УДК 338.245
JEL classification: O33
https://doi.org/10.31891/dsim-2024-8(53)

КІБЕРБЕЗПЕКА БІЗНЕСУ В ПЕРІОД ПІСЛЯВОЄННОГО ВІДНОВЛЕННЯ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

ТРУБНІКОВ Артем
аспірант факультету менеджменту та маркетингу,
Національний технічний університет України Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0009-0003-6278-0794

Кібербезпека є критично важливою складовою післявоєнного відновлення українського бізнесу. Ця стаття аналізує основні кіберзагрози, з якими стикається український бізнес після війни, а також окреслює можливі рішення та перспективи розвитку кібербезпеки у країні.

Для забезпечення захисту компанії мають інвестувати у технічні, організаційні та кадрові заходи. Співпраця держави, приватного сектору та міжнародних партнерів сприятиме ефективному захисту від кіберзагроз. Післявоєнне відновлення України передбачає не лише фізичну реконструкцію інфраструктури, а й посилення захисту цифрового простору, особливо для бізнесу. Сучасні компанії значною мірою залежать від технологій, що робить їх потенційною мішенню для кібератак. В умовах гібридної війни кіберзагрози стали частиною економічної безпеки, а тому питання кіберзахисту бізнесу є пріоритетним.

Ключові слова: кібербезпека бізнесу, період післявоєнного відновлення, виклики, перспективи.

BUSINESS CYBERSECURITY IN THE POST-WAR RECOVERY PERIOD: CHALLENGES AND PROSPECTS

TRUBNIKOV Artem
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Cybersecurity is a critical component of the post-war recovery of Ukrainian business. This analysis article presents the main cyber threats that Ukrainian businesses face after the war and outlines possible solutions and prospects for the development of cybersecurity in the country.

As Ukraine rebuilds its infrastructure and economy, the protection of its digital space must be prioritized. In the modern world, businesses rely heavily on technology, making them increasingly vulnerable to cyberattacks. With the ongoing hybrid war, cyber threats have become an integral aspect of economic security. As a result, ensuring the cyber defense of businesses has become a key priority in the country's post-war recovery efforts.

The main cyber threats Ukrainian businesses face post-war are diverse and complex. One of the most significant threats is state-sponsored cyberattacks, which can involve cyber espionage, sabotage, and the disruption of critical infrastructure. These attacks are often part of hybrid warfare strategies designed to destabilize the country's economy and security. Another major threat is ransomware, which has grown increasingly common and dangerous. These attacks often paralyze business operations and demand ransoms in exchange for restoring access to critical data.

Phishing attacks and social engineering tactics are also a serious concern. With many businesses in recovery mode, employees may be less vigilant, making it easier for cybercriminals to exploit human error. Additionally, as businesses re-establish their supply chains, there is a heightened risk of supply chain attacks. Cybercriminals often target third-party suppliers, knowing that a single vulnerability in the supply chain can compromise entire networks.

To ensure the protection of businesses, it is essential for companies to invest in a combination of technical, organizational, and human resources. Investing in state-of-the-art cybersecurity tools, such as firewalls, encryption, and intrusion detection systems, will significantly strengthen the digital infrastructure. However, it is not enough to simply invest in technology; companies must also ensure that their employees are trained in cybersecurity best practices. Ongoing education and awareness programs will reduce the risk of human error, such as falling victim to phishing attempts or other social engineering tactics.

Collaboration between the state, the private sector, and international partners is crucial to tackling these cyber threats effectively. The government can play a vital role by providing guidance, sharing threat intelligence, and offering financial support to businesses to strengthen their cybersecurity defenses. In addition, partnerships with international cybersecurity organizations will allow Ukraine to access global expertise, tools, and resources, further enhancing its resilience to cyber threats.

A national cybersecurity framework is also necessary to guide businesses in managing their cyber risks. By aligning with international standards such as NIST or ISO 27001, Ukraine can ensure that its businesses are adopting the best cybersecurity practices and maintaining compliance with global security norms. This framework can also help establish a common language for identifying and addressing cyber threats, making it easier for businesses to communicate and collaborate with each other and the government.

Finally, businesses should prioritize disaster recovery and business continuity planning. This includes regularly backing up critical data, implementing failover systems, and ensuring that recovery processes are in place and tested regularly. Cybersecurity insurance is another option businesses might explore to mitigate the financial impact of cyberattacks.

The prospects for the development of cybersecurity in Ukraine are promising. By investing in the cybersecurity sector and fostering public-private partnerships, Ukraine can position itself as a regional leader in digital security. The country's recovery from war presents an opportunity to not only rebuild physical infrastructure but to also create a more secure and resilient

digital economy. Strengthening cybersecurity will not only protect Ukrainian businesses but will also attract international investment, as companies will be more likely to do business in a country with robust cyber defenses.

In conclusion, cybersecurity is no longer a luxury but a necessity for Ukrainian businesses in the post-war period. By addressing cyber threats head-on and fostering collaboration between all sectors, Ukraine can build a strong and secure digital future, supporting its economic recovery and development.

***Keywords**: business cybersecurity, post-war recovery period, challenges, prospects.*

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Останніми роками відбулися дві великі події, які глибоко вплинули на ландшафт кіберзагроз і потреби в зусиллях з кібербезпеки. Першою з цих двох подій стала криза COVID-19. Більш ніж рік часткового або повного локдауну населення наклав сильний відбиток на людей і структури на глобальному рівні. Оскільки населення світу постійно входило в локдауни і виходило з них, економіка зазнавала краху, системи охорони здоров'я були перевантажені, школи та університети закривали свої класи, міжнародні подорожі впали до рівня, небаченого в наш час. Проте не всі сектори зіткнулися з однаковою боротьбою. У міру того, як комунікаційні технології з'являлися як панацея для пом'якшення наслідків вимушеного соціального дистанціювання, принаймні один сектор світової економіки скористався пандемією – кіберзлочинність. Другою з цих двох подій є нинішня російсько-українська війна, яка поєднує в собі як звичайний, так і кібервоєнний компонент, і з цим кібервиміром війни надає надзвичайно цікаві уявлення про те, як може виглядати сучасна війна в майбутньому, де технології стають переважаючими, особливо в економічній діяльності.

Повномасштабне вторгнення Росії в Україну не тільки завдало колосальної шкоди фізичній інфраструктурі та економіці країни, але й суттєво актуалізувало питання кібербезпеки для українського бізнесу. В умовах воєнного стану та післявоєнного відновлення, кіберзагрози набувають нових форм та масштабів, що робить дослідження цієї теми особливо важливим та своєчасним.

Війна в Україні призвела до активізації кіберзлочинців, спрямованих на українські підприємства. Збільшилася кількість DDoS-атак, фішингових кампаній, атак з використанням програм-вимагачів та інших видів кіберзлочинів. Післявоєнне відновлення, ймовірно, супроводжуватиметься подальшим зростанням кіберзагроз, оскільки бізнес буде активно впроваджувати цифрові технології, що розширює поле для кібератак.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Серед дослідників, котрі займалися аналізом у сфері кібербезпеки бізнесу в Україні, особливо в контексті післявоєнного відновлення, працюють кілька провідних дослідників та експертів. Серед них: Сироватченко М. [1], Жарикова А. [2], Кузьменко, О., Маклюк, О., & Чернишова О. [3], Berdar, Marharyta M.; Yaremko-Hladun, Roman A. [4]. Ці фахівці роблять значний внесок у дослідження та розвиток кібербезпеки українського бізнесу в умовах післявоєнного відновлення.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

В ультраглобалізованому та не державоцентричному контексті передкризових стратегій реагування на кіберзагрози буде недостатньо для відповіді новій реальності. Для того, щоб оптимально реагувати на ці загрози, службам громадської безпеки доведеться розгортати нові форми інтегрованих стратегій кібербезпеки, розслідувань та реагування правоохоронних органів, як для видимих, очевидних компонентів національної безпеки (поліція, підрозділи по боротьбі з шахрайством), так і для менш помітних компонентів (контррозвідка). Крім того, реагування у сфері безпеки потребуватиме більшої координації різних компонентів континууму національної безпеки. Таким чином, посткризова реальність змусить політичних лідерів переосмислити структури спецслужб і заходи реагування, щоб протистояти безперервній і прискореній еволюції кіберзагроз.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є аналіз основних кіберзагроз, з якими стикається український бізнес після війни, а також окреслення можливих рішень та перспектив розвитку кібербезпеки у країні.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Кіберзагрози не є чимось новим. Люди з недоброзичливими намірами не очікували кризи COVID-19, щоб побачити потенціал, який цифрові простори представляють для злочинної діяльності [6]. Кіберзагрози вже існували до кризи COVID-19, починаючи від кіберзлочинності до ворожих дій, спричинених (або підозрюваними в тому, що їх створюють) іноземні суб'єкти – те, що зараз часто називають кібервійною. Проте, як і в багатьох речах, пандемія COVID-19 загострила та прискорила основні технологічні зміни в суспільстві, які були засвідчені протягом кількох десятиліть. Цікаво, що корпоративний сектор надзвичайно швидко прийняв цю нову реальність, підштовхнуту необхідністю продовжувати бізнес-діяльність, незважаючи на

кризовий контекст. Проте обізнаність про загрози кібербезпеки в більшості випадків залишалася низькою [8]. Вимушене соціальне дистанціювання населення призвело до значного збільшення доступу до цифрових просторів і додатків, а отже, підвищило вразливість до кіберзагроз. Не дивно, що однією з галузей економіки, яка найшвидше скористалася пандемією та адаптувалася, став сектор злочинності. Дійсно, збільшення кримінальних можливостей призвело до зростання кіберзлочинності через те, що існуючі кіберзлочинці стають більш продуктивними, до все більш звичайних (тобто спочатку не заснованих на Інтернеті) злочинців, які інвестують у кіберпростір, або до комбінації цих двох факторів. Водночас масова міграція повсякденних дій у цифровий простір також призвела до підвищення обізнаності користувачів про кібербезпеку, що призвело до прискорення еволюції методів кіберзлочинності. Безтілесність злочину, а особливо делокалізація злочинців, які вже не перебувають у безпосередньому фізичному контакті зі своєю жертвою, призводить до зниження відсотка розкриття злочинів, а отже, і до сприйняття співвідношення витрат і вигод для підвищення кваліфікації злочинців.

Кібернетичні атаки на об'єкти критичної інфраструктури, такі як енергетичні компанії, транспортні системи та фінансові установи, можуть мати катастрофічні наслідки для економіки країни та національної безпеки. Забезпечення кібербезпеки критичної інфраструктури є першочерговим завданням в умовах післявоєнного відновлення.

Коли йдеться про кіберзагрози, цифрові простори потрібно розуміти – і підходити до них – пам'ятаючи про їхню подвійну природу. Справді, кіберпростір в Інтернеті є одночасно і вектором, і набором інструментів для доступу до злочину, і місцем, де може відбутися злочин. Російсько-українська війна, яка розпочалася на початку 2022 року, також проливає нове світло на потенційні цілі майбутньої кібервійни. Дійсно, і хоча військові та урядові установи, очевидно, стали серйозними мішенями з обох сторін у кіберпросторі, цікаво зазначити, що кібератаки є значно більш дифузними та різноманітними, і націлені на численні корпоративні структури, окрім військових цілей. Посткризові кіберзагрози будуть наслідком збільшення масштабів використання громадянами цифрового простору, а також ускладнення загроз, як з точки зору технічної складності, так і з точки зору різноманітності цілей.

За понад два з половиною роки від початку широкомасштабного вторгнення Росії в Україну очевидно, що український бізнес вистояв навалі. На другий день після початку обстрілів на забитих дошками вікнах багатьох приміщень з'явилися таблички «Відкрито для бізнесу». Під час блекаутів у маленькій кав'ярні на першому поверсі мого багатоповерхового будинку вмикають генератор і подають каву для тих, хто поспішає на роботу. Така стійкість українського бізнесу є стратегічно важливою з кількох причин. По-перше, коли я бачу своїх сусідів, які стоять у черзі за кавою по дорозі на роботу, це свідчить про те, що у них є робота, а це означає, що вони роблять свій внесок у ВВП України, наповнюють державну скарбницю та підтримують попит. По-друге, можливість гідного працевлаштування в Україні є вирішальним фактором у поверненні біженців з-за кордону, що підтверджують дослідження Центру економічної стратегії. По-третє, бізнес вже відіграє ключову роль у зусиллях з відбудови України, ще до завершення бойових дій.

Тому моніторинг здоров'я українського бізнесу є важливим, зокрема, для своєчасного виявлення проблем та надання відповідної підтримки. Кілька постачальників даних регулярно вимірюють температуру українського бізнесу: Національний банк України (НБУ), Інститут економічних досліджень та політичних консультацій (IER) та Advanter Group, яка працює у співпраці з Центром розвитку інновацій, Офісом з розвитку підприємництва та експорту та національним проєктом Дія.Бізнес. Кожна з цих організацій регулярно проводить опитування кількох сотень компаній. Однак, коли йдеться про отримання загального уявлення про стан та перспективи українського бізнесу, між даними з цих джерел є суттєві відмінності. Наприклад, відповіді на запитання про поточну ситуацію компаній розкривають різні перспективи. У дослідженні II кварталу 2024 року 18,3% підприємств охарактеризували своє становище як «незадовільне». На противагу цьому, опитування IER у серпні 2024 року показало нижчий показник – 16,1 відсотка, тоді як опитування Advanter [9], того ж місяця мало вищий показник – 22,5 відсотка. Що стосується чистої оцінки становища компаній, яка розраховується як різниця між тими, хто відповів «добре» і тих, хто відповів «погано», то диспропорція була ще більш разючою: в опитуваннях НБУ оцінки були в цілому негативними, .

Після війни українські підприємства опиняться перед низкою нових загроз у цифровій сфері. Вразливість бізнесу вже посилилася через перебої у роботі IT-інфраструктури, нестачу кадрів та обмежені фінансові ресурси. Українські компанії стикаються з такими видами атак:

Рис. 1. Основні типи кіберзагроз для бізнесу

Джерело: розроблено автором

Основними факторами, що ускладнюють захист бізнесу є:

1. Кадровий дефіцит. Велика кількість IT-фахівців виїхала за кордон або працює на міжнародні компанії.
2. Обмеженість ресурсів. Малий та середній бізнес часто не має можливості інвестувати в дорогі системи кіберзахисту.
3. Адаптація атак до нових реалій. Хакери використовують соціальну інженерію та воєнні наративи для маніпуляцій.
4. Відсутність комплексного підходу. Багато підприємств недостатньо приділяють увагу кібербезпеці.

Що стосується очікувань компаній щодо свого майбутнього, то різниця була ще більш разючою. Згідно з опитуванням НБУ [10], частки тих, хто вважав, що їхні перспективи погіршаться, і тих, хто вважав, що вони покращаться, були майже однаковими – близько 14%. Одне з можливих пояснень полягає в тому, що існує значна різниця у структурах вибірки, які використовуються цими організаціями у своїх опитуваннях. Незважаючи на те, що в усіх опитуваннях проводиться опитування керівників підприємств, компанії у вибірках різняться за розміром. Наприклад, НБУ будує свою вибірку таким чином, щоб однаково представляти малі, середні та великі компанії. Такий підхід дає можливість оцінити стан кожної групи окремо, але загальні результати не відображають стан українського бізнесу в цілому. Це пов'язано з тим, що, за даними Державної служби статистики України, з усіх українських компаній 94% є малими, 6% – середніми і лише 0,2% – великими. У той же час малі підприємства генерують лише 19 відсотків всього товарообігу і забезпечують роботою 27 відсотків робочої сили. Великі компанії, незважаючи на свою невелику кількість, виробляють 36 відсотків товарообігу і становлять 25 відсотків працівників.

За даними Державної служби статистики України, найбільше з початку вторгнення постраждав малий бізнес. З 2021 по 2022 рік кількість великих компаній скоротилася на 19 відсотків, середніх – на 16 відсотків, а малих – на 30 відсотків. Таким чином, аналізуючи дані різних провайдерів, варто порівнювати дані Advanter, де у вибірковій структурі переважають невеликі компанії, з підвибіркою малого бізнесу НБУ. Однак певні упередження залишаються навіть після того, як вибірки були дезагреговані таким чином. Наприклад, респонденти НБУ налаштовані більш песимістично, ніж респонденти, опитані іншими провайдерами. Незважаючи на відмінності, в даних також є багато спільного. Наприклад, опитування НБУ та ІЕД чітко показують, що респонденти у великому бізнесі почуваються набагато краще, ніж у малому та середньому. Мало того, працівники невеликих компаній також частіше очікують погіршення ситуації.

У проблемах, з якими стикається бізнес, також є багато спільного. До трійки головних викликів НБУ відносить нестачу кваліфікованих працівників, недостатній попит та високі ціни на сировину та енергоносії. Великі компанії значно більше страждають від нестачі кадрів, ніж малі та середні, тоді як з іншими проблемами однаково стикаються фірми будь-якого розміру. Нестача робочої сили також входить до трійки основних проблем, на які посилаються Advanter та IER. Тому можна представити заходи захисту бізнесу що можуть бути включено в стратегію кібербезпеки бізнесу в період післявоєнного відновлення Україні (рис.2).

З посиленням цифрової трансформації бізнесу зростає обсяг персональних даних, які обробляються підприємствами. Забезпечення захисту цих даних від кіберзлочинців є не тільки питанням довіри клієнтів, але й вимогою законодавства.

Війна та її наслідки значно підвищили рівень усвідомлення важливості кібербезпеки серед керівників підприємств та працівників. Кіберзагрози стали реальною та відчутною проблемою, що мотивує бізнес інвестувати в кіберзахист та приділяти більше уваги питанням кібергігієни.

Післявоєнне відновлення України потребуватиме значних інвестицій, у тому числі в сферу кібербезпеки. Міжнародні організації та країни-партнери можуть надати фінансову та технічну допомогу для розвитку кібербезпеки українського бізнесу, що сприятиме його модернізації та інтеграції у світовий економічний простір.

Рис. 2. Схема стратегічних підходів до захисту бізнесу в Україні

Джерело: розроблено автором

Разом з тим, скласти послідовну картину викликів, що стоять перед бізнесом, непросто через неузгодженість у списках можливих проблем, з яких респондентам було запропоновано обирати. Наприклад, НБУ та ІЕД більше зосереджуються на суто економічних питаннях, таких як вартість сировини та зниження попиту. Водночас, такі проблеми, як, по-перше, непередбачуваний розвиток подій в Україні та на зовнішніх ринках через війну та, по-друге, непередбачувані дії держави і нестача персоналу незмінно входять до трійки головних проблем компаній з листопада 2023 року. Ці ризики можна значно пом'якшити, якщо уряд оприлюднить чітку стратегію та налагодить діалог з бізнесом. Економіка України також потребує плану перемоги: чітка вказівка на наміри уряду зменшила б невизначеність та покращила настрої серед бізнес-лідерів. Рік тому коаліція українського бізнесу оприлюднила меморандум, в якому назвала відсутність такої стратегії червоною лінією для економіки України. Залучення українського бізнесу до формування економічних політик також є критично важливим для підприємців. Компанії України готові брати участь у

розробці майбутніх стратегій та політик країни. Для ефективного розвитку кіберзахисту потрібні значні інвестиції, зокрема: розширення програм підготовки IT-спеціалістів з кібербезпеки, розвиток інноваційних технологій у сфері кіберзахисту, зокрема ШІ та блокчейн-рішень, впровадження кіберстрахування, що дозволить компенсувати втрати бізнесу від атак.

За останні вісім років ринок кібербезпеки в Україні збільшився в чотири рази. Станом на 2024 році український ринок оцінюється в $138 мільйонів [11]. **Кіберзагрози продовжують еволюціонувати як у світі, так і в Україні, демонструючи з**ростання кількості та складності атак. Різке зростання кількості атак. Ці тенденції підкреслюють важливість постійного вдосконалення заходів кібербезпеки як на глобальному рівні, так і в Україні, а також необхідність підвищення обізнаності про кіберзагрози серед організацій та населення. У 2023 році зафіксовано 1105 кіберінцидентів, що на 62,5% більше, ніж роком раніше. **Державні установи знаходяться в зоні ризику.** У 2022 році українські інформаційні ресурси зазнали понад 7000 атак, що втричі перевищує показник 2021 року [11].

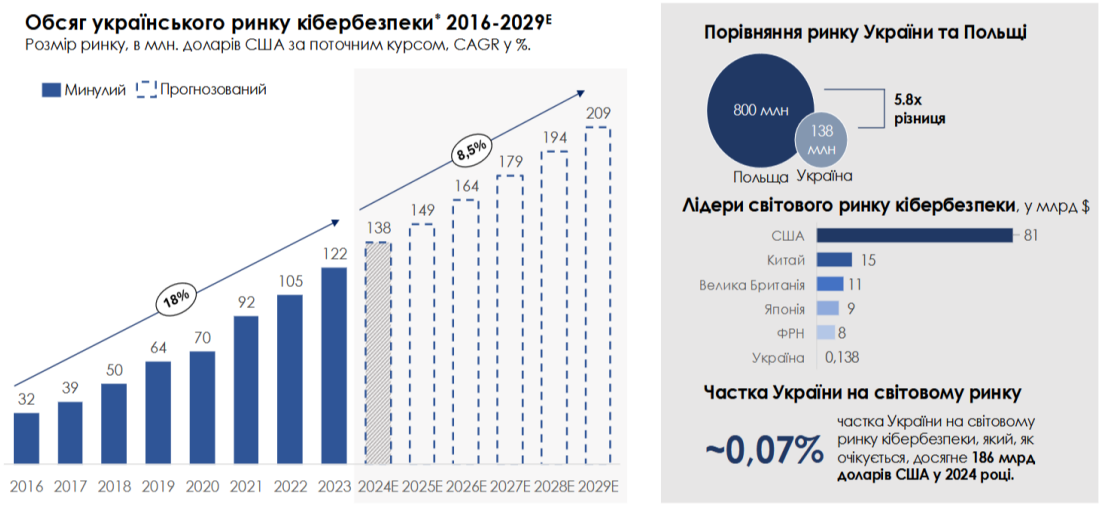

Рис. 3. Обсяг українського ринку кібербезпеки за 2016-прогноз 2029 роки

Джерело: [11]

Хакери найчастіше використовують фішингові листи, впроваджують шкідливі програми та експлуатують слабкі місця в програмному забезпеченні. З огляду на такі тенденції, посилення заходів кібербезпеки стає критично важливим не лише для компаній, а й для держави в цілому. Найбільші споживачі послуг кібербезпеки — це фінанси, телекомунікації, енергетика та промисловість. Особливості кібербезпеки для кожної з цих галузей охоплюють захист даних, мережевої інфраструктури та критичних систем.

Важливим позитивним моментом є формування культури кібербезпеки в українському суспільстві. Підвищення рівня обізнаності громадян та працівників щодо кіберзагроз та правил кібергігієни сприятиме зменшенню кількості кіберінцидентів та зміцненню кіберстійкості бізнесу.

Розвиток кібербезпеки бізнесу в період післявоєнного відновлення є складним та багатогранним процесом, який супроводжується як викликами, так і можливостями. Проте, враховуючи позитивні моменти, які були описані вище, можна з упевненістю стверджувати, що Україна має значний потенціал для створення сучасної та ефективної системи кібербезпеки, яка буде надійно захищати інтереси бізнесу та сприяти його успішному розвитку. Успішне вирішення цього завдання сприятиме зміцненню економіки країни, підвищенню її конкурентоспроможності та забезпеченню національної безпеки.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Післявоєнне відновлення України неможливе без забезпечення кібербезпеки бізнесу. Враховуючи зростаючі загрози, підприємствам необхідно інвестувати у технічний захист, навчання персоналу та адаптацію до нових викликів. Співпраця бізнесу, держави та міжнародних партнерів дозволить створити ефективну систему кібербезпеки, що забезпечить стійкість української економіки в умовах цифровізації та глобальних кіберзагроз.

Хоча і наголошується на економічному вимірі кібербезпеки, важливо пам'ятати, що головне завдання поліцейських служб полягає в забезпеченні безпеки громадян, а не в захисті інтересів приватних корпорацій – навіть якщо вони можуть у певний момент перетинатися з інтересами національної безпеки. Це принципова відмінність між поліцією, з одного боку, яка фокусується на «мікро» рівні (безпека громадян), і контррозвідкою та приватними службами корпоративної безпеки з іншого, які зосереджуються на «макро» інтересах (економічна безпека компаній або нації). Ці відмінності в підходах є серйозними, і одним із ризиків глобалізації ризиків є втрата «мікро» фокусу, тобто безпеки людей. Якщо громадяни відчувають себе покинутими чиновниками, то управління та політика національної безпеки можуть швидко опинитися під

питанням населення, що може призвести до наслідків для соціального миру та суспільної рівноваги. Хоча кіберзагрози є реальними, соціальна прийнятність дій силовиків є центральним параметром, який не можна ігнорувати. Готовність посідає центральне місце в дискурсах антикризового менеджменту багатьох країн. Однак нещодавні події чітко продемонстрували, що ми все ще не повністю готові впоратися з деякими наслідками великих криз на глобальному рівні. Кібербезпека є прекрасним прикладом цього, але саме їй могла б протистояти оптимальна реакція національних служб безпеки.

Література

1. Syrovatchenko M. (2024). Legal aspects of cybersecurity in Ukraine: current challenges and the role of national legislation. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences*, 11(1), 314-320. https://doi.org/10.23939/law2024.41.314
2. Жарикова А. (2024). Кількість кібератак у 2023 році зросла на 16 % – Держспецзв'язку. *Економічна правда*. Retrieved from https://www.epravda.com.ua/news/2024/01/31/709355
3. Кузьменко О., Маклюк О., & Чернишова О. (2022). Кібебезпека бізнесу під час війни. *Економіка та суспільство*, (44). https://doi.org/10.32782/2524-0072/2022-44-21
4. Berdar M. M., & Yaremko-Hladun R. A. (2024). Innovation and Investment Model for the Development of Small and Medium-Sized Businesses in Ukraine. *Theoretical and Practical Research in Economic Fields*, 15(2), 174-185. https://doi.org/10.14505/tpref.v15.2(30).02
5. Закон України "Про кібербезпеку" № 2163-VIII.
6. ENISA. (2024). Cybersecurity Threat Landscape 2024.
7. ISO/IEC 27001:2023 – міжнародний стандарт інформаційної безпеки.
8. CERT-UA. (2024). Аналітичний звіт про кіберзагрози в Україні.
9. NIST. (2024). Cybersecurity Framework.
10. Dligach A., & Stavytskyy A. (2024). Resilience Factors of Ukrainian Micro, Small, and Medium-Sized Business. *Economies*, 12(12), 319. https://doi.org/10.3390/economies12120319
11. *Dou.ua*. (2024). Ukraine Cybersecurity Market Review. Retrieved from https://dou.ua/lenta/news/ukraine-cybersecurity-market-review/

References

1. Syrovatchenko, M. (2024). Legal aspects of cybersecurity in Ukraine: current challenges and the role of national legislation. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences*, 11(1), 314-320. https://doi.org/10.23939/law2024.41.314
2. Zharykova, A. (2024). Kilkist kiberatak u 2023 rotsi zrosla na 16 % – Derzhspetszviazku. *Ekonomichna pravda*. Retrieved from https://www.epravda.com.ua/news/2024/01/31/709355
3. Kuzmenko, O., Makliuk, O., & Chernyshova, O. (2022). Kiberbezpeka biznesu pid chas viyny. *Ekonomika ta suspilstvo*, 44. https://doi.org/10.32782/2524-0072/2022-44-21
4. Berdar, M. M., & Yaremko-Hladun, R. A. (2024). Innovation and Investment Model for the Development of Small and Medium-Sized Businesses in Ukraine. *Theoretical and Practical Research in Economic Fields*, 15(2), 174-185. https://doi.org/10.14505/tpref.v15.2(30).02
5. Закон України "Про кібербезпеку" № 2163-VIII.
6. ENISA. (2024). Cybersecurity Threat Landscape 2024.
7. ISO/IEC 27001:2023 – mizhnarodnyi standart informatsiinoi bezpeky
8. CERT-UA. Analitychnyi zvit pro kiberzahrozy v Ukraini
9. NIST. (2024). Cybersecurity Framework.
10. Dligach, A., & Stavytskyy, A. (2024). Resilience Factors of Ukrainian Micro, Small, and Medium-Sized Business. *Economies*, 12(12), 319. https://doi.org/10.3390/economies12120319
11. *Dou.ua*. (2024). Ukraine Cybersecurity Market Review. Retrieved from https://dou.ua/lenta/news/ukraine-cybersecurity-market-review/