УДК 004.056:330.341.1
DOI: https://doi.org/10.32782/business-navigator.78-74

Саврацький О.О.
аспірант
Національний університет «Одеська юридична академія»

Savratskyi Oleksandr
Postgraduate Student
National University "Odesa Law Academy"

АНАЛІЗ КОН'ЮНКТУРИ РИНКУ ПРОДУКТІВ ТА ПОСЛУГ КІБЕРБЕЗПЕКИ

ANALYSIS OF THE MARKET CONDITIONS FOR CYBERSECURITY PRODUCTS AND SERVICES

Стаття присвячена дослідженню сучасного стану ринку продуктів та послуг кібербезпеки, його ключових тенденцій, особливостей попиту та пропозиції. Проведено аналіз глобального та українського ринків. Окреслено проблеми, що стримують попит, зокрема недостатню готовність малого та середнього бізнесу до інвестицій у цю сферу. Розглянуто динаміку зростання кіберзагроз, особливо в умовах повномасштабного вторгнення, та їхній вплив на економіку. Виокремлено основні бар'єри розвитку галузі, такі як відсутність систематизованої статистики, брак стандартів і інституційних механізмів. Проаналізовано внесок українських розробників та інтеграторів у міжнародний ринок кібербезпеки та їхні конкурентні переваги. Запропоновано рекомендації для підвищення ефективності функціонування ринку, включаючи розвиток інноваційних технологій, удосконалення політики кіберзахисту та підвищення обізнаності суб'єктів підприємництва щодо кіберризиків.

Ключові слова: кібербезпека, ринок, послуги, попит, пропозиція, економічний аналіз, конкуренція, ціна.

This article is dedicated to analyzing the current state of the cybersecurity products and services market, its key trends, and the specific characteristics of supply and demand. It highlights critical challenges faced by Ukrainian companies in adopting effective cybersecurity measures, particularly the low readiness of small and medium-sized enterprises (SMEs) to invest in data protection. The study evaluates the dynamics of the global and Ukrainian cybersecurity markets, noting the rising frequency and complexity of cyber threats, especially amidst the full-scale invasion. The lack of systematic statistics, institutional mechanisms, and standards in Ukraine is identified as a significant barrier to the development of the sector. The research emphasizes the competitive advantages of Ukrainian specialists and companies, including their substantial contributions to the global cybersecurity industry. Ukrainian expertise has proven effective in addressing challenges such as DDoS attacks, malware protection, and incident response, showcasing the potential for integration into the international market. The study also analyzes the primary consumers of cybersecurity products and services, focusing on large and medium-sized businesses, critical infrastructure sectors, and industries such as finance, energy, and transportation. Recommendations are provided to enhance the efficiency of the cybersecurity market, including fostering innovation, improving public-private partnerships, and raising awareness among businesses about the importance of cybersecurity investments. Additionally, the potential for comprehensive "turnkey" solutions and educational initiatives to increase the overall cybersecurity culture within organizations is explored. This research concludes that cybersecurity is not only an economic necessity but also a strategic priority for Ukraine's stability and development, particularly in the face of escalating cyber threats. The findings underline the importance of continuous improvement in cybersecurity measures through technological advancement, regulatory updates, and proactive engagement with international best practices.

Keywords: cybersecurity, cybersecurity market, cyber threats, economic analysis, innovative technologies.

Постановка проблеми. В умовах цифрових трансформацій кібербезпека поступово перетворюється на один з фундаментальних чинників вливу не тільки на фінансові результати діяльності суб'єктів підприємництва, а й взагалі на їхнє існування. Надійний кіберзахист потрібен для підтримки усіх основних бізнес-процесів, а також збереження банківських рахунків, електронної пошти, вебсайтів, мобільних застосунків та акаунтів у соцмережах і месенджерах, особистих даних клієнтів тощо.

Ще навіть до початку повномасштабного вторгнення Україна перебувала серед лідерів за рівнем кіберризиків, а з 2022 року кількість кібератак взагалі зростає майже щодня. Це дозволяє стверджувати про стійку наявність запитів на впровадження ефективної системи кібербезпеки з боку підприємств та організацій, зокрема тих, що відносяться до критичної інфраструктури. Однак вітчизняні підприємства та організації здебільшого мінімізують або, взагалі, відкладають інвестиції в кіберзахист. Означений факт можна пояс-

нити, насамперед, низькою обізнаністю, як менеджменту, так і пересічних працівників, щодо важливості кіберзахисту. Адже її розуміння приходить, найчастіше, лише після першого кіберінциденту та подальшою оцінкою його наслідків.

Аналіз останніх досліджень і публікацій. В останні роки під впливом збільшення кіберзагроз і розвитку цифрових технологій науковці почали досліджувати кібербезпеку не тільки в технологічній площині, а і в якості певного товару чи послуги (в залежності від обставин), що є об'єктом купівлі-продажу. Зокрема, у дослідженнях В. Смєсової [1] аналізується глобальна кон'юнктура ринку товарів і послуг, включаючи ІТ-напрям. Наукові праці В. Поліщука [3] фокусуються на правових аспектах боротьби з кіберзлочинністю, зокрема через роль CERT-UA [4]. У свою чергу С. Оніщенко [5] та А. Глушко [5] підкреслюють необхідність пошуку нових моделей безпеки через зростаючі зовнішні загрози [6]. В контексті питань національної безпеки І. Бегаль [7] відзначає різке зростання кількості кібератак на Україну, більшість з яких здійснюється групами, що контролюються Росією. Це підкреслює необхідність посилення кіберзахисту на національному рівні. Паралельно із цим М. Рахман [8] і С. Корабельський [8] підкреслюють важливість розвитку кібербезпеки в Україні з урахуванням її технічного потенціалу. Вони вказують на необхідність впровадження інноваційних рішень для захисту від зовнішніх загроз і розвитку національного ринку кібербезпеки для інтеграції в глобальний контекст. І, нарешті, дослідження С. Горбаченка [9] зосереджуть увагу на менеджменті кібербезпеки та його місці в сучасній управлінській практиці.

Таким чином проблеми кібербезпеки формують окремий междисциплінарний напрям досліджень, але саме кон'юнктурних досліджень за цим напрямом все ще повноцінно не проводилось.

Формулювання завдання дослідження. Метою дослідження є аналіз поточної кон'юнктури ринку продуктів та послуг кібербезпеки, визначення ключових тенденцій, особливостей попиту та пропозиції, а також розробка рекомендацій щодо підвищення ефективності функціонування ринку в умовах трансформацій кіберзагроз. Особливу увагу приділено виявленню бар'єрів, які стримують впровадження якісних рішень у сфері кіберзахисту, та пошуку шляхів їх подолання з урахуванням специфіки українського бізнес-середовища і сучасних безпекових викликів, пов'язаних з війною.

Виклад основного матеріалу дослідження. Під кон'юнктурою ринку слід розуміти ситуацію у певний момент або період часу, що формується під впливом внутрішніх і зовнішніх, цінових і нецінових факторів, а їхніх трансформацій та характеризується рівнем і динамікою попиту, пропозиції, рівня цін [1].

Дослідження наведених факторів передбачають аналіз поточного та перспективного стану внутрішнього та зовнішнього середовища, а також їхньої взаємодії. На рівні окремих галузей національної економіки, зокрема, й ІТ-сфери, кожен об'єкт дослідження розглядається у взаємодії із загальногосподарською кон'юнктурою, а також із кон'юнктурою споживаючих галузей, суміжних галузей і допоміжних галузей. У свою чергу дослідження сегменту кібербезпеки, як окремої складової ІТ-сфери, доцільно проводити на трьох рівнях: вивчення об'єкта загалом, із наданням характеристики узагальнених показників, вивчення структури об'єкта та системи зв'язків між його окремими складовими, і опис поточного стану та прогнозування розвитку окремих складових об'єкта.

Глобальний ринок кібербезпеки демонструє стійке зростання, обумовлене збільшенням кількості та складності кібератак. Так, у 2023 році обсяг світового ринку кібербезпеки становив 238,13 млрд доларів США, у 2024 році – 268,13 млрд доларів США, а до 2034 року очікується, що він сягне близько 878,48 млрд доларів США. Можна стверджувати, що ринок розширюється і характеризується стабільним середньорічним темпом зростання (CAGR) 12,6% протягом прогнозованого періоду з 2024 по 2034 рік [2]. І, згідно з прогнозами, у майбутньому обсяг вказаного ринку також буде стало збільшуватися (рис. 1.).

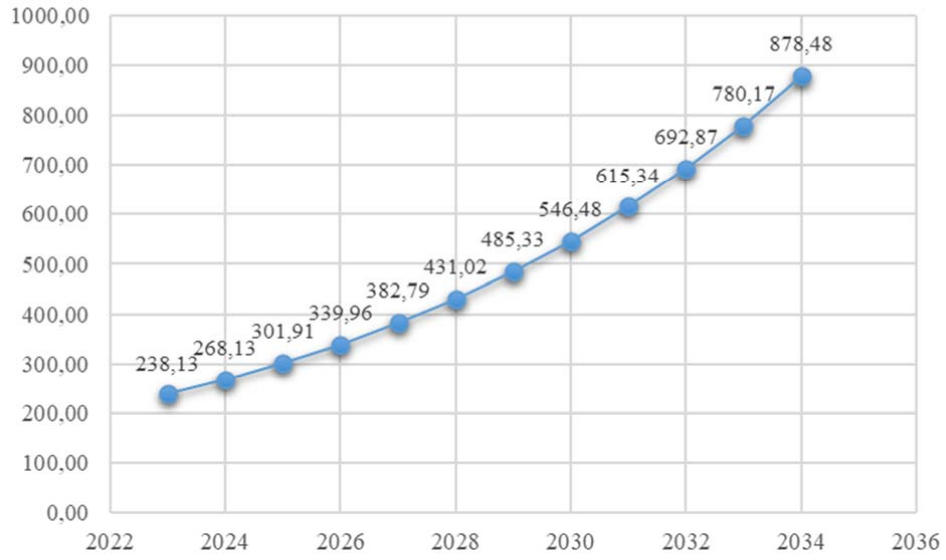

Рис. 1. Динаміка та прогноз обсягів ринку кібербезпеки 2023–2034 рр., млрд дол

Джерело: складено за даними [2]

Однак, одночасно із збільшенням витрат на кібер-захист, збитки від кіберзлочинності у 2023 році сягнули 8 трильйонів доларів США, і очікується, що до 2025 року ця цифра зросте до 10,5 трильйонів доларів [3]. І при цьому саме Україна знаходиться серед лідерів за темпами зростання кіберзагроз. Так, лише у 2023 році кількість кібератак зросла на 16% порівняно з попереднім роком, досягнувши 2543 інцидентів. Найчастіше атак зазнавали урядові організації та місцеві органи влади [4].

Попри ці виклики, а, інколи, й, завдяки ним, Україна покращує свої позиції у сфері кібербезпеки. У 2020 році країна посіла 25-те місце у Національному індексі кібербезпеки, піднявшись на 4 позиції порівняно з попереднім рейтингом [5]. Можна стверджувати, що Україна, зберігає всі шанси на успішну інтеграцію в міжнародний ринок, особливо завдяки своїм внутрішнім конкурентним перевагам.

По-перше, в Україні існує значний потенціал для розвитку внутрішнього ринку кібербезпеки, адже більшість секторів ще й досі не забезпечені належним кіберзахистом. Це відкриває перспективи для впровадження сучасних технологій захисту даних та інфраструктури. Уряди, комерційні організації, освітні установи та навіть медичні заклади все частіше стають об'єктами кібератак, що створює попит на комплексні рішення у сфері кіберзахисту [6]. З іншого боку, офіційної статистики щодо обсягів внутрішнього ринку продуктів та послуг кібербезпеки в Україні наразі фактично не існує. Це пов'язано з кількома факторами: відсутністю систематизованих даних для проведення якісного аналізу та складнощами їх оприлюднення через засекреченість значної частини інформації. Тому більшість кількісних даних отримується виключно експертним методом.

По-друге, Україна володіє безцінним досвідом протистояння кіберзагрозам, отриманим в умовах повномасштабного вторгнення Росії. Починаючи з 2022 року, Україна займає друге місце у світі за кількістю кібератак, поступаючись лише США. Кількість атак на критично важливу інфраструктуру та організації країни зросла майже втричі, що свідчить про безпрецедентний рівень загроз. У таких умовах українські фахівці розробили і впровадили інноваційні підходи до боротьби з хакерськими атаками, включаючи відбиття масових DDoS-атак, захист від шкідливого програмного забезпечення та побудову ефективних систем моніторингу кіберзагроз [7].

Особливим досягненням України у сфері кібербезпеки стало створення та удосконалення національної системи захисту. Синергія зусиль державних органів, приватного сектору та міжнародних партнерів забезпечила розробку передових технологій та підвищила стійкість до зовнішніх загроз. Українські кіберексперти беруть активну участь у міжнародних проектах, ділячись своїм досвідом із глобальною спільнотою, що допомагає розширити експорт послуг у цій сфері.

По-третє, значний кадровий потенціал. Насамперед, середній вік вітчизняних фахівців становить приблизно 30 років, у той час як у США – 40 років. Це свідчить про переважання молодих, перспективних кадрів, котрі зможуть працювати продуктивно протягом більшого періоду часу. Крім того, за рівнем кваліфікації 63% доводиться на фахівців Middle, які вже мають значний досвід роботи (рис. 2) [8]. Далі йдуть фахівці Senior і Junior, з частками 25% та 8% відповідно.

Коли мова йде окремо про сегмент кібербезпеки, слід додати, що крім профільних знань, кваліфікований фахівець повинен вміти працювати із базовими програмами, мати знання проєктного менеджменту, бути адаптивним та гнучким [2]. Наявність Soft skills для фахівця з кібербезпеки (вміння презентувати результат роботи, працювати в команді, відчувати емпатію) настільки ж важливі, як і орієнтування у технічному матеріалі.

Основними споживачами продуктів та послуг у сфері кібербезпеки залишаються представники великого та середнього бізнесу, для яких питання захищеності комп'ютерних та інформаційних мереж є критично важливим. У сучасних умовах вказані під-

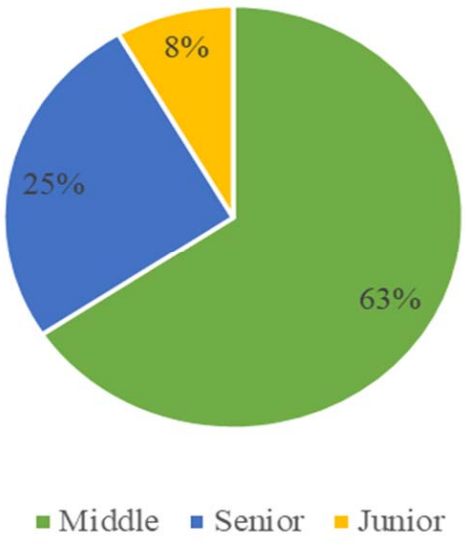

Рис. 2. Структура кадрів ІТ-сфери за рівнем кваліфікації

Джерело: складено за даними [8]

приємства та організації стикаються із дедалі складнішими викликами, від дрібного фішингу до масових DDoS-атак. Впровадження новітніх технологій захисту дозволяє мінімізувати ризики фінансових втрат, втрати даних і порушення нормального функціонування.

Серед галузей, які найбільше інвестують у кібербезпеку, можна виділити військово-промисловий комплекс, який в умовах війни активно впроваджує нові методи захисту від атак на критично важливу інфраструктуру та військові системи. Банки та кредитно-фінансові організації також перебувають у зоні високого ризику, адже саме вони часто стають об'єктами кібератак, спрямованих на крадіжку коштів чи доступ до конфіденційних даних клієнтів (рис. 3) [9].

Енергетика є ще однією стратегічною галуззю, яка активно користується послугами кібербезпеки. Адже атаки на енергетичну інфраструктуру можуть мати катастрофічні наслідки для країни, тому представники цієї галузі інвестують у сучасні системи моніторингу та запобігання загрозам. Розробники програмного забезпечення, які самі створюють засоби захисту, також витрачають значні ресурси на забезпечення безпеки своїх продуктів.

Транспортна сфера, зокрема авіація, залізниця та автомобільні перевезення, також залежить від якісного кіберзахисту, оскільки кібератаки на системи управління можуть призвести до серйозних порушень роботи. І навіть класичні торговельні підприємства, які дедалі активніше переходять до електронної комерції, відповідно починають стикатися з кіберзагрозами і впроваджують нові рішення для захисту своїх бізнес-процесів.

З іншого боку представники малого бізнесу, зазвичай, недостатньо обізнані у питаннях кібербезпеки та обмежені у ресурсах для реалізації проєктів з кіберзахисту. Відтак важливо щоб саме власники бізнесу визнали наявність кіберризиків і взяли на себе лідерство та відповідальність в процесі впровадження заходів кібербезпеки, які необхідно вживати не тільки для самого суб'єкта підприємництва, але й для його бізнес-партнерів та контрагентів [10].

Щодо мотивації до витрачання коштів на продукти та послуги кібербезпеки, в першу чергу мова йде про можливі витоки та компрометацію даних, ризик викрадання грошових коштів та інших ресурсів суб'єкта підприємництва, блокування публічних інформаційних ресурсів, які використовуються для комунікації з клієнтами, промислове шпигунство та інші методи недобросовісної конкуренції і, звісно, призупинення або припинення деяких бізнес-процесів.

Все вищевказане дозволяє сформувати «портрет клієнта», в сегменті продуктів та послуг кібербезпеки, якому притаманні певні особливості попиту (табл. 1).

Пропозицію на ринку продуктів та послуг кібербезпеки формують декілька великих груп підприємців. Насамперед, це виробники (вендори) програмного забезпечення (software) та обладнання (hardware) для кіберзахисту. Можна зауважити, що на українському ринку прямо чи через посередників представлені практично усі провідні світові вендори, зокрема, Cisco, Fortinet, Mikrotik, McAfee, PaloAlto, FireEye. Далі, інтегратори, які адаптують стандартні рішення від різних виробників під наявні запити та потреби клієнтів. І, нарешті, консалтингові бізнес-структури, які пропонують окремі послуги з кібербезпеки, такі як аудит безпеки IT-інфраструктури, тестування на проникнення, аналіз коду, відповідність нормативним вимогам, кіберрозвідка тощо [12].

Щодо цінових чинників, варто зазначити, що вартість розробки, впровадження та підтримки системи

Рис. 3. Структура інвестування у кібербезпеку за секторами в Україні

Джерело: складено автором

Таблиця 1

Особливості клієнтів в сегменті продуктів та послуг кібербезпеки

Характеристика	Опис
Індивідуальність запитів.	Майже кожний замовник бажає придбати персоніфіковане рішення, наприклад, з урахуванням особливостей власних бізнес-процесів.
Варіативність.	На ринку присутня значна кількість готових рішень, а також розробники та інтеграторів, які пропонують власні послуги у сфері кіберзахисту. Отже клієнт обирає з декількох варіантів, які можуть відрізнятися, навіть, концептуально.
Технічна обізнаність.	Кожне замовлення обов'язково погоджується із технічним відділом або іншими профільними фахівцями.
Значні бюджети замовлень/ велика середня сума чеку.	Основними замовниками є представники великого та середнього бізнесу, діяльність яких залежить від рівня захищеності комп'ютерних та інформаційних мереж.
Прагнення до комплексного захисту.	Джерела кіберзагроз можуть бути дуже різними, але замовник зазвичай вимагає рішення, яке захистить від усіх, що призводить до формування системи кіберзахисту суб'єкта підприємництва.
Бажання швидкого виконання	Інколи замовник розуміє потребу у кібербезпеці після інциденту і підрахування втрат від нього. І, отже бажає негайного отримання надійного кіберзахисту, щоб унеможливити втрати у майбутньому.

Джерело: [11]

кібербезпеки може значно варіюватися залежно від багатьох параметрів. Основними з них є розмір і складність організації, обсяг даних, які необхідно захистити, рівень ризику, бажаний рівень захисту, а також тип і структура інфраструктури, яка підлягає захисту [10]. З огляду на це для малих підприємств витрати на кібербезпеку можуть бути невеликими, оскільки вони зазвичай потребують базових рішень для захисту даних, таких як антивірусне програмне забезпечення, системи фільтрації електронної пошти чи базова політика управління доступом. Вартість таких рішень може становити 300–1000 дол. залежно від кількості користувачів та особливостей конфігурації.

Для середнього та великого бізнесу витрати зростають у геометричній прогресії через необхідність впровадження комплексних рішень. Наприклад, розробка та впровадження спеціалізованих систем виявлення загроз (IDS/IPS), шифрування даних або розгортання багаторівневих систем моніторингу та реагування на інциденти може обійтися від десятків тисяч до сотень тисяч доларів. Крім того, великі організації змушені враховувати витрати на регулярне оновлення програмного забезпечення, проведення аудитів безпеки та навчання персоналу [13].

Окремо слід зазначити значення постійних витрат на підтримку кібербезпеки. Вони включають оцінку ризиків, модернізацію систем, впровадження нових захисних механізмів, а також управління інцидентами. За оцінками експертів, такі витрати можуть становити від 10% до 20% початкових інвестицій щороку, залежно від складності інфраструктури та динаміки змін у сфері кіберзагроз.

У випадку великих корпорацій, особливо в секторах з підвищеними вимогами до безпеки (наприклад, банківський сектор або військово-промисловий комплекс), часто застосовується концепція кібербезпечного кола (Cybersecurity Circle) [14]. Це інтегрована стратегія, яка включає такі компоненти:

– інформаційні ресурси (визначення та захист критичних даних);
– інформаційна інфраструктура;
– кібербезпека (впровадження технологій захисту, таких як фаєрволи, системи шифрування тощо);
– аудит та моніторинг;
– ідентифікація, оцінка та мінімізація ризиків;
– безпека персоналу, в першу чергу, навчання працівників правилам кібергігієни.
– управління інцидентами, насамперед, швидке реагування на загрози.

Цінова політика на ринку продуктів та послуг кібербезпеки може бути реалізована за кількома моделями. Перший варіант – це модель разової оплати, коли суб'єкт підприємництва один раз інвестує у розробку та впровадження рішень. Другий варіант – модель підписки, яка передбачає регулярні платежі за використання програмного забезпечення чи послуг (наприклад, Security as a Service). Третій варіант – гібридний підхід, що поєднує початкові інвестиції та постійні платежі за підтримку та оновлення систем.

Для отримання конкурентних переваг вітчизняні суб'єкти підприємництва, що працюють у сфері кібербезпеки, активно використовують інноваційні підходи до вивчення потреб своїх клієнтів. Глибше розуміння специфіки роботи клієнтів досягається, зокрема, через проведення детальних інтерв'ю перед початком співпраці. Такий підхід дозволяє не тільки ідентифікувати основні потреби та вразливості клієнта, але й зміцнює рівень довіри між сторонами. Наприклад, SoftServe, один із лідерів IT-індустрії в Україні, активно практикує попередні консультації з клієнтами для аналізу їхніх потреб, а також надає комплексні послуги з кібербезпеки, включаючи аудит, розробку та впровадження рішень.

Одним із найбільш ефективних інструментів підвищення лояльності споживачів є надання послуг «під ключ». Такі компанії, як ISS Art і CyberLab, пропонують замовникам комплексні рішення, які включають усе: від оцінки ризиків до розробки та підтримки захисних систем. Це дозволяє клієнтам уникнути необхідності залучення сторонніх підрядників, зменшує витрати часу та підвищує ефективність впровадження кібербезпеки.

Для активізації співпраці між підприємцями, що пропонують кібербезпекові послуги, та їхніми клієнтами в Україні впроваджено Програму кібердіагностики бізнесу. У межах зазначеної програми підпри-

ємства можуть скористатися послугами, такими як тестування на проникнення, оцінка безпеки мобільних застосунків або аналіз вразливостей інформаційного середовища. Наприклад, компанія 10Guards, яка є одним з лідерів у сегменті проведення пентестів, бере активну участь у таких ініціативах і допомагає малому та середньому бізнесу краще зрозуміти свої кіберризики [15].

Ще одним прикладом є HackControl, яка спеціалізується на оцінці вразливостей і тестуванні інформаційної інфраструктури клієнтів. Їхні послуги вже допомогли багатьом українським підприємствам зменшити ризик кібератак та зміцнити свої системи безпеки [16]. Серед інших компаній, які активно підтримують програму кібердіагностики, можна відзначити Beetroot [17] та EPAM Ukraine [18], які надають не лише послуги з безпеки, а й навчання персоналу основам кібергігієни, що є важливим компонентом комплексного підходу до захисту інформації.

Висновок. Надійний кіберзахист є однією з базових потреб українського бізнесу, хоча його представники не завжди це усвідомлюють повною мірою. З початком повномасштабного вторгнення, коли багато українських підприємств зіткнулися з масштабними кібератаками з боку ворожих структур, цей аспект набув критичного значення.

На вітчизняному ринку продуктів та послуг кібербезпеки наразі представлені майже всі світові лідери: від виробників програмного забезпечення до постачальників апаратного захисту та консалтингових послуг. Крім того, зростає попит на розробку індивідуальних рішень «під ключ», які враховують специфіку діяльності конкретних суб'єктів підприємництва. Зокрема, підприємства все частіше замовляють комплексні пакети послуг, які включають як моніторинг систем, так і регулярне навчання персоналу основам кібергігієни.

Подальший розвиток ринку напряму залежить як від зовнішніх, так і від внутрішніх чинників. Зовнішні фактори, такі як блекаути, енергетична криза та постійна кіберзагроза, змушують підприємства шукати інноваційні рішення. Особливий інтерес викликають хмарні технології, які дозволяють зберігати дані у віддалених центрах обробки, забезпечуючи їх безпеку навіть у разі фізичних руйнувань. Водночас вітчизняний бізнес починає усвідомлювати переваги створення резервних копій, розгортання систем відновлення після аварій (Disaster Recovery) та впровадження сучасних інструментів управління доступом.

Щодо внутрішніх ресурсів ринку, можна виокремити кілька ключових напрямів для розвитку. По-перше, це налагодження механізмів взаємодії між окремими представниками ринку, що дозволить обмінюватися досвідом, розробляти спільні ініціативи та забезпечувати швидке реагування на нові виклики. По-друге, впровадження кращих практик суміжних ринків, таких як фінансовий чи телекомунікаційний, які вже давно працюють над вдосконаленням систем кіберзахисту. По-третє, активне використання сучасних маркетингових інструментів, таких як просвітницькі кампанії для бізнесу, що покращують обізнаність про кіберзагрози, та платформи для взаємодії з клієнтами.

Список використаних джерел:

1. Смєсова В.Л. Кон'юнктурний аналіз сучасного світового ринку товарів та послуг. *Economics Bulletin*. 2022. №1. С. 62–76.
2. Cyber Security Market Size, Share, Growth, Report 2023–2032. *Precedence Research,* 2024. URL: https://www.precedenceresearch.com/cyber-security-market (дата звернення: 27.10.2024).
3. Поліщук В. Кіберзлочини та кібербезпека: боротьба з комп'ютерними злочинами і кібератаками. Наукові праці Міжрегіональної академії управління персоналом. *Юридичні науки*, 2023. Вип. 3 (66). С. 44–47.
4. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. *Державної служби спеціального зв'язку та захисту інформації України*, 2023. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti?utm_source=chatgpt.com (дата звернення: 30.10.2024).
5. Оніщенко С., Глушко, А. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Науковий журнал «Економіка і регіон»*. 2022. № 1 (84). С. 13–20.
6. Названа кількість кібератак в Україні за минулий рік. *Слово і діло Аналітичний портал,* 2024. URL: https://www.slovoidilo.ua/2024/01/31/novyna/suspilstvo/nazvana-kilkist-kiberatak-ukrayini-mynulyj-rik#google_vignette (дата звернення: 02.10.2024).
7. Бегаль І. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики. *Forbes.ua.* 2023. URL: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (дата звернення: 02.10.2024).
8. Рахман М.С., Корабельский С.О. IT-галузь України в очах світової спільноти. *Business Inform*, 2020. № 7. С. 181–188.
9. Литюга Є., Яценко В. Перспективи розвитку хактивізму та хакерських атак в сфері фінансових послуг: виклики та шляхи протидії. *Виклики кібербезпеки індустрії фінансових послуг*: матеріали наук. онлайн-конф., м. Суми, 07 вересн. 2023 / За загальною редакцією доц. Койбічук В.В. Суми : Сумський державний університет, 2023. С. 67–70.
10. Горбаченко С.А. Місце менеджменту кібербезпеки у сучасній управлінській науці та практиці. *Сталий розвиток економіки.* 2024. № 1 (4). С. 144–149. URL: https://www.economdevelopment.in.ua/index.php/journal/article/view/895/857 (дата звернення: 04.10.2024).
11. Горбаченко С.А. Особливості рекламних кампаній продуктів та послуг у сфері кібербезпеки. *Конкурентоспроможна модель інноваційного розвитку економіки України:* матеріали VII Міжнар. наук.-практ. конф., м. Кропивницький, 7–8 листоп. 2024 р. Кропивницький, 2024. С. 52–54.
12. Васильєва Н.Б., Нижниченко Я.Є., Заболотна О.С. Вплив цифровізації на трансформацію бізнес-моделей традиційних галузях економіки. *Академічні візії*. 2024. Вип. 37. С. 1–9.
13. Крижановський В.Г., Сергієнко С.П. Апаратно-програмні засоби захисту інформації у корпораціях: навчально-методичний посібник. Вінниця : ДонНУ імені Василя Стуса, 2019. 36 с.

14. Prins S. The measurement of cybersecurity awareness in an industrial control systems company. South Africa. *University of Johannesburg*, 2019. URL: https://www.proquest.com/openview/09d7ef7f621f4439904b43e60e3c496d/1?pq-origsite=gscholar&cbl=2026366&diss=y (дата звернення: 19.10.2024).
15. 10Guards. *Official website.* URL: https://10guards.com/en/?utm_source=chatgpt.com (дата звернення: 02.11.204).
16. HackControl. Official website. URL: https://hackcontrol.org/ (дата звернення: 04.11.2024).
17. Beetroot. Official website. URL: https://beetroot.co/ (дата звернення: 06.11.2024).
18. EPAM Ukraine. Official website. URL: https://careers.epam.ua/ (дата звернення: 06.11.2024).

References:

1. Smiesova V. L. (2022) Kon'unkturnyi analiz suchasnoho svitovoho rynku tovariv ta posluh [Conjunctural analysis of the modern global market for goods and services]. *Economics Bulletin*, no. 1, pp. 62–76.
2. Cyber Security Market Size, Share, Growth, Report 2023–2032 (2024). Precedence Research. Available at: https://www.precedenceresearch.com/cyber-security-market (accessed October 27, 2024).
3. Polishchuk V. (2023) Kiberzlochyny ta kiberbezpeka: borotba z kompiuternymy zlochynamy i kiberatakamy [Cybercrimes and cybersecurity: combating computer crimes and cyberattacks]. *Naukovi pratsi Mizhreihionalnoi akademii upravlinnia personalom. Yurydychni nauky*, issue 3 (66), pp. 44–47.
4. Uriadova komanda CERT-UA v 2023 rotsi opratsiuvala 2543 kiberincydenty [The government team CERT-UA processed 2543 cyber incidents in 2023] (2023). Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. Available at: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti?utm_source=chatgpt.com (accessed October 30, 2024).
5. Onishchenko S., Hlushko A. (2022) Analitychnyi vymir kiberbezpeky Ukrainy v umovakh zrostannia vyklykiv ta zahroz [Analytical dimension of Ukraine's cybersecurity under growing challenges and threats]. *Naukovyi zhurnal "Ekonomika i rehion"*, no. 1 (84), pp. 13–20.
6. Nazvana kilkist kiberatak v Ukraini za mynulyi rik [The number of cyberattacks in Ukraine last year has been named] (2024). Slovo i dilo Analitichnyi portal. Available at: https://www.slovoidilo.ua/2024/01/31/novyna/suspilstvo/nazvana-kilkist-kiberatak-ukrayini-mynulyj-rik#google_vignette (accessed October 2, 2024).
7. Behal I. (2023) U 2022 rotsi kilkist kiberatak na Ukrainu zrosla maizhe vtrychi. 90% kherkerskykh hrup z RF kontroluiut sylovyky [In 2022, the number of cyberattacks on Ukraine increased almost threefold. 90% of hacker groups from Russia are controlled by law enforcement]. Forbes.ua. Available at: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (accessed October 2, 2024).
8. Rakhman M. S., Korabelskyi S. O. (2020) IT-haluzi Ukrainy v ochakh svitovoi spilnoty [IT sector of Ukraine in the eyes of the global community]. *Business Inform*, no. 7, pp. 181–188.
9. Litiuha Ye., Yatsenko V. (September 7, 2023) Perspektyvy rozvytku khaktyvizmu ta kherkerskykh atak v sferi finansovykh posluh: vyklyky ta shliakhy protydii [Prospects for the development of hacktivism and hacker attacks in the financial services sector: challenges and countermeasures]. *Vyklyky kiberbezpeky industrii finansovykh posluh*: materialy nauk. online-konf. / Za zahalnoiu red. dots. Koibichuk V. V. Sumy: Sumskyi derzhavnyi universytet, pp. 67–70.
10. Horbachenko S. A. (2024) Mistsie menedzhmentu kiberbezpeky u suchasnii upravlinski naukiv ta praktytsi [The place of cybersecurity management in modern management science and practice]. *Stalyi rozvytok ekonomiky*, no. 1 (4), pp. 144–149. Available at: https://www.economdevelopment.in.ua/index.php/journal/article/view/895/857 (accessed October 4, 2024).
11. Horbachenko S. A. (2024) Osoblyvosti reklamnykh kampanii produktiv ta posluh u sferi kiberbezpeky [Features of advertising campaigns for products and services in the field of cybersecurity]. *Konkurentospromozhna model innovatsiinoho rozvytku ekonomiky Ukrainy*: materialy VII Mizhnar. nauk.-prakt. konf., m. Kropyvnytskyi, 7–8 lystop. 2024 r. Kropyvnytskyi, pp. 52–54.
12. Vasylieva N. B., Nyzhnychenko Ya. Ye., Zabolotna O. S. (2024) Vplyv tsyfrovyzatsii na transformatsiiu biznes-modelei tradytsiinykh haluzakh ekonomiky [The impact of digitalization on the transformation of business models in traditional industries]. *Akademichni vizii*, issue 37, pp. 1–9.
13. Kryzhanovskyi V. H., Serhiienko S. P. (2019) Aparatno-prohramni zasoby zakhystu informatsii u korporatsiiakh [Hardware and software tools for information protection in corporations]: navch.-metod. posibnyk. Vinnytsia: DonNU imeni V. Stusa, 36 p. (in Ukrainian).
14. Prins S. (2019) The measurement of cybersecurity awareness in an industrial control systems company. South Africa. University of Johannesburg. Available at: https://www.proquest.com/openview/09d7ef7f621f4439904b43e60e3c496d/1?pq-origsite=gscholar&cbl=2026366&diss=y (accessed October 19, 2024).
15. 10Guards. Official website. Available at: https://10guards.com/en/?utm_source=chatgpt.com (accessed November 2, 2024).
16. HackControl. Official website. Available at: https://hackcontrol.org/ (accessed November 4, 2024).
17. Beetroot. Official website. Available at: https://beetroot.co/ (accessed November 6, 2024).
18. EPAM Ukraine. Official website. Available at: https://careers.epam.ua/ (accessed November 6, 2024).