ОСОБЛИВОСТІ КІБЕРБЕЗПЕКИ БІЗНЕСУ В УМОВАХ ВОЄННОГО ЧАСУ
FEATURES OF BUSINESS CYBER SECURITY IN WARTIME CONDITIONS

УДК 336.658
DOI: https://doi.org/10.32782/dees.12-22

Шостак Л.В.[1]
к.е.н., доцент,
доцент кафедри економіки і торгівлі,
Волинський національний університет
імені Лесі Українки
Федонюк А.А.[2]
к.ф.-м.н., доцент,
доцент кафедри загальної математики
та методики навчання інформатики,
Волинський національний університет
імені Лесі Українки
Помазун О.О.[3]
асистент кафедри
інформаційних технологій та туризму,
Луцький інститут розвитку людини
Університету "Україна"

Shostak Liudmyla
Lesya Ukrainka Volyn National University
Fedoniuk Anatolii
Lesya Ukrainka Volyn National University
Pomazun Olena
Lutsk Institute of Human Development
of the University "Ukraine"

Дана стаття присвячена дослідженню проблеми кібербезпеки бізнесу в умовах воєнних дій в Україні є надзвичайно актуальним і критично важливим на сьогоднішній день. Автори зазначають, що Україна стала ареною активних кібератак з боку супротивників, які спрямовані на різні сектори її економіки та критичну інфраструктуру. Ці атаки можуть мати різні мотивації, включаючи розвідувальні дії, спроби дестабілізації та економічне вимагання через вимагачів. Чималі малі та середні підприємства в Україні можуть бути менше підготовлені до кіберзагроз порівняно з більшими корпораціями. Вони часто мають обмежені ресурси для інвестування у кібербезпеку та підготовку свого персоналу, що робить їх особливо вразливими. Авторами досліджено, що в умовах воєнного конфлікту кібербезпека вимагає не лише постійного вдосконалення, але й адаптації до нових загроз. Зловмисники постійно адаптують свої методи, щоб обходити захисні бар'єри, що підкреслює важливість регулярного оновлення заходів захисту та моніторингу кіберпотенцій. Тому дослідження проблеми кібербезпеки бізнесу в умовах воєнних дій в Україні необхідне для розуміння сучасних загроз і розробки стратегій захисту, що відповідають унікальним викликам і умовам країни.
Ключові слова: *безпека, кібербезпека, інформаційна безпека, цифровізація бізнесу, кіберрозвідка, кібератаки, кіберзагрози, кібершпигуни, види кібератак.*

The study of the problem of cyber security of business in the conditions of military operations in Ukraine is extremely relevant and critically important today. The authors note that Ukraine has become an arena of active cyberattacks by adversaries, which are aimed at various sectors of its economy and critical infrastructure. These attacks can have various motivations, including reconnaissance, destabilization attempts, and economic extortion through ransomware. Many small and medium-sized enterprises in Ukraine may be less prepared for cyber threats compared to larger corporations. They often have limited resources to invest in cybersecurity and train their staff, making them particularly vulnerable. The authors researched that in the conditions of a military conflict, cyber security requires not only constant improvement, but also adaptation to new threats. Attackers are constantly adapting their methods to bypass security barriers, which underscores the importance of regularly updating cyber security and monitoring measures. Therefore, the study of the problem of cyber security of business in the conditions of military operations in Ukraine is necessary for understanding modern threats and developing protection strategies that meet the country's unique challenges and conditions. In the conditions of war, the risk of using disinformation and social engineering to achieve their goals by cybercriminals increases. This may include the spread of fake news, phishing attacks, and manipulation to destabilize the situation in the region. In times of war, many companies face limited resources and a shortage of skilled cybersecurity professionals. This makes it difficult to detect and respond to cyber attacks in a timely manner, as well as to take the necessary measures to protect information systems. One of the key tasks of business in the conditions of military operations is to ensure the continuity of operations. This requires effective disaster recovery plans, as well as data backups and alternative communication channels. According to the authors, cyber security of business is a continuous and extremely relevant process in modern Ukrainian realities. It is a process, since the enemy is constantly working on improving attacks – which means that we should work on improving defense. This task remains strategically important for both government institutions and private businesses. Another front on the way to our sure victory!
Key words: *security, cyber security, information security, digitalization of business, cyber intelligence, cyber attacks, cyber threats, cyber spies, types of cyber attacks.*

Постановка проблеми. В умовах воєнних дій кібербезпека бізнесу набуває особливого значення. Поєднання військових конфліктів та кіберзагроз створює нові виклики для компаній, які змушені адаптуватися до змін в умовах підвищеного ризику. Під час воєнних дій спостерігається значне зростання кількості та складності кібератак. Атакуючі можуть бути як державними акторами, так і приватними хакерськими групами, що використовують хаос війни для своїх цілей. Атаки можуть бути спрямовані на критичну інфраструктуру, державні установи та приватні компанії, що створює додаткові загрози для безперервності бізнесу.

Загострення кібербезпеки під час воєнних дій також зумовлено вразливістю критичної інфраструктури, зокрема енергетики, транспорту, зв'язку та фінансової системи. Атаки на ці об'єкти можуть призвести до значних перебоїв у їх роботі, що вплине на весь бізнес-сектор.

Аналіз останніх досліджень та публікацій. Незважаючи на значний прогрес у сфері кібербезпеки, існує ряд невирішених проблем, які потребують подальшого дослідження та впровадження ефективних рішень, особливо в умовах війни. Вивчення проблематики кібербезпеки бізнесу, особливо в умовах війни, проводять різні науковці та експерти. Серед них можна виділити

[1] ORCID: https://orcid.org/0000-0001-8786-9582
[2] ORCID: https://orcid.org/0000-0003-0942-227X
[3] ORCID: https://orcid.org/0009-0003-0803-6307

праці Вишківського В., Когута Ю., Кузьменка О., Криворучка О. та інших. Багато дослідників зробили вагомий внесок у розуміння загроз, методів захисту та організаційних підходів до кібербезпеки. Однак, незважаючи на значний прогрес, залишаються області, які потребують додаткового дослідження. Невирішеними залишаються питання у сфері кібербезпеки бізнесу в умовах воєнного стану динаміка та еволюція кібератак, специфіка ризиків для різних галузей національної економіки, психологічні аспекти наслідків кібератак тощо. Проблематика кібербезпеки бізнесу в умовах війни є багатогранною і вимагає комплексного підходу. Незважаючи на значні досягнення в цій сфері, багато аспектів залишаються недостатньо дослідженими. Подальші дослідження повинні враховувати специфічні виклики та умови, які виникають під час військових конфліктів, щоб розробити ефективні стратегії захисту та забезпечити безперервність бізнес-процесів.

Постановка завдання. Саме питанню особливостей забезпечення кібербезпеки вітчизняного бізнесу в умовах війни буде присвячене наукове дослідження.

Виклад основного матеріалу дослідження. Кібербезбека в бізнесі є надзвичайно важливим елементом, оскільки сучасний цифровий простір підприємств стикається стикаються з різноманітними кіберзагрозами, що можуть призвести до серйозних фінансових втрат, втрати даних, порушення репутації та інших негативних наслідків. Важливим моментом при захисті комерційної інформації та даних є конфіденційність, яка включає захист від несанкціонованого доступу, крадіжок даних, втрати даних тощо. Підприємства повинні вживати заходів для шифрування даних, встановлення сильних паролів, регулярного резервного копіювання даних та використання захисного програмного забезпечення.

Особливе місце у бізнесі займає захист мережі та інфраструктури підприємства, який можливий за допомогою встановлення брандмауерів, антивірусного програмного забезпечення, систем виявлення вторгнень (IDS), систем управління доступом (IAM) та інших заходів захисту.

В епоху тотальної цифровізації актуальним лишається і освіта та навчання персоналу, надання інформації про загрози кібербезпеки та процедури безпеки. Це може включати навчання про сильні паролі, виявлення шахрайства, управління електронною поштою та інші аспекти кібербезпеки.

Підприємства повинні мати системи моніторингу та виявлення інцидентів, які дозволяють вчасно виявляти та реагувати на потенційні загрози кібербезпеки. Це включає в себе встановлення систем журналювання подій, аналіз відхилень та виявлення аномальних активностей.

Особливої актуальності та критичної необхідності забезпечення кібербезпеки в бізнесі набуло з початком повномасштабного вторгнення росії на нашу територію.

В реаліях, коли Україна захищає свою національну безпеку та цілісність від агресії з боку рф, кіберпростір – це стратегічно важливий фронт. Наша країна щоденно продовжує бути мішенню хакерських атак, спрямованих на державні установи критичної інфраструктури, приватний бізнес та на українських громадян. За даними Державної служби спеціального зв'язку та захисту інформації України, від початку повномасштабної війни, росія здійснила 796 кібератак проти України, що втричі більше у порівнянні з аналогічним періодом минулого року [1].

Варто також відзначити, що, незважаючи на складну ситуацію і численні виклики для кібербезпеки, Україна їм протистоїть. Вона посідає 24-те зі 160 місць у рейтингу Національного індексу кібербезпеки, який щорічно складає Фонд електронного врядування Естонії. Це доволі потужний показник, бо в цьому переліку ми випереджаємо навіть такі європейські країни, як Австрія, Швейцарія, Ірландія та Норвегія. Однак, 24 місце говорить про те, що слабкі місця в українському кіберзахисті все ще присутні і працювати точно є над чим [2].

Проте, в умовах військових дій дані показники досить важко поліпшувати через значну низку чинників. На нашу думку, серед основних загроз для вітчизняного бізнесу під час війни варто виділити наступні:

1. Гібридна агресія з боку рф, яка проявляється у дестабілізації інформаційної системи, шляхом нападів на критичну інфраструктуру з метою виведення з ладу ключових інформаційних систем. Не варто залишати поза увагою і порушення доступу до Інтернету через блокування або обмеження доступу до Інтернету для створення хаосу і дезорганізації.

2. Кіберзлочинність, яка представлена у вигляді порушення інформаційних ресурсів у вигляді атак на сайти і сервери для отримання фінансової вигоди або політичних цілей або маніпуляції з даними для створення недовіри до державних структур і виборчих процесів.

3. Техніко-технологічна залежність від іноземних виробників IT-продукції, яка в деяких випадках через обмеженість місцевого виробництва IT-продукції ускладнює заміну ризикових технологій.

4. Вразливість IT-інфраструктури компаній, яка проявляється у розосередженні працівників через віддалену роботу, оскільки це збільшує ризики, пов'язані з безпекою домашніх мереж та використання незахищених каналів зв'язку та пристроїв.

5. Відсутність належного контролю за кіберзахистом проявляється у недостатньому контролі

з боку державних органів через відсутність чіткої стратегії та моніторингу заходів з кіберзахисту та недостатню підготовку кадрів у сфері кібербезпеки. Звичайно, що в сучасних умовах війни більше уваги приділяється кіберзахисту стратегічних військових планів та стратегій на рівні держави, а не на рівні окремих підприємств.

Реальні прояви кібератак є мало прогнозованими, а їх результатом, стають значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які впливають на стан фінансової та економічної безпеки бізнесу та процесу його споживання. Прикладом такої непрогнозованої кібератаки є славетна ніч з 13 на 14 січня 2022 року під час якої хакери за допомогою атак вивели із ладу понад 70 урядових сайтів. Наслідком такої атаки було те, що бізнес був позбавлений можливості зайти на будь-який сайт міністерства і дізнатися потрібну йому інформацію. Також, вони були позбавлені можливості моніторингу свої судових рішень, оскільки ані вебсайт судової влади, ані реєстр судових рішень не працювали [3].

Саме з початком військових дій на території України найбільше від кібератак постраждали державні установи (атаки на урядові сайти та системи з метою паралізувати роботу державних органів), банки та фінансові організації (кібератаки, спрямовані на викрадення коштів, злам систем обробки платежів та порушення роботи банківських сервісів), Інтернет-магазини (атаки, спрямовані на викрадення платіжних даних клієнтів та порушення роботи онлайн-платформ), IT-компанії (зломи корпоративних мереж, крадіжка інтелектуальної власності та порушення послуг), виробничі підприємства (атаки з метою блокування виробництва та крадіжки конфіденційної інформації), стартапи (точкові атаки на молоді компанії для отримання інноваційних технологій або дестабілізації роботи).

Перед початком війни та на її початковому етапі кількість та інтенсивність кібератак різко зросла. Для прикладу, щодо найбільш вагомих дат масованих кібератак:

1) 13-14 січня – перші серйозні атаки на державні установи;

2) 15-16 лютого – наступна хвиля атак, що передувала вторгненню;

3) 23-24 лютого – кібератаки, синхронізовані з початком вторгнення.

Кожна українська компанія повинна бути готова до кібератак та заздалегідь оцінити свою вразливість. Комплексний підхід, що включає технічні, організаційні та юридичні заходи, є ключем до ефективного захисту від кіберінцидентів та забезпечення безпеки бізнесу в умовах війни.

Не менш важливу роль відіграє український IT-бізнес. Найбільші гравці ринку та волонтери об'єднали IT-спеціалістів, працюючи над відбиттям кібератак на об'єкти критичної інфраструктури, нейтралізацією російських чат-ботів та хакерів, а також допомагаючи іншим бізнесам адаптуватися до умов, що кардинально змінилися. Наприклад, Gigacloud безкоштовно евакуював дата-центр Prozorro з Києва до Львова, незважаючи на обстріли [4].

Головна загроза в тому, що підприємства налагоджують потужний кіберзахист своїх інформаційних систем, але водночас їм важко контролювати всіх своїх партнерів та підрядників, яким дають доступ до своїх даних. Ці партнери та підрядники можуть мати нижчий рівень кіберграмотності серед співробітників, слабші рішення з кібербезпеки тощо. Саме цими вразливостями хакери й користуються, атакуючи компанії-підрядники та отримуючи доступ до потрібних їм інформаційних систем [5].

Однозначно, що із цифровізацією економіки, функціонуванням вітчизняного бізнесу в складних умовах значно змінюється і структура основних видів кібербезпеки, що мають місце на вітчизняних ринках.

Нами узагальнено основні види кіберзагроз з можливими їх наслідками для вітчизняного бізнесу.

Відповідно варто зауважити, що незалежно від виду кіберзагрози наслідки для бізнесу можуть бути досить серйозними. В контексті виявлених наслідків варто виокремити наступні стратегії вирішення зазначених проблем:

1. Покращення координації між секторами бізнесу та державних органів, створенням централізованих спеціальних органів та постійний обмін інформацією про загрози.

2. Розробка нових технологій захисту можлива при підтримці наукових досліджень у сфері кібербезпеки та розробці систем на основі AI для виявлення і реагування на кіберзагрози.

3. Посилення контролю та підготовки, розробляючи програмні навчання та регулярним аудитом безпеки.

4. Підтримка віддаленої роботи, особливо в сучасних умовах це є вимушеною необхідністю. Це можливе забезпеченням захищеного доступу використанням VPN та інших засобів захисту для віддаленої роботи та підвищенням безпеки домашніх мереж.

В умовах воєнних дій усі галузі національної економіки намагаються адаптуватись до функціонування в сучасних реаліях. Військові конфлікти часто стимулюють розвиток нових типів кібератак. Хакери можуть націлюватися на постачальників і партнерів бізнесу для отримання доступу до основних систем. Використання більш витончених вірусів та інших шкідливих програм, які важко виявити стандартними засобами захисту.

Таблиця 1

Основні види кібератак на можливі їх наслідки

Вид кібератаки	Характеристика	Наслідки
Фішинг	є однією з найпоширеніших форм кіберзлочинів, яка спрямована на викрадення конфіденційної інформації та облікових даних. Цей вид атак призводить до значних фінансових втрат щороку. Метою фішингу є обманом змусити користувачів надати особисті дані або встановити зловмисне програмне забезпечення	Викрадення коштів з банківських рахунків або зловмисне використання кредитних карток. Викрадення конфіденційної інформації, що може призвести до порушення приватності клієнтів і втрати конкурентної переваги. Порушення довіри клієнтів та партнерів, що може призвести до втрати бізнесу.
Смішинг	різновид фішингу, де зловмисники використовують текстові повідомлення замість електронної пошти для здійснення своїх атак. Метою є отримання доступу до конфіденційної інформації, яка зберігається на мобільних пристроях, або встановлення зловмисного програмного забезпечення	Поширення зловмисного ПЗ в корпоративній мережі, викрадення конфіденційної інформації, порушення безпеки мережі.
Зловмисне програмне забезпечення	загроза для кібербезпеки компаній, яке може існувати в багатьох формах і здійснювати різні шкідливі дії. Зловмисники розробляють такі програми для отримання постійного доступу до пристроїв компанії, що дозволяє їм викрадати дані, досліджувати локальну мережу або використовувати пристрої для інших злочинних дій	Прямі фінансові збитки, витрати на відновлення, штрафи та компенсації, викрадення даних, порушення роботи систем, репутаційні втрати, компрометація безпеки
Програмні вимагачі	вид шкідливого програмного забезпечення, який блокує доступ до комп'ютерної системи або шифрує дані користувача до моменту сплати викупу. Зазвичай зловмисники вимагають платежі у криптовалюті, щоб уникнути відстеження	фінансові, репутаційні та операційні втрати
Внутрішні загрози	виникають, коли нинішні чи колишні співробітники, партнери або підрядники зловживають своїм доступом до конфіденційної інформації компанії	можуть бути руйнівними для фінансової стабільності, репутації та операційної ефективності компанії
Компрометація корпоративної електронної пошти	полягає у використанні зловмисниками обманних методів для компрометації корпоративних електронних листів з метою обману компаній. Зловмисники зламують бізнес-системи, отримують доступ до інформації про платіжні системи компанії та маніпулюють працівниками, щоб ті здійснювали платежі на підставні банківські рахунки.	є однією з найдорожчих та найнебезпечніших форм кіберзлочинів, яка може завдати значних фінансових, репутаційних та юридичних збитків
Ненавмисне розголошення		фінансові збитки через витік конфіденційної інформації, може негативно вплинути на репутацію компанії серед клієнтів і партнерів
Атаки нульового дня	вони використовують раніше невідомі вразливості в програмному забезпеченні або апаратур	втратити значні суми через крадіжку даних, вимоги викупу або втрату бізнесу
Розвідка сховища	кіберзлочинці активно шукають незахищені інтерфейси та конфігураційні помилки, щоб отримати доступ до важливих даних	фінансові збитки через відшкодування шкоди клієнтам або покарання від регулюючих органів, компанії можуть стикнутися з правовими санкціями і штрафами за порушення законодавства про захист персональних даних або конфіденційної інформації
Витік даних	будь-яке несанкціоноване переміщення даних з особистих або робочих пристроїв	Фінансові збитки, юридичні, технологічні, технічні, організаційні проблеми
Соціальна інженерія	є одним з найбільш ефективних методів атаки в сучасній кібербезпеці, оскільки вона використовує психологічні маніпуляції для отримання доступу до конфіденційної інформації або систем компанії	Крадіжка даних і фінансових втрат, порушення довіри і репутаційні ризики, операційні зупинки і втрати виробничої потужності

Джерело: узагальнено авторами на основі [6]

В умовах війни ефективна координація між державними органами, приватними компаніями та міжнародними партнерами є критично важливою, але часто недостатньо розвиненою. Компанії часто не бажають ділитися інформацією про інциденти, що заважає створенню загальної картини загроз і розробці спільних заходів захисту.

Висновки із цього дослідження і дальші перспективи в цьому напрямку. Враховуючи вищезазначені аспекти, бізнес повинен підвищити свою готовність до кіберзагроз в умовах воєнних дій, що забезпечить їх стабільну роботу та захист від потенційних атак.

Кібербезпека в Україні сьогодні дійсно є критично важливим аспектом, оскільки країна знаходиться під надзвичайною кіберінтенсивністю через військові дії та постійні кібератаки. Великий системний бізнес та державні установи, такі як урядові організації, критична інфраструктура, оборонні підприємства та інші ключові сектори економіки, є основними мішенями для кіберзлочинців та кібершпигунів. Україна, будучи на передньому краї кібервійни, постійно стикається зі складними і високорівневими кібератаками, які мають на меті не лише викрадення даних, а й дестабілізацію критично важливих інфраструктурних об'єктів. Зловмисники постійно вдосконалюють свої техніки, тому захист від кіберзагроз також повинен бути постійно оновлюваним і адаптивним. Це вимагає великих витрат на кібербезпеку та регулярні тренування персоналу. Україна активно співпрацює з міжнародними партнерами, щоб підвищити кібербезпеку через обмін інформацією про загрози та технологічні засоби захисту. Великий акцент приділяється навчанню та підвищенню кібербезпекової культури серед співробітників усіх рівнів, оскільки люди часто є слабким ланцюжком у кіберзахисті. Забезпечення надійного захисту критичної інфраструктури, такої як енергетика, телекомунікації, транспорт і фінанси, є пріоритетом для української держави.

У цих умовах кібербезпека стає не лише обов'язковою вимогою для успішної діяльності підприємств та державних установ, але й стратегічним завданням для збереження національної безпеки та стійкості економіки.

БІБЛІОГРАФІЧИЙ СПИСОК:

1. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html

2. Кібербезпека бізнесу під час війни. URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny

3. Кібербезпека підприємства: що врахувати. URL: https://jurliga.ligazakon.net/news/209245_kberbezpeka-pdprimstva-shcho-vrakhuvati

4. Кібербезпека бізнесу під час війни. URL: https://mklegalservice.com/tpost/k123zz39h1-kberbezpeka-bznesu-pd-chas-vini

5. Кузьменко О., Маклюк О., & Чернишова О. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. № 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-21

6. ТОП 10 загроз кібербезпеці бізнесу у 2023 році. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023

7. Шостак Л.В., Сур'як А.В. Особливості забезпечення безпеки діяльності підприємства в умовах цифрової трансформації економіки. *Науковий погляд: економіка та управління.* 2023. № 3(83). С. 140–145.

REFERENCES:

1. Kiberbezpeka biznesu v umovakh nestabilnosti [Business cyber security in conditions of instability]. Available at: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html

2. Kiberbezpeka biznesu pid chas viiny [Business Cybersecurity in a Time of War]. Available at: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny

3. Kiberbezpeka pidpryiemstva: shcho vrakhuvaty [Enterprise cyber security: what to consider]. Available at: https://jurliga.ligazakon.net/news/209245_kberbezpeka-pdprimstva-shcho-vrakhuvati

4. Kiberbezpeka biznesu pid chas viiny [Business Cybersecurity in a Time of War]. Available at: https://mklegalservice.com/tpost/k123zz39h1-kberbezpeka-bznesu-pd-chas-vini

5. Kuzmenko, O., Makliuk, O., & Chernyshova, O. (2022) Kiberbezpeka biznesu pid chas viiny [Business Cybersecurity in a Time of War]. *Ekonomika ta suspilstvo*, vol. 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-21

6. TOP 10 zahroz kiberbezpetsi biznesu u 2023 rotsi [TOP 10 business cyber security threats in 2023]. Available at: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023

7. Shostak L.V., Suriak A.V. (2023). Osoblyvosti zabezpechennia bezpeky diialnosti pidpryiemstva v umovakh tsyfrovoi transformatsii ekonomiky [Features of ensuring the security of the enterprise in the conditions of digital transformation of the economy]. *Naukovyi pohliad: ekonomika ta upravlinnia*, no. 3(83), pp. 140–145.