cybersecurityventures.com/

4. Офіційний сайт УНІАН (Українське Незалежне Інформаційне Агентство Новин). URL: https://www.unian.ua/science/10-viklikiv-kiberbezpeki-eksperti-rozpovili-do-chogo-gotuvatisya-koristuvacham-ta-kompaniyam-12033828.html#goog_rewarded