Огляд ринку кібербезпеки в Україні

Січень 2025

Дане дослідження проводилося DataDriven за ініціативою підкомітету з кібербезпеки ЕВА та CyberTech комітету Асоціації IT Ukraine за сприяння Аспен Інституту Київ, що реалізує Програму «Діалог про кібербезпеку», за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»

Головні партнери дослідження

USAID ВІД АМЕРИКАНСЬКОГО НАРОДУ

THE ASPEN INSTITUTE KYIV

За ініціативою

EBA European Business Association

IT Ukraine Association

Дякуємо за сприяння у підготовці матеріалу*

IO GUARDS

ASTERS

CHECKEYE

CyberLab Комп'ютерна криміналістика

DataArt

EVE.calls

EY

FSG feel secured globally

ICWR INSTITUTE OF CYBER WARFARE RESEARCH

InDev LAB

INTELLIGENT IT DISTRIBUTION

ISSP

inovo VC

molfar

osavul

seeton

uklon

UNIT.City

UVCA UKRAINIAN VENTURE CAPITAL & PRIVATE EQUITY ASSOCIATION

ZAS VENTURES

*З даними організаціями були проведені інтерв'ю при підготовці дослідження. Список надано в алфавітному порядку. Дослідження представляє позицію авторів і не обов'язково відображає позиції організацій з якими були проведені інтерв'ю чи партнерів дослідження

Визначення 1/2

Кібербезпека – це процес, спрямований на забезпечення конфіденційності, цілісності та доступності інформаційних систем, мереж, програм і даних. Вона включає заходи з управління ідентифікацію, виявленням, захистом, реагуванням та відновленням.

Огляд ринку кібербезпеки в Україні охоплює рішення для забезпечення кібербезпеки, включаючи професійні послуги, керовані послуги та продукти, що можуть охоплювати функції ідентифікації, виявлення, захисту та реагування, а також послуги з підтримки та розгортання рішень, навчання. Безперервність бізнесу та аварійне відновлення, фізична безпека та внутрішні заходи з кібербезпеки виходять за рамки цього дослідження і, відповідно, не включені до нього.

Професійні (консалтингові) послуги: це спеціалізовані послуги фахівців, спрямовані на оцінку та управління ідентифікацією, виявлення, захистом, реагування та відновленням.

Керовані послуги та продукти: забезпечують підтримку завдань в сфері кібербезпеки через спеціалізовані платформи, що виконують функції моніторингу, розвідки загроз, реагування на інциденти тощо. Вони допомагають організаціям масштабувати та автоматизувати виконання таких функцій.

Визначення 2/2

Кіберрішення – продукти або послуги, адаптовані до унікальних вимог організацій з урахуванням їхнього ландшафту ризиків і стратегій безпеки. Кіберрішення включають:

Безпека додатків	Хмарна безпека	Безпека даних	Мережева безпека	Безпека кінцевих точок	Інші рішення
Методи захисту для забезпечення безпеки комп'ютерних програм від зовнішніх загроз, експлуатації вразливостей і несанкціонованого доступу до програмного забезпечення.	Практики захисту в публічних, приватних і гібридних хмарних середовищах, спрямовані на забезпечення безпеки IT-систем, даних і додатків від кіберзагроз та ризиків витоку даних.	Заходи безпеки для забезпечення доступності, цілісності та конфіденційності чутливих даних, що включають контроль доступу та шифрування для запобігання несанкціонованому доступу і крадіжкам.	Технології та процедури, що захищають мережі від несанкціонованого доступу, зломів і саботажу даних.	Захист кінцевих точок, таких як робочі станції, сервери і мобільні пристрої, від різних атак, з використанням антивірусного захисту та сучасних рішень проти загроз нульового дня.	Додаткові рішення для управління ідентифікацією та доступом, управління ризиками, що підтримують відповідність нормативним вимогам і захищають від ризиків безпеки.

Зміст

1. Огляд Ринку

Важливість кібербезпеки зростає одночасно з технічним прогресом

Історичний контекст. Найвідоміші кіберзлочини

1962. Перша кібератака

Злиття паролів з комп'ютерної мережі MIT

1988. "Morris worm"

Атака, що зачепила бази даних NASA та Університету Стенфорда

1995. Перший злам банківської системи

Атака на Citibank, зі збитками у щонайменше 10,7 $ млн

2000. Серія DDoS-атак

Атака на сервіси Amazon, Yahoo, Ebay, CNN та ін.

2010. Stuxnet

Атака на індустріальні об'єкти Ірану, що входять до її ядерної програми

2017. WannaCry Ransomware

Кібератака на держустанови 150 країн, з можливим залученням хакерів з КНДР

2020. Злам SolarWinds

Російські хакери отримали доступ до 18000 масивів даних

2024. Атака на Royal Mail

Ransomware за можливого залучення хакерів з РФ спричинив хаос в роботі сервісу по всьому світу

Ключові факти про кібербезпеку в світі

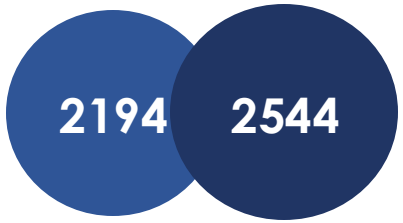
- Найчастіше під ураження потрапляють сектори **виробництва, фінансів, охорони здоров'я та цифрових послуг.**
- Найпопулярніші види кібератак: **DDoS, Ransomware, Phishing**
- **Країни, на які** здійснюється найбільша кількість кібератак: **США, Україна, Південна Корея, Китай.**

- Ринок послуг з кібербезпеки зберігає **стійкий ріст.**
- Найбільша частка ринку припадає на **США, Китай, Німеччину та Велику Британію.**
- Прогнозується ріст світового ринку до **$186 млрд** у 2024 з показником **щорічного зростання у 7,92%** до 2029 року.

Джерела: Teal, Knowledge academy, Statista, Fortra, Fortune Business Insights, Oxford University, Microsoft Digital Defence Report.

Російська кібер-агресія проти України підкреслює необхідність розвитку національної індустрії послуг та продуктів кібербезпеки

Кількість зареєстрованих кіберінцидентів в Україні:

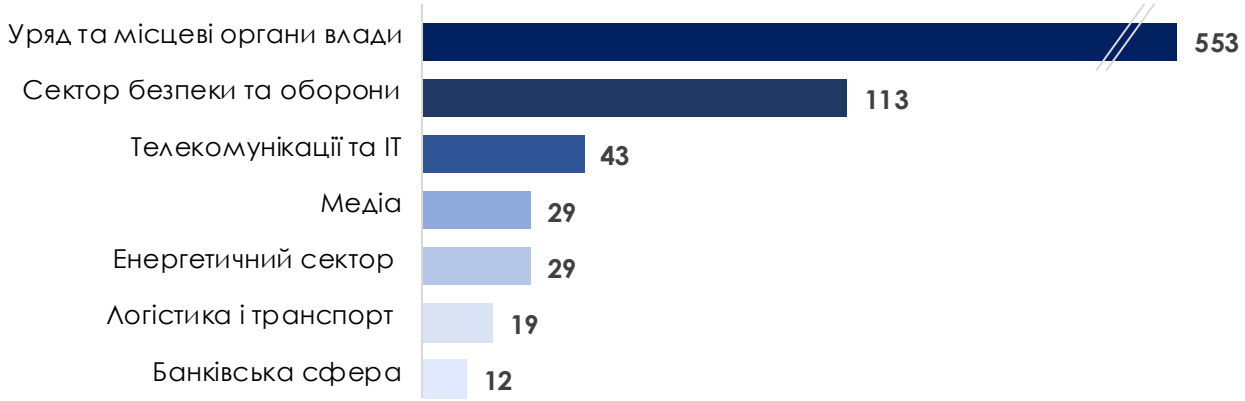


UAC-0010 (Gamaredon/ФСБ) залишається найбільш активним російським хакерським угрупованням:

- За перше півріччя 2022 року, угрупування провело **76** кібератак.
- За перше півріччя 2023 року, вони провели **94** кібератаки.

Основні сектори*:

*кількість кіберінцидентів, дані 2022 року

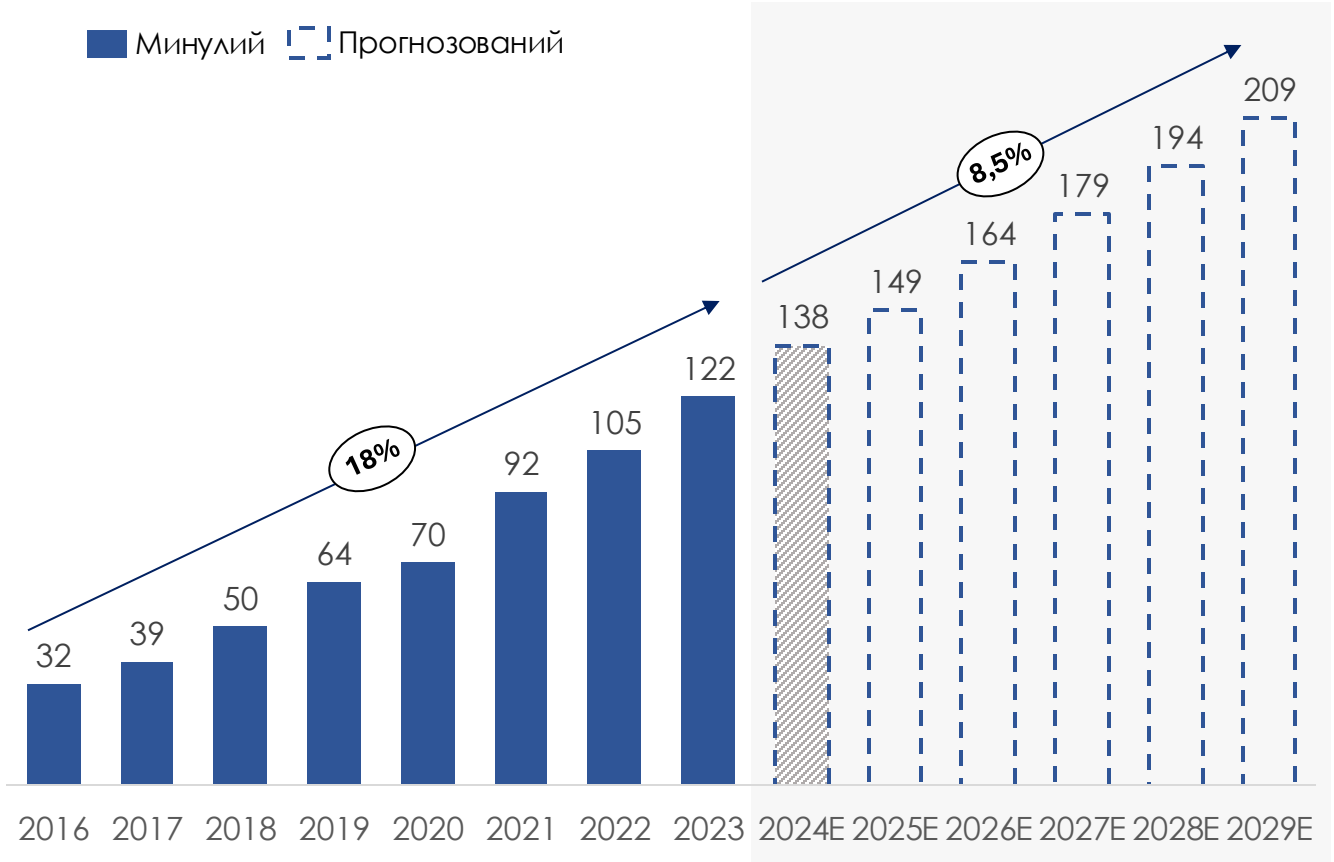


Джерела: Державна служба спеціального зв'язку та захисту інформації України, Аналіз DataDriven.

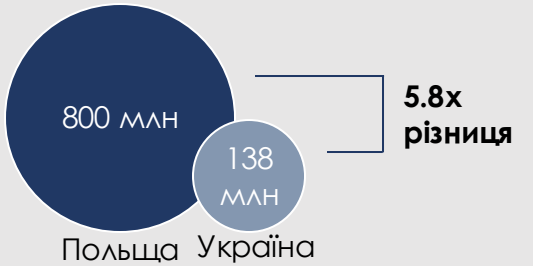
Український ринок кібербезпеки зріс у 4 рази за останні 8 років і, за прогнозами, зросте ще на 50% до 2029 року

Обсяг українського ринку кібербезпеки* 2016-2029E

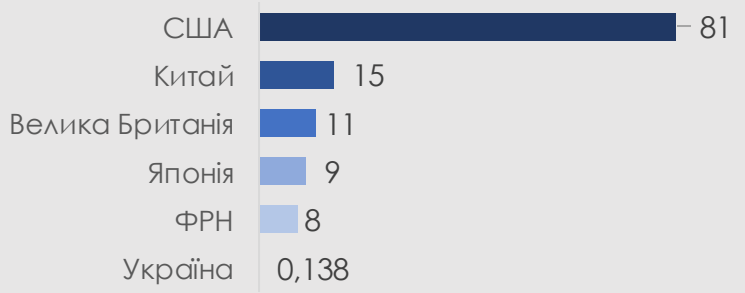
Розмір ринку, в млн. доларів США за поточним курсом, CAGR у %.



Порівняння ринку України та Польщі



Лідери світового ринку кібербезпеки, у млрд $



Частка України на світовому ринку

~0,07%

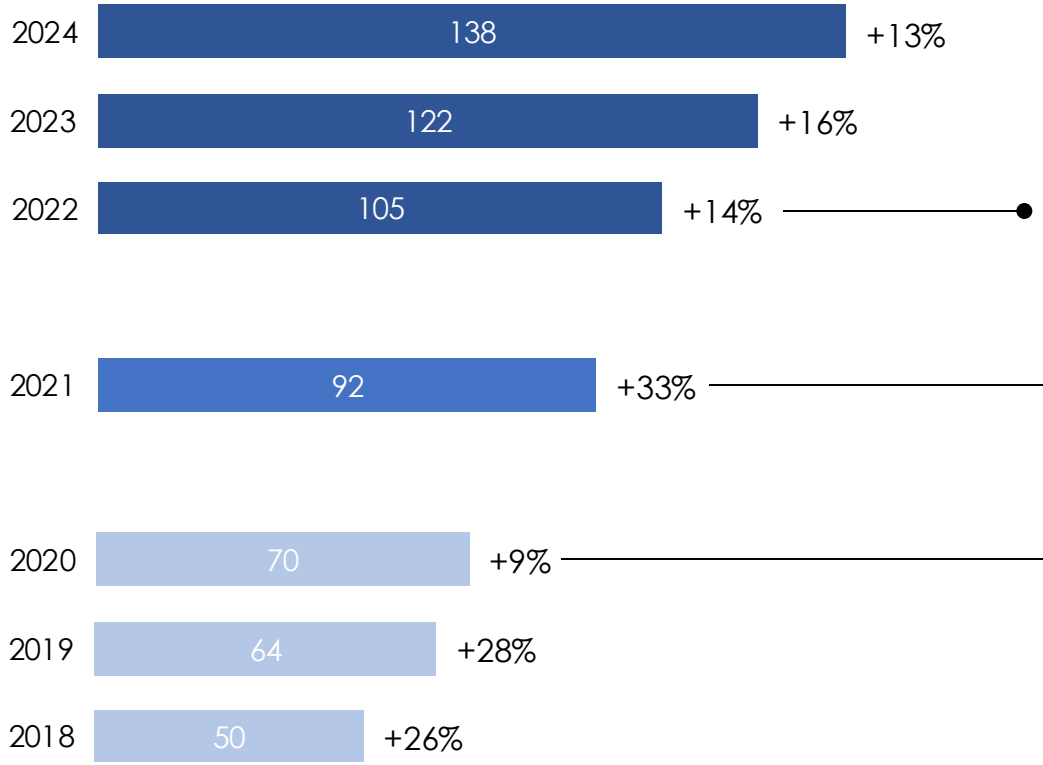
частка України на світовому ринку кібербезпеки, який, як очікується, досягне **186 млрд доларів США у 2024 році.**

*Вибірка даних враховує компанії з B2B, B2C, та B2G сегментів. Ринкова динаміка представлена очима споживачів кібербезпекових послуг і продуктів. Дані базуються на витратах компаній на кібербезпеку // Джерела: Statista, Аналіз DataDriven.

Ріст ринку кібербезпеки був неоднорідним, з періодами прискорення та сповільнення, в 2020, 2021 та 2022 роках

Щорічне зростання українського ринку кібербезпеки*

в млн. доларів США за поточним курсом



- Помірний ріст ринку у 2022 році був зумовлений релокаціями компаній та закриттями офісів, що призвели до зменшення внутрішнього попиту на кібербезпеку та сповільнення росту інвестицій.
- Держава частково задовільнила зростаючі потреби у сфері кібербезпеки за рахунок робітників держсектору та мобілізації.

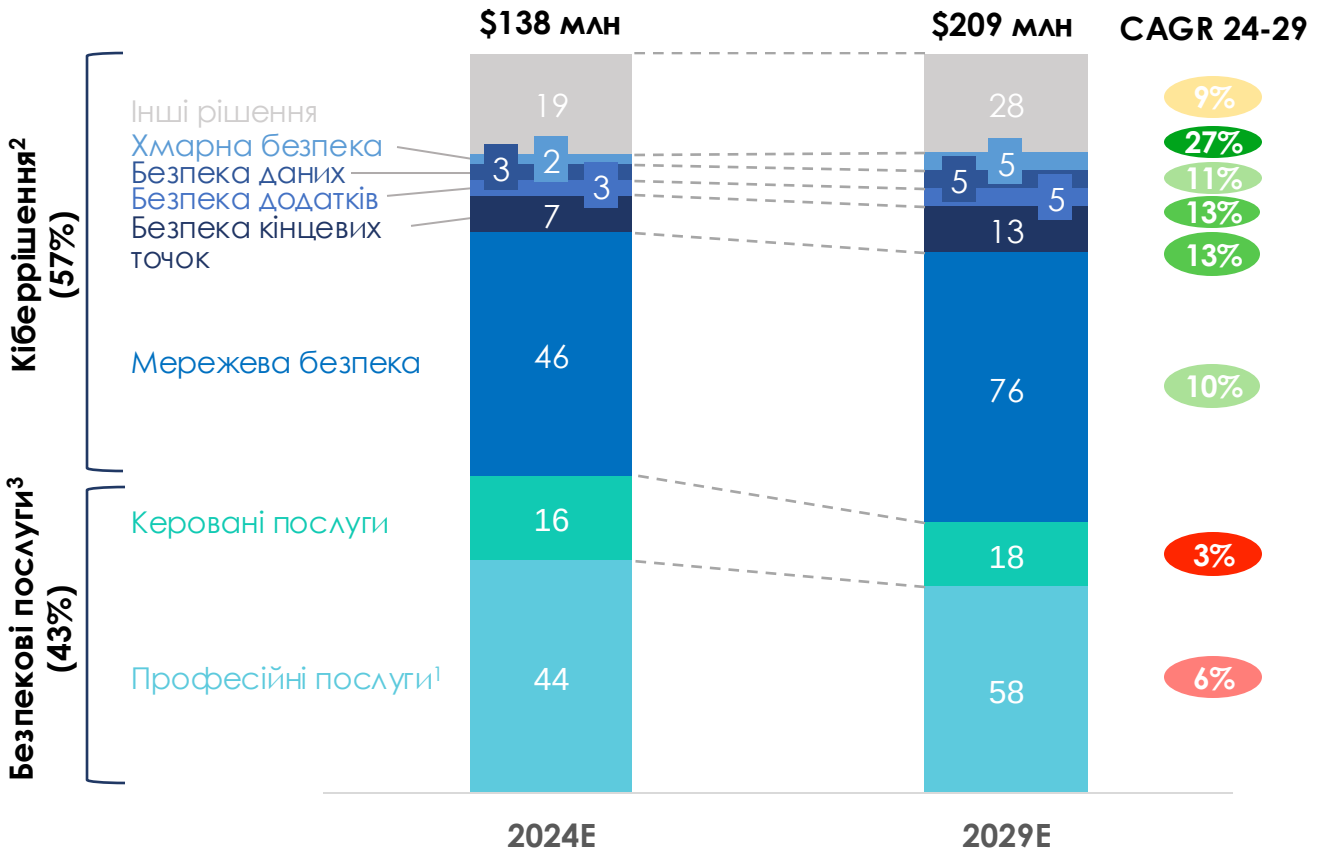
- Прискорення росту ринку у 2021 році було зумовлено зростанням кіберзлочинності, посиленням уваги до кібербезпеки та безперервною діловою активністю через реструктуризацію в умовах карантину.
- Найбільше зростання спостерігалося у сфері **хмарної безпеки (+76%)**, оскільки компанії все більше покладалися на хмарні сервіси для віддаленої роботи.

- У 2020 році, під впливом COVID-19 бізнес зіткнувся з фінансовими проблемами та бюджетними обмеженнями, надаючи пріоритет основним оперативним процесам, а не інвестиціям у кібербезпеку.
- Ресурси були перерозподілені на підтримку віддаленої роботи, що призвело до скорочення витрат на передові рішення з кібербезпеки.

* Вибірка даних враховує компанії з B2B, B2C, та B2G сегментів. Ринкова динаміка представлена очима споживачів кібербезпекових послуг і продуктів. Дані базуються на витратах компаній на кібербезпеку // Джерела: Statista, Cyber Safety Unit, Експертні інтерв'ю, Аналіз DataDriven.

Сегмент мережевої безпеки переважає на ринку, але хмарна безпека, безпека додатків та кінцевих точок швидко зростають

Розмір та зростання українського ринку кібербезпеки за сегментами
2024E та 2029E , у млн доларів США, CAGR у %.



Основні Висновки

- Хоча на світовому ринку кібербезпеки домінує сегмент безпекових послуг з часткою **53% у 2024 році**, на українському ринку переважають кіберрішення з **часткою 57%**. Це пов'язано з наступними чинниками:
  - **Підвищення частоти та масштабу кібератак**: війна збільшила кількість та складність кібератак на Україну, що призвело до швидкого впровадження автоматизованих рішень, як шифрування даних, автоматизоване виявлення загроз.
  - **Необхідність негайних рішень**: загрози масштабних кібератак, змусили компанії надавати перевагу готовим кіберрішенням над планомірним впровадженням персоналізованих рішень.
  - **Нестача кадрів:** обмеженість спеціалістів призвело до використання автоматизованих рішень, які потребують меншого втручання людини.
- **До 2029 року на світовому ринку сегмент кіберрішень** випередить сегмент безпекових послуг та стане домінуючим (**55% проти 45%** відповідно). Україна є трендсеттером, адже випереджає інші країни в кібер-експертизі завдяки роботі в R&D.

Примітки: 1.в основному аудиторські та консалтингові послуги; 2. Комплексні послуги з загального підвищення захисту компанії; 3. Окремі продукти, що відповідають конкретним потребам та ризикам в кібербезпеці // Джерела: Statista, Аналіз DataDriven.

Основними рушійними силами ринку в Україні є цифровізація та зростання ризику реальних втрат від кібератак

Всебічна цифровізація

У міру того, як бізнес та уряд впроваджують цифрові рішення, вони стикаються з підвищеним ризиком кіберзагроз, що вимагає посилення заходів кібербезпеки для захисту конфіденційних даних та забезпечення безперебійної роботи.

Ріст обсягу кібератак

Фактичне перебування у стані кібервійни є основною причиною збільшення кількості кібератак. Організації в усіх секторах стикаються з підвищеними ризиками для своєї діяльності та безпеки даних, що змушує інвестувати в передові рішення з кібербезпеки.

Зростання ризику реальних втрат

Кібератаки, такі як віруси-вимагачі, витоки даних порушують бізнес-діяльність, призводять до простоїв, і часто вимагають значних витрат на відновлення. Окрім фінансових збитків, компанії можуть зіткнутись зі зниженням доходів, репутаційними збитками та втратою довіри клієнтів.

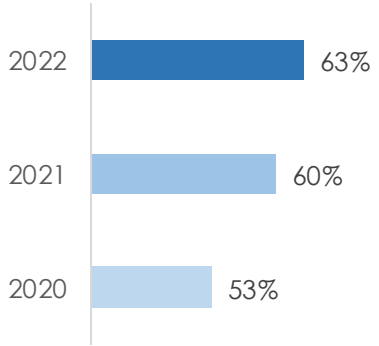
Стимулювання ринку донорами

Під час повномасштабної агресії розвиток галузі значною мірою залежить від фінансування за рахунок МТД (наприклад, проекти USAID) або прямої підтримки світовими та національними компаніями. Їх підтримка залишається критично важливою в умовах обмеженої участі держави.

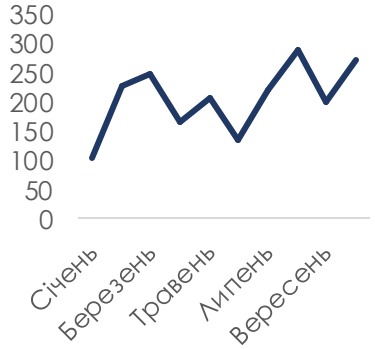
Ріст популярності ШІ

Зростання спроможностей продуктів ШІ створює можливості для здійснення кібератак нової потужності та інтенсивності і використовується для посилення заходів безпеки, дозволяючи швидше виявляти загрози, аналізувати дані і автоматизувати механізми захисту.

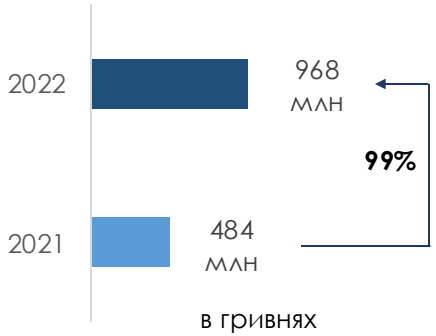
Користування цифровими держпослугами в Україні



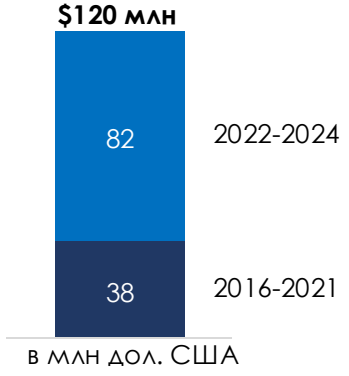
Кількість кібератак РФ на Україну в 2023 році



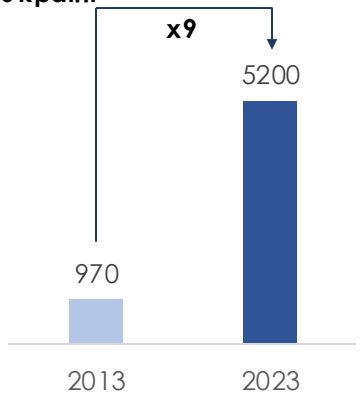
Збитки громадян України від кіберзлочинності



Допомога США Україні в кібербезпеці за 2016-2024



Кількість ШІ/ML спеціалістів в Україні

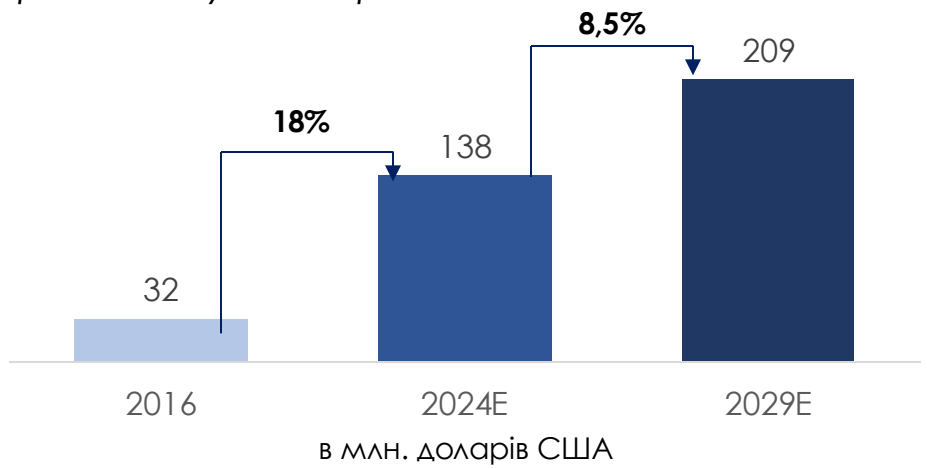


Джерела: Statista, UNDP, The AI Ecosystem of Ukraine, Дослідження ЄМА, Forbes Ukraine, Міністр Цифрової Трансформації, Експертні інтерв'ю.

Проте є очікування що ріст ринку сповільниться протягом наступних 5 років

Порівняння темпів росту ринку в Україні в минулому та майбутньому

Прогноз за умови продовження військових дій



в млн. доларів США

Очікування сповільнення росту пов'язані з:

- Зменшення фінансування з боку донорів;
- Завершення війни може призвести до зменшення очікувань настання ризиків і в сфері кібербезпеки, що буде поєднуватись із послабленою економікою та відповідно недостатністю власних фінансових ресурсів для інвестування в заходи кібербезпеки;
- Кадрова криза та дефіцит молодих фахівців в умовах воєнного стану та післявоєний період.

Головні тренди в українській кібербезпеці

Інновації

- **Штучний інтелект:** застосовується для виявлення загроз та автоматизації реагування.
- **Блокчейн:** захищає передачу даних і запобігає DDoS-атакам за допомогою децентралізованої системи перевірки.

Сегменти ринку

- **Мережева безпека** продовжить лідирувати на ринку, зберігаючи частку в 36% до 2029 року.
- **Хмарна безпека** буде найбільш швидко зростаючим сегментом завдяки гнучкості та простоті впровадження хмарних сервісів безпеки.

Частка гравців

- **Українські розробники ПЗ** зберігатимуть через об'єктивні причини відставання від міжнародних компаній за комплексністю рішень, що призводитиме до більшої залежності від міжнародних провайдерів.

Паттерни споживання

- **Принцип нульової довіри:** модель безпеки, яка передбачає сувору перевірку пристроїв і користувачів, надання мінімально необхідних прав і моніторинг поведінки при доступі до даних або послуг, що реалізується як політика в рамках цифрової інфраструктури.

Джерела: Statista, Wezom, Аналіз DataDriven, Експертні інтерв'ю.

Позитивні та негативні тенденції на ринку кібербезпеки

Сильні сторони ринку

Унікальний досвід протидії повномасштабній кібервійні
- Масові кібератаки на мережі критичної інфраструктури, телекомунікації та фінансові установи з початку російського вторгнення призвели до підвищення обізнаності в загрозах.
- Унікальний досвід України в реальній кібервійні дає цінну інформацію, якою слід ділитися з іноземними партнерами.

Зміни в цифровому ландшафті
- Тривала тенденція до цифровізації виконання функцій державного сектору, а також сервісів та бізнес-процесів приватного сектору, що призводить до постійної генерації попиту на продукти та послуги в сфері кібербезпеки.

Міжнародна матеріально-технічна допомога
- З початком повномасштабного вторгнення уряди іноземних держав підвищили свою зацікавленість у підтримці функціонування української кібербезпеки.
- USAID поставили на меті надати допомоги розміром у 38$ млн, та у 2024 надали $500 тис. прямої грантової допомоги українським ініціативам.
- Євросоюз виділив $10 млн грантової допомоги для зміцнення національної кібербезпеки у співробітництві з E-riigi Akadeemia Sihtasutus (Естонія).

Слабкі сторони ринку

Відсутність систематичного фінансування
- Несприятливий інвестиційний клімат ускладнюється воєнними ризиками та низькою обізнаністю у сфері кібербезпеки.

Фрагментація пропозиції на ринку
- Нові стартапи у сфері кібербезпеки частіше уникають співпраці з колегами та не мають тенденції до об'єднання в універсальні кластери.

Недовершене правове регулювання галузі
- Імплементація кращих практик в систему національного законодавства в сфері кібербезпеки та захисту інформації залишається точковою, що також є стримуючим фактором розвитку загальної культури кібербезпеки як приватного, так і державного секторів.
- Вимоги кіберзахисту щодо державного сектору та критичної інфраструктури, які є основними споживачами продуктів та послуг, не повністю відповідають кращим практикам, а імплементація вимог є фрагментарною.

Джерела: Аналіз DataDriven, Interfax, Forbes, Microsoft Digital Defense Report, Aspen Institute, PwC, Стратегія кібербезпеки України.

Виклики та перспективи на ринку кібербезпеки

Можливості розвитку ринку

Диверсифікація ринку

- Список сьогоднішніх викликів та інструментів реалізації кібербезпеки, як у світі, так і в Україні, не є остаточним і розширюється з розвитком цифрових технологій.
- Поступово в поняття "кібербезпека" інтегруються інформаційна і наративна безпеки та OSINT-практики, що збільшує сектор діяльності.

Перспектива збільшення попиту

- Прогрес в цифровізації є серед основних викликів та мотивом зміни підходів до управління безпекою і заходів захисту.
- Євроінтеграційний процес передбачає поступове впровадження національних і галузевих практик безпеки, норм відповідності для цифрових продуктів і послуг, що призведе до попиту більш широкого впровадження організаційно технічних заходів безпеки.

Умови для впровадження нових рішень

- Кіберзагрози воєнного часу та недовершена архітектура кібербезпеки України роблять місцеві ринки вдалими для тестування експериментальних рішень у цій сфері.
- Постачальники послуг з кібербезпеки мають можливість навчити свої продукти на унікальних даних та перевірити їх на стійкість перед найсучаснішими викликами.

Ризики для ринку

Нестача кадрів

- Зручність роботи в аутсорсі на іноземні компанії, реалії воєнного часу та довготривалий відтік талантів за кордон - ключові причини нестачі кваліфікованих співробітників у вітчизняних компаніях.
- Актуальною залишається проблема підготовки спеціалістів. Якість вищої освіти часто не відповідає потребам та викликам сучасності.

Небезпека кібератак з-за кордону

- На Україну в 2023 р. прийшлась найбільша частина спонсорованих державами кібератак у Європі.
- У час війни з Росією та політичного конфлікту з її союзниками (Іран та КНДР) завжди можливе збільшення кількості та різноманіття кібератак ззовні, особливо на критично важливі галузі економіки.

Залежність систем від забезпечення з-за кордону

- Робота цифрових систем в Україні можлива завдяки присутності на ринку закордонних виробників та постачальників.
- Український ринок має труднощі у виробництві hardware, що ставить його у вразливе положення.

Джерела: Аналіз DataDriven, Microsoft Digital Defense Report, Oxford University, Національна стратегія кібербезпеки.

2. Технології

Наступні технології забезпечуватимуть найбільший ріст ринку протягом наступних 5 років

Сегмент*	Ріст до 2029	Характеристика
Безпека хмарних сервісів	**+3,78** млн дол. або **226%**	• Сегмент, що охоплює захист середовищ та даних, розміщених у хмарі. • Прогнозується ріст поширення хмарних сервісів, при цьому зберігатиметься переважання традиційних методів зберігання даних у деяких секторах бізнесу. • Прогнозований лідер росту у відсотковому вимірі.
Безпека кінцевих точок	**+6,08** млн дол. або **85,8%**	• Сегмент розуміє під собою захист пристроїв, які підключені до корпоративної мережі. • Паралельно зі зростанням поширеності віддаленої роботи, очікується сталий ріст цього сегменту (другий показник, як у відсотковому, так і у грошовому вимірах).
Безпека мережі	**+29,4** млн дол. або **63,5%**	• Сегмент означається сукупністю заходів та потужностей, спрямованих на недопущення несанкціонованого проникнення в мережу. • Очікується послідовне зростання, котре становитиме найбільшу в кількісному вимірі частку ринку.
Інше	**+14,03** млн дол. або **58,1%**	• Серед іншого, включає безпеку додатків, даних тощо. • Прогнозується пропорційне помірне зростання, котре відбуватиметься паралельно зі зростанням використання просунутих інформаційних технологій у різних галузях бізнесу.

Примітки: * Наступні сегменти забезпечуватимуть найбільший ріст ринку (безпека хмарні сервіси – найбільший відносний ріст, безпека мережі – найбільший абсолютний ріст, безпека кінцевих точок – другий найбільший відносний ріст) // Джерела: Statista, Експертні інтерв'ю, аналіз DataDriven.

За час повномасштабного вторгнення ринок хмарної безпеки виріс втричі до 1,7 млн доларів

Обсяг ринку хмарної безпеки в Україні 2016-2029E

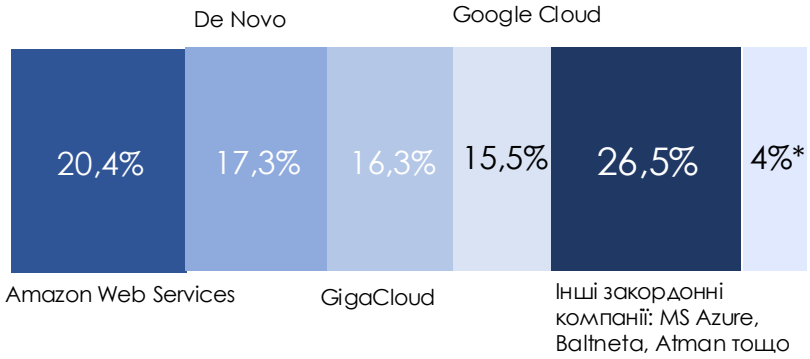
Розмір ринку, в млн. доларів США за поточним курсом

592 млрд доларів США
- витрати на публічні хмарні сервіси у світі у 2023 році.

Через імовірність пошкодження сервісів та систем підчас російського вторгнення, компанії почали перенесення IT-інфраструктури в хмарні сервіси Після початку російського вторгнення, Національний банк України дозволив фінансовим установам перенести дані та системи за межі країни, що збільшило попит на хмарні сервіси.

Поточний обсяг ринку хмарної безпеки не враховує істотні обсяги рішень, які надаються державним органам на безоплатній основі в рамках міжнародної технічної допомоги (МТД). Після закінчення військових дій та зменшення обсягу МТД державні органи перейдуть на оплату цих послуг, що призведе до зростання загального обсягу ринку хмарної безпеки

Частка компаній на ринку хмарних сервісів України у 2022 році

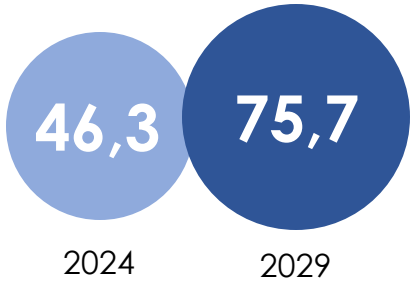


***Інші українські компанії: Ucloud, Парковий тощо**

Примітки: Міжнародна технічна допомога. // Джерела: Statista, Gartner, МтБ.

Сегменти безпеки мережі та кінцевих точок виростуть в середньому на 70% до 2029 року

Безпека інфраструктури та мережі

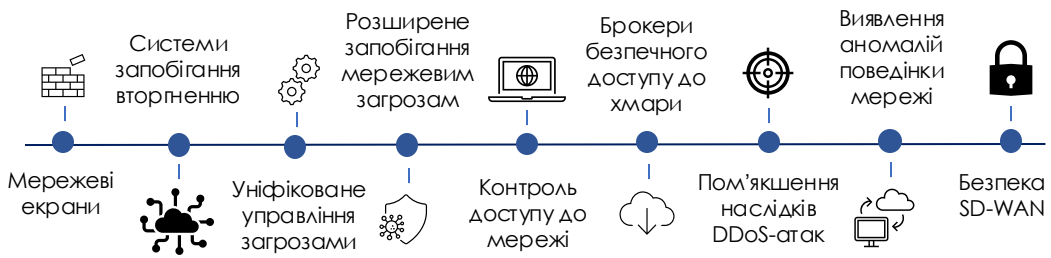


очікуваний ріст ринку мережевої безпеки в Україні, млн доларів США.

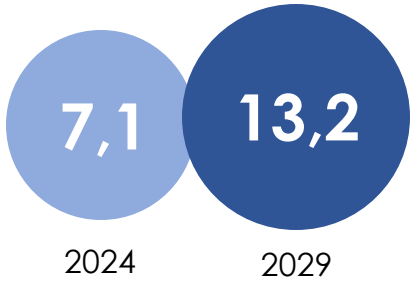
24,9 **млрд дол. США**

очікуваний обсяг світового ринку мережевої безпеки у 2024 році.

9 складових мережевої безпеки



Безпека кінцевих точок



очікуваний ріст ринку безпеки кінцевих точок в Україні, млн доларів США.

Основні гравці в Україні

Zillya! Антивірус, UnderDefense, CROWDSTRIKE, CISCO, Octava Defence, ISSP, SentinelOne, IT.Integrator

Топ-4 тренди безпеки кінцевих точок

- Еволюція технологій Zero Trust
- Використання ШІ
- Посилення захисту для віддалених працівників
- Інтеграція EDR / XDR

Ключові драйвери

- Зростання кіберзагроз.
- Цифрова трансформація та збільшення залежності від кінцевих пристроїв.
- Тенденції віддаленої роботи.

Джерела: Statista, Аналіз DataDriven.

Використання штучного інтелекту (ШІ) – одна з ключових інновацій у галузі

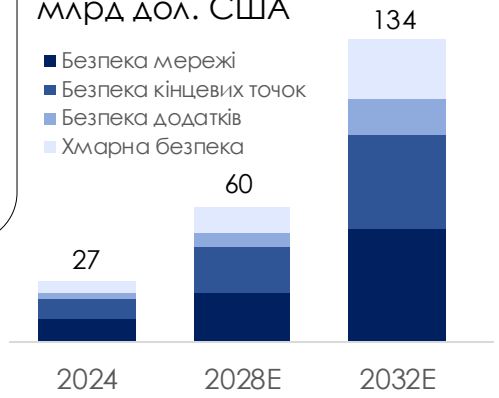
163

Розмір світового ринку ШІ в Кібербезпеці у 2033 році, млрд дол. США

Безпека мережі та кінцевих точок демонструють помітне зростання, що робить їх найбільшими сегментами на ринку кібербезпеки з ШІ.

Ринок ШІ в Кібербезпеці

млрд дол. США



В Україні наразі відсутнє спеціальне законодавство щодо ШІ, проте діє низка рекомендацій (soft law), що надають загальні орієнтири для впровадження цих технологій

Впроваджуються пілотні ініціативи (зокрема Декларація про відповідальне використання ШІ від Мінцифри). Під час євроінтеграційних процесів, зокрема і щодо впровадження регулювання ШІ у сфері кібербезпеки важливо врахувати можливість України бути конкурентноздатною, в тому числі порівняно з державою-агресором, під час впровадження та застосування таких рішень.

Ключові переваги ШІ

Автоматизація рутинних завдань
- здатний автоматично відслідковувати порушення чи аномаліїї та реагувати на них без участі людини.

Економічна ефективність
- допомагає мінімізувати людські помилки, які є однією з основних причин порушень кібербезпеки.

Пришвидшення процесу усування загроз

Основі загрози ШІ

Зростання випадків кіберзлочинів
- кіберзлочинці активно використовують AI для вдосконалення методів атак.

Залежність від точних даних
- упередженість або недостатність даних може призвести до помилкових спрацьовувань, пропущених загроз або несправедливого націлювання на певних користувачів.

Пришвидшення знаходження вразливостей нульового дня

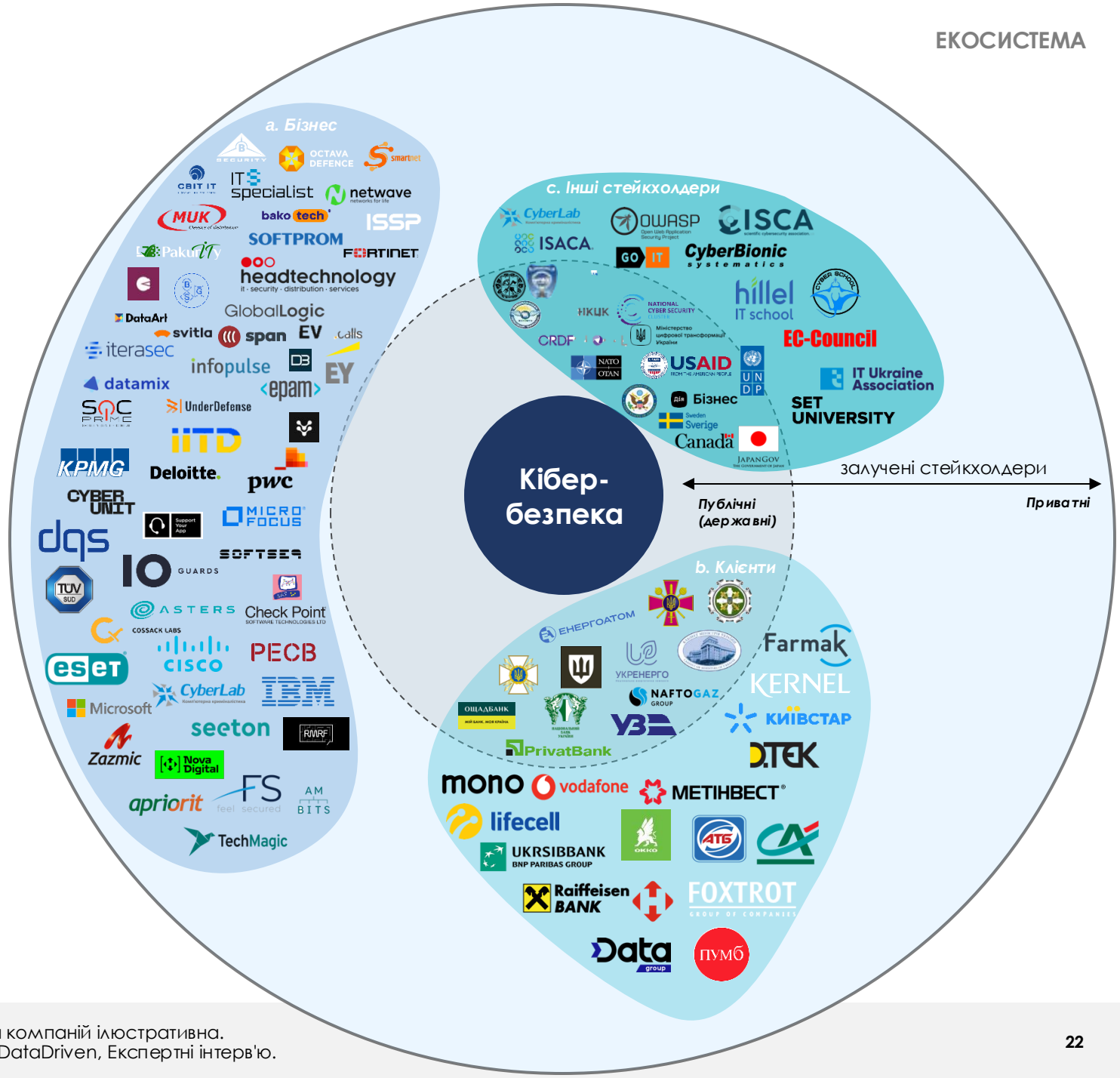
Джерела: Міністерство цифрової трансформації України, Market.US.

3. Екосистема

Головні гравці на ринку кібербезпеки

Українська екосистема кібербезпеки перебуває на стадії формування. На даному етапі, можна виділити наступні характеристики:

- **Партнерством між державою, бізнесом та міжнародними структурами:** приватний сектор взаємодіє з державою (наприклад Держспецзв'язку, НБУ, НКЦК, СБУ, МОУ) та міжнародними структурами для спільного моніторингу загроз, обміну даними, реагування, навчання.
- **Закритістю спільноти:** вітчизняний ринок кібербезпеки видається ще більш закритим та ізольований за світовий, що робить вихід на нього складним для нових гравців та стартапів.
- **Значний практичний досвід:** українські фахівці з кібербезпеки мають виняткову експертизу в захисті від DDoS-атак та інших видів кібератак, сформовану завдяки великому досвіду реагування на російську кібератрегресію. Їхній практичний досвід захисту критичної інфраструктури вигідно відрізняє їх від регіональних конкурентів.



Примітки: Вибірка компаній ілюстративна.
Джерела: Аналіз DataDriven, Експертні інтерв'ю.

Різні типи комерційних гравців представлені на українському ринку кібербезпеки

Дистриб'ютори

AXOFT, bako tech, CLICO, COREWIN, ficha, FORT SOFT, headtechnology (it · security · distribution · services), iiTD INTELLIGENT IT DISTRIBUTION, MUK Classics of distribution, Oberig it, SoftKey, Softlist, SoftOnline, SOFTPROM

Системні інтегратори

IT.Integrator, ESKA Integration, LANTEC, InDev LAB, ACCORD GROUP, CBIT IT, Winncom Technologies, B SECURITY, SIBIS, INTRA SYSTEMS, wise it, ISSP, seeton, integrity systems, netwave networks for life, AM BITS, IT-Solutions Інновації, що змінюють

Професійні послуги[2]

iterasec, a led packy, SOFTSERV, KPMG, BSG, CYBER UNIT, HackCtrl, Nova Digital, DataArt, EY, pwc, PECB, TechMagic, apriorit, EV calls, datamix, GlobalLogic, IO GUARDS, infopulse, Yalantis, CyberLab, epam, Support Your App, Deloitte., TÜV SÜD, RNB TEAM, RELEVANT, MODUS X, adaptiq, PakuriTy, ASTERS, Zazmic, astarios, UnderDefense, SOC PRIME

Вендори[3]

Малі (>50 людей)

COSSACK LABS, Evolveum, CQR, Plug the leak, PROTECTIMUS, LABYRINTH, DECEPTION, respeecher, Mantis Analytics, EVE calls, A4.tech, Cybrex, CYBERJAB, OCTAVA DEFENCE, osavul, EXTRACTOR, SET CYBER LABS, FS feel secured

Середні (50-100 людей)

Zillya! АНТИВІРУС, Syteca

Великі (100< людей)

BROADCOM, f5, Microsoft, Trellix, FORTINET, IBM, cisco, CROWDSTRIKE, TREND MICRO, eset, Check Point, paloalto NETWORKS

Примітки: 1. Вибірка компаній ілюстративна. 2. Категорія охоплює два види компаній: що надають бізнес-консалтинг (аудит, юридичне забезпечення) та технічний консалтинг (IT-рішення, внутрішні проєкти і тд.). 3. Компанії було поділено на категорії за кількістю працівників.

Ринок професійних послуг міцнішає та стає важливою частиною сфери кібербезпеки в Україні

Сегментація професійних послуг

Управління та оцінка

Включає побудови системи управління кібербезпекою, розробку і імплементацію політик, оцінку ризиків, оцінка стан, аудит, перевірка на відповідність, сертифікація, оцінювання впливу на захист даних, тощо.

Тестування та вразливості

Тестування, розвідка та аналіз загроз, управління вразливостями, аналіз захищеності кодів/веб та додатків.

Інші послуги

Включають планування реагування, управління реагуванням та розслідування, тренування та навчання, моніторинг.

Динаміка сегменту

Джерела фінансування

- Враховуючі високу частку потреб в залучені професійних послуг з боку державного сектору, головним джерелом фінансування таких послуг в Україні залишається донорська допомога.

Можливості

- Необхідність дотримання кращих практик та вимог відповідності стандартам безпеки на національному та галузевому рівні прогнозовано буде збільшувати попит на професійні послуги.
- Унікальність досвіду фахівців українського ринку може бути масштабована на міжнародних ринках.

Тренди

- Зростання попиту на залучення зовнішніх консультантів для отримання рекомендацій з метою стратегічного планування, управління ризиками та розбудови управління кіберризиками.
- Посилення вимог захисту відносно критичної інфраструктури, а також галузевих вимог відповідності.

60% з найбільших вітчизняних системних інтеграторів надають послуги з кібербезпеки

Системні інтегратори – це сервісні компанії з кібербезпеки повного циклу, які спеціалізуються на впровадженні різних технологій безпеки в єдине рішення. Вони надають комплексні послуги для забезпечення повного захисту бізнесу від кіберзагроз.

Види послуг

Розробка рішень

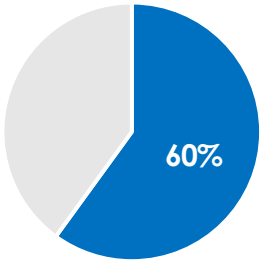
Розробка захищеної архітектури та впровадження індивідуальних рішень з кібербезпеки.

Впровадження та підтримка

Комплексні послуги від завдань до цілих проектів та обслуговування інфраструктури компанії.

Професійне навчання

Навчання з кібербезпеки для всіх рівнів кваліфікації, надаючи програми також в підгалузях.



Кількість системних інтеграторів, що надають послуги кібербезпеки з топ-35 гравців

- **Послуги, якими користуються системні інтегратори:** переважно покладаються на послуги міжнародних вендорів, таких як Cisco, IBM та Microsoft, тощо. Вони часто уникають використання вітчизняних послуг, через обмеженість функціоналу.
- **Доступність послуг:** послуги системних інтеграторів часто занадто дорогі для малих та середніх підприємств, що робить їх доступними переважно для великих компаній зі значними бюджетами.

Примітки: 1. Вибірка компаній ілюстративна.

Українським вендорам необхідно шукати конкурентну перевагу над міжнародними компаніями

На українському ринку кібербезпеки значною мірою домінують міжнародні компанії, які надають передові рішення та послуги. Дані гравці пропонують комплексні інструменти кібербезпеки, які все ширше впроваджуються бізнесом та державними організаціями по всій країні. Вітчизняним розробникам необхідно шукати конкурентну перевагу над світовими компаніями.

Розмір вендора[1]	Потреби	Приклади[2]
До 50 працівників	• Потреби щодо позиціонування та визнання. • Необхідність забезпечення стабільності портфелю клієнтів та вирішення недостатності кваліфікованого ресурсу для задоволення нових запитів. • Недостатність досвіду, що ускладнює залучення інвестицій. • Потреба в наймі більшої кількості фахівців з кібербезпеки для задоволення потреб клієнтів.	COSSACK LABS, respeecher, Plug the leak, CYBERJAB, Cybrex, LABYRINTH, Mantis Analytics, FS feel secured, PROTECTIMUS, A42.tech, osavul, DECEPTION, SET CYBER LABS, CQR, OCTAVA DEFENCE, EXTRACTOR
Від 50 до 100 працівників	• Залучення достатньої кількості кваліфікованих фахівців при масштабуванні команди: більшість компаній на ринку мають до 50 працівників • Необхідність забезпечення стабільності портфелю клієнтів. • Необхідність залучення додаткового фінансового ресурсу для забезпечення зростання. • Потреби структурування бізнес-діяльності та перегляду операційних процесів.	Zillya АНТИВІРУС, Syteca
Від 100 працівників	• Масштабування з виходом на міжнародні ринки, що вимагає збільшення розміру команд, за рахунок найму нових фахівців. • Необхідність посилення процедур відповідності регуляторним вимогам на відповідних ринках в інших юрисдикціях. • Необхідність вдосконалення та масштабування операцій для міжнародного зростання при одночасному управлінні ризиками ефективності.	

Примітки: 1. На даному слайді представлені українські вендори, зареєстровані або з кінцевими бенефіціарами в Україні. Розподіл компаній за розміром є умовним. 2. Вибірка компаній ілюстративна // Джерела: Аналіз DataDriven, Експертні інтерв'ю.

На українському ринку домінують міжнародні вендори: представлено понад 100 компаній

Примітки: Вибірка компаній ілюстративна.

Через більший асортимент рішень, дистриб'ютори в більшості співпрацюють з міжнародними вендорами

Дистриб'ютор кібербезпеки виступає посередником між постачальниками рішень з кібербезпеки та торговими посередниками, партнерами або системними інтеграторами. Вони купують продукти кібербезпеки, такі як фаєрволи, антивірусне програмне забезпечення та засоби шифрування, у постачальників і поширюють їх серед інших підприємств у ланцюжку поставок.

Види послуг

Закупівля ПЗ: закупівля рішення для кібербезпеки у міжнародних та вітчизняних постачальників, забезпечуючи клієнтам доступ до найновіших інструментів.

Логістика: займаються транспортуванням і зберіганням продуктів кібербезпеки, забезпечуючи своєчасну доставку посередникам і кінцевим користувачам.

Додаткові послуги: надають технічну підтримку, послуги з інсталяції, навчання роботі з продуктом та постійне обслуговування клієнтам.

Партнерства

Дистриб'ютори у більшості випадків співпрацюють з світовими вендорами забезпечуючи доступ до найбільш сучасних рішень для місцевого ринку.

Приклади

Виклики на ринку

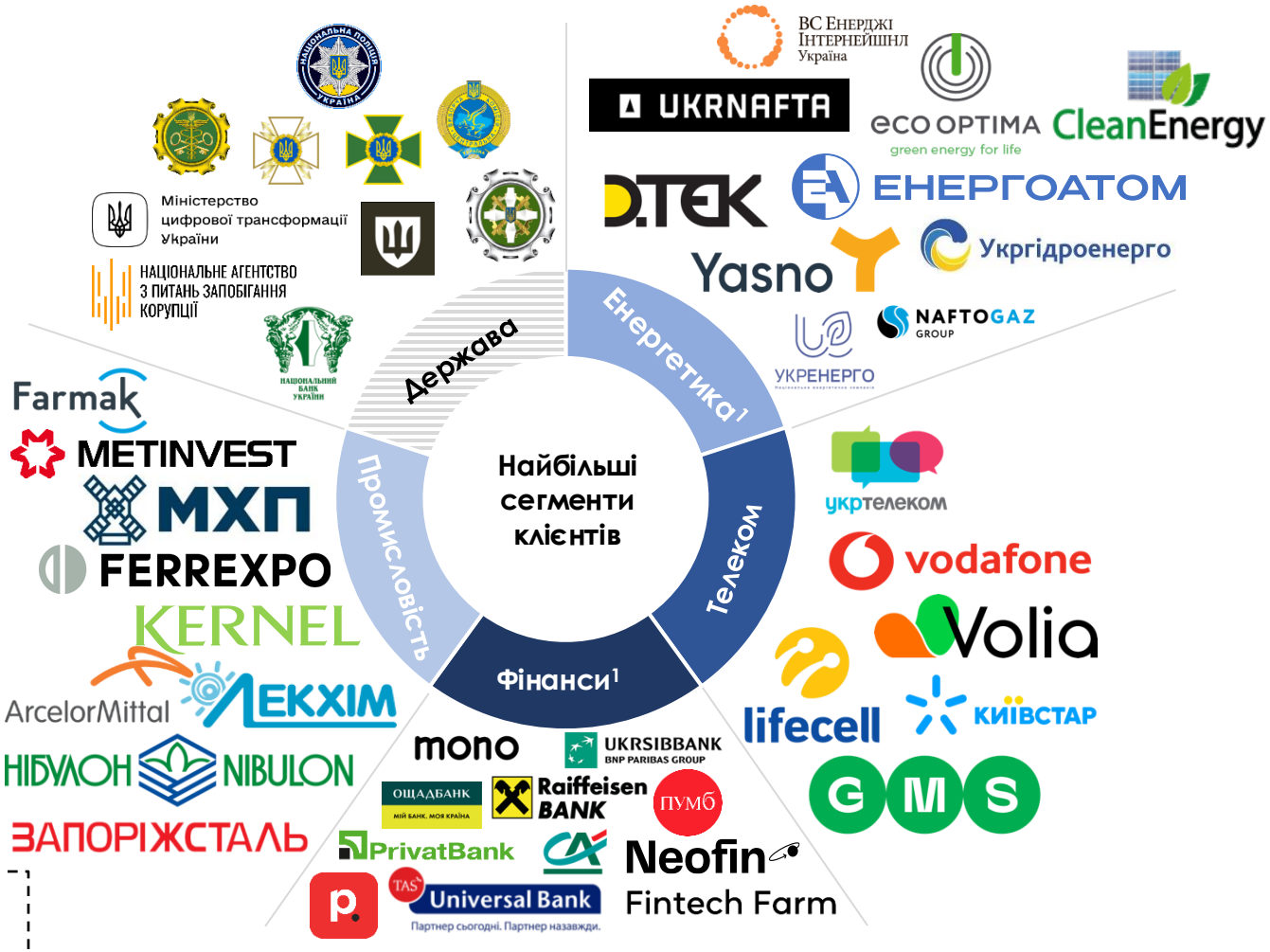
Порушення ланцюгів постачання: постійні логістичні проблеми, спричинені такими факторами, як війна в Україні, ускладнюють для дистриб'юторів забезпечення своєчасної доставки продуктів кібербезпеки.

Обмежена присутність місцевих вендорів: на ринку домінують міжнародні вендори, тому дистриб'ютори переважно мають справу з іноземними продуктами, що може обмежувати можливості вітчизняних вендорів.

Примітки: Вибірка компаній ілюстративна.
Джерела: Експертні інтерв'ю, Аналіз DataDriven.

Фінанси, телеком та енергетика – найбільші комерційні споживачі продуктів та послуг в українській кібербезпеці

- 3 червня 2022 року український бізнес зіткнувся з безпрецедентним збільшенням кількості кібератак. Серед основних цілей – **телеком, державні інформаційні ресурси, енергетика, фінанси, промисловість**.
- Кожен клієнт має унікальні потреби через характер діяльності та конкретні загрози:
  - **Фінанси:** пріоритетами є захист даних, безпека транзакцій, дотримання галузевих стандартів (наприклад, PCI DSS) та надійність захисту від шахрайства, фішингу та атак з вимогою викупу.
  - **Телеком:** пріоритетами є захист мережевої інфраструктури, запобігання DDoS-атакам, захист даних.
  - **Промисловість:** пріоритетами є захист промислових систем управління (ПСУ) і забезпечити безперервності бізнес-процесів.
  - **Держава:** пріоритетами є побудова та модернізації систем захисту, в яких обробляються державні інформаційні ресурси, в тому числі, інформація з обмеженим доступом, організаційні та технічні заходи кіберзахисту критичної інформаційної інфраструктури, вдосконалення нормативних документів для запровадження кращих практик.
  - **Енергетика:** пріоритетами є захист енергосистем і ланцюгів енергопостачання, безпека операційних технологій.



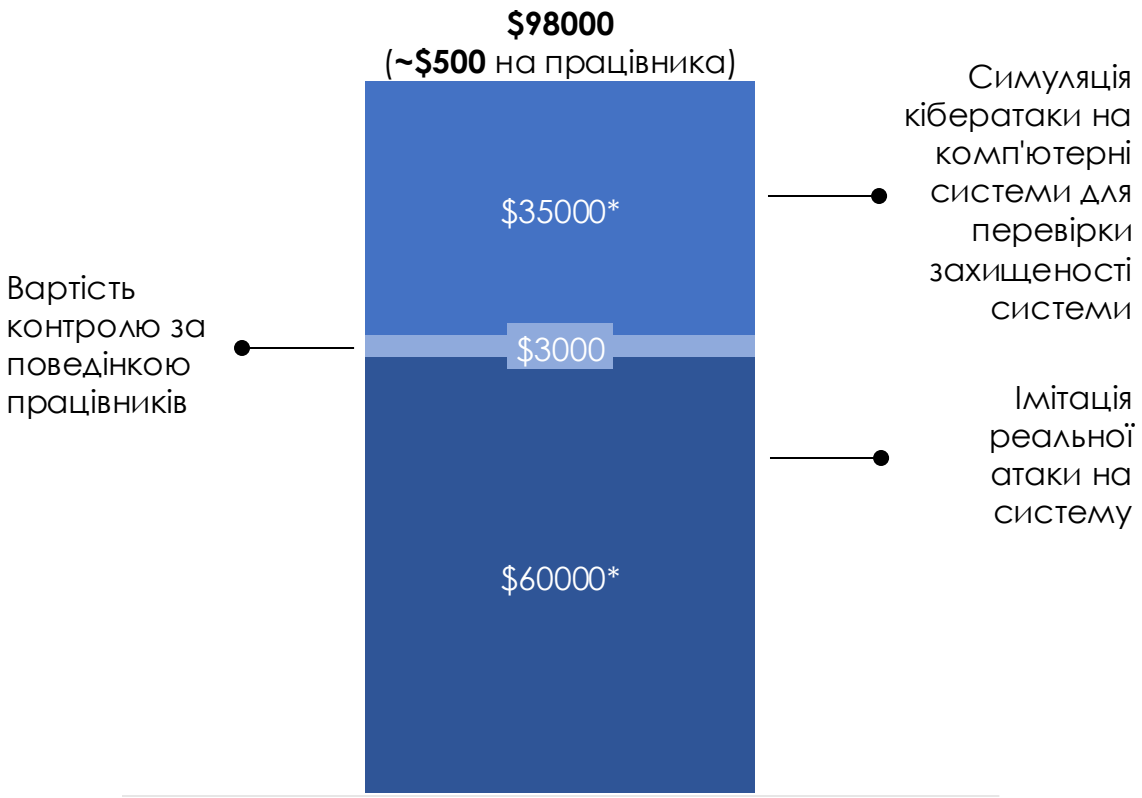
Серед всіх споживачів на ринку – найбільшу частку займає держава
На комерційному ринку[1] розподіл наступний:
1. Фінанси, 2. Телеком, 3. Енергетика, 4. Промисловість

Примітки: 1. Хоча деякі компанії за формою власності є державними (наприклад, Ощадбанк), вони діють як комерційні підприємства, тому були включені до відповідних категорій приватних гравців. 2. Вибірка компаній ілюстративна // Джерела: Forbes Ukraine, Експертні інтерв'ю, Аналіз DataDriven.

В залежності від розміру, компанії можуть витрачати від 10 до 50% свого річного бюджету на кібербезпеку

Витрати на кіберзахист компанії в Україні в 2023

(На прикладі компанії розміром в 200 працівників)



Рівень користування послугами кібербезпеки серед компаній

63% компаній користуються послугами іноземних вендорів

37% компаній працюють лише з українськими вендорами

61% замовників не отримували пропозицію співпраці від укр вендорів

% витрат на кібербезпеку з загального річного бюджету компаній

10-15% в середньому витрачають великі компанії* з свого річного бюджету на кібербезпеку

>20% в середньому витрачають невеликі компанії*, що обслуговують багато клієнтів з критичними даними

*Невеликі компанії – компанії з кількістю працівників до 50 осіб; великі компанії – компанії, що мають більше ніж 250 працівників.
Джерела: Forbes Ukraine, Експертні інтерв'ю, Аналіз DataDriven, USAID.

Класична освіта залишається об'єктом критики. Професійні практичні програмні курси заповнюють прогалини

Основні Висновки

- Незважаючи на те, що існує **55 державних університетів***, що пропонують **освітні програми з кібербезпеки** (спеціальність №125), а якнайменше **16 приватних IT-шкіл** надають спеціалізовані програми, розрив у якості між державною та приватною освітою є значним. Співвідношення державних і приватних програм **3.5:1** підкреслює, що кількість не дорівнює якості.
  - **Відсутність практичних навичок**: багато університетів не дають студентам необхідних практичних навичок з кібербезпеки, що призводить до браку практичного досвіду та спеціальних знань, необхідних у сфері кібербезпеки.
  - **Перехід до загальних IT-ролей**: через недостатню підготовку багато студентів в кінці працюють на загальних IT-ролях, таких як фронт-енд або бек-енд розробка.
  - **Приватні компанії заповнюють прогалини:** пропонують широкий спектр практичних програм та спеціалізованих курсів, практичну підготовку з кібербезпеки, з урахуванням вимог професійних стандартів та вимог індустрії.

Примітки: *до аналізу державних університетів були включені лише основні університети, без урахування їхніх філіалів.
Джерела: Експертні інтерв'ю, Аналіз DataDriven

Індустрія кібербезпеки в Україні потребує стимулювання

- Міжнародні програми допомоги, які є основним джерелом фінансування споживання продуктів та послуг в сфері кібербезпеки, в багатьох випадках надають перевагу обрання компаній зі свого національного ринку, ігноруючи наявність пропозицій на українському ринку. Продовження у великих масштабах такої політики є фактором для можливої деградації українського ринку;
- Державі доцільно прийняти програми та впроваджувати заходи, що мають забезпечувати розвиток конкурентоспроможності національної індустрії, з можливою локалізацією R&D діяльності в сфері кібербезпеки, що здійснюється в т.ч. за рахунок отримання унікальної інформації в умовах кіберагресії проти України;
- Державі доцільно не тільки декларативно визнати, а впроваджувати принцип розвитку державно-приватного партнерства як одного із пріоритетів державної політики в сфері кібербезпеки;
- Індустрії доцільно консолідувати свої зусилля через конференції, комітети, клуби для системної просування інтересів та взаємодії всіх стейкхолдерів кібербезпеки в Україні.

Асоціації[2] / Клуби

71% є членами професійних груп в соцмережах (Slack, Telegram, LinkedIn тощо)

19% входять до складу профільних робочих груп та комітетів

EBA European Business Association

NATIONAL CYBERSECURITY CLUSTER

IT Ukraine Association

ISCA scientific cybersecurity association

Конференції

63% спеціалістів беруть участь у масштабних конференціях з кібербезпеки

44% працівників сектору відвідують професійні форуми з кібербезпеки

DEFCON

REGIONAL CYBER RESILIENCE FORUM: LVIV

PCSITS

KYIV INTERNATIONAL CYBER RESILIENCE FORUM 2025

Expert Security

Примітки: 1. Вибірка асоціацій, клубів та конференцій ілюстративна. 2. Асоціації з наявними комітетами з питань кібербезпеки (EBA, IT Ukraine) теж були додані до списку. // Джерела: Berezha Security Group, Огляд ринку кібербезпеки України 2021, Експертні інтерв'ю.

Основна частина донорської підтримки припадає на державний сектор, телекомунікації та фінанси

Обсяг фінансування донорами кібербезпеки

~$200 млн

було виділено країнами-партнерами України на розвиток інфраструктури кібербезпеки в Україні.

~$120 млн

було виділено Україні від США, в тому числі через USAID, який залишається найбільшим донором в кібербезпеці.

- Донори кібербезпеки в Україні зосереджені на фінансуванні урядових ініціатив, а також бізнесу, що спрямоване на зміцнення інфраструктури кібербезпеки та захист важливих об'єктів.
- Уряд отримує підтримку для реалізації державних проектів, таких як посилення кіберзахисту та захист критичної інфраструктури, як наприклад від **USAID, уряду Великої Британії та Данії**.
- У бізнес-секторі донори спрямовують фінансування на проекти у **сфері телекомунікацій та фінансів**, які мають на меті вдосконалити рішення з кібербезпеки та забезпечити безперебійну роботу компаній.
- Хоча освіта не є першочерговим завданням, певна непряма підтримка може надаватися через державні проекти, як, наприклад, створення **Cyberlab, за підтримки ЄС**.

Грантова програма USAID на посилення кібербезпеки критичної інфраструктури

$500 тис

загальний фонд грантової підтримки, оголошений **USAID** в **вересні 2024 року** з метою реалізації ефективних рішень для зміцнення готовності та зменшення вразливості критичної інфраструктури України в кібербезпеці.

Примітки: Вибірка донорських організацій ілюстративна

4. Інвестиції

Молоді українські стартапи в галузі мають потенціал росту, особливо завдяки фокусу на послугах та МСБ[1]

Можливості фінансування для молодих стартапів

BRAVE1 UKRAINIAN DEFENSE INNOVATIONS

USAID FROM THE AMERICAN PEOPLE

USF

Українські стартапи у сфері кібербезпеки мають доступ до грантів від Brave1 на суму **від $12 000 до $194 000**, від USAID на суму **від $20 000 до $150 000** та від USF **до $35 000** для розвитку своїх ідей та початкових рішень.

Перспективні напрямки розвитку кібербезпеки

- Оскільки міжнародні вендори домінують на більшій частині ринку кібербезпеки, українським стартапам варто зосередитися на нерозвинених сегментах.
- Надання рішень з кіберзахисту для таких секторів, як **освіта, малі та середні бізнеси та громадські організації** – особливо тих, що мають обмежені внутрішні ресурси – є доступною опцією для зростання молодих стартапів.
- Орієнтуючись на ринки з низькою кількістю представлених рішень, стартапи можуть зайняти свою нішу, на якій вендори проявляють нижчий рівень активності.

Молоді українські стартапи в кібербезпеці, що мають потенціал до зростання

CYBER UNIT | SET CYBER LABS | LABYRINTH Better protection. Less complexity. More confidence. | CQR

A42.tech | DECEPTION Advanced Cyber Track | Dzerkalo Innovatins | Cybrex

CYBERJAB | LD | Plug the leak | EXTRACTOR

Примітки: 1. Малий та Середній Бізнес. 2. Вибірка стартапів ілюстративна.
Джерела: Brave1, USAID, Vector, Експертні інтерв'ю, Аналіз DataDriven.

Втім існує низка бар'єрів для інвестицій у стартапи зі сфери безпеки на пізніх стадіях

Інвестиції в кібербезпеку в Україні демонструють неоднозначні результати, з окремими успіхами, але одночасно з обмеженою активністю компаній та інвестиційним інтересом, що перешкоджають росту.

Брак інновацій у стартапах

- Більшість вендорів покладаються на вже існуючі рішення, а не розробляють інноваційні продукти.
- В Україні фактично відсутні потужні наукові центри, здатні створювати інновації високого рівня.

Складність галузі

- Галузь кібербезпеки сприймається інвесторами як високо-технічна і складна, вимагаючи спеціалізованих знань.
- Рівень профільної освіти в українських ВНЗ не відповідає вимогам часу, через що можливості молодих команд часто викликають сумнів інвестора.

Нестача спеціалізованих команд

- В Україні бракує повністю спеціалізованих команд з кібербезпеки (більшість гравців - частина ширших IT команд).
- Участь в таких стартапах є ризикованою в розумінні перспектив кар'єрного зростання.

Відсутність конкурентної переваги

- Щоб конкурувати з глобальними рішеннями, місцевим стартапам необхідно розробити унікальну конкурентну перевагу.
- В Україні не було помітних історій успіху стартапів у сфері кібербезпеки, на відміну від таких секторів, як defence-tech.

Незважаючи на бар'єри у секторі, є приклади успішних стартапів з залученням капіталу від інвестиційних фондів

Osavul – це стартап, що позиціонує себе як представників сектору "information / narrative security" , заснований у лютому 2022 року. Платформа обслуговує клієнтів у п'яти країнах, аналізує текстові, відео- та аудіодані на веб-сайтах і в соціальних мережах для виявлення онлайн-загроз. Компанія також планує розширити свою діяльність з ринку B2G на ринок B2B.

Фінансування

$1 млн	SMRK VC Fund
$3 млн	SMRK VC Fund, 42 CAP, u.ventures

Mantis Analytics - це стартап, що домагає організаціям безпечно масштабуватися за допомогою штучного інтелекту. Платформа надає **ситуативну обізнаність** та **захист активів**, дозволяючи контролювати ризики в режимі реального часу. Продукт **Mantis Incident Feed** допомагає збагачувати дані користувачів для виявлення загроз.

Фінансування

$240 тис	uklon
$50 тис	ZAS VENTURES
$30 тис	

SOC Prime – заснований українцями стартап у сфері **виявлення кіберзагроз**. SOC Prime пропонує маркетплейс рішень для детекції загроз («Spotify для кібербезпеки»), що дозволяє організаціям знаходити та впроваджувати необхідні захисні механізми. Розробники монетизують свій контент, а клієнти отримують доступ до інноваційних продуктів.

Фінансування

Пул інвесторів у Серії А ($13 млн)

dnx ventures, Rembrandt Venture Partners, streamlined, Atlantic Bridge

Стартап з українськими засновниками, Україна ж займає ~1% від продажів

* Soc Prime був заснований та в період з 2015 по 2021 базувався в Україні, але після отримання фінансування Серії А провів релокацію до США.
Джерела: AIN, Osavul, Forbes Ukraine, Експертні інтерв'ю, Аналіз DataDriven.

5. Про Нас

DataDriven надає дослідницькі та консалтингові послуги, що допомагають працювати на українському ринку

DataDriven це консалтингова агенція широкого профілю…

Дослідження

Використовуючи наш багаторічний досвід у збиранні, аналізі та інтерпретації даних, а також у створенні рекомендацій для державних і приватних стейкхолдерів.

Консалтинг

Застосовувати глибокі знання української політики та бізнесу на користь наших клієнтів. Прокладати шлях для світу до України, а українським підприємствам - до світу.

…з експертизою щодо технологій подвійного призначення…

Наші публічні дослідження включають:

- **Комерційний ринок гуманітарного розмінування в Україні** (Квітень *2024*)

- **Український ринок дефенс-тех** *(Вересень 2024)*

- **Вплив українських морських безпілотників на бойові дії на морі** *(Жовтень 2024)*
- **Штучний інтелект в процесах розмінування** *(Готується, 2025)*

…працює з широким спектром клієнтів:

Виробники обладнання
(вихід на ринок, сприяння партнерству, оцінка ризиків, комплексна перевірка постачальників)

Інвестиційні фонди
(комплексна юридична перевірка, розуміння ринку, підтримка портфоліо)

Стартапи
(розширення, валідація технологій, доступ до фінансування)

6. Джерела та Методологія

Загальна методологія

Основні джерела інформації

- Публічні джерела, такі як офіційні портали державних установ та відомств
- Офіційно опубліковані матеріали публічних досліджень
- Авторитетні українські та міжнародні ЗМІ
- Коротке опитування DataDriven, проведене серед гравців на ринку
- Інтерв'ю з інвесторами, стартапами та іншими стейкхолдерами галузі

Підхід до інтерв'ю

- Інтерв'ю включали як конфіденційні, так і публічні розмови з інвесторами, командами стартапів та незалежними експертами
- Інтерв'ю доповнювалися базовими анкетами, які розповсюджувалися через прямі контакти з представниками та галузевими асоціаціями.

Підхід до прогнозування

- Аналіз даних дозволив нам перетворити набір статистичних даних на кваліативну оцінку.
- При цьому ми взяли до уваги широкий спектр ринкових тенденцій, які можуть вплинути на розвиток ринку в різні часові проміжки.
- Особливу увагу було приділено інтеграції інсайдів від широкого кола опитаних стейкхолдерів, які наразі формують ринок.

Методологія оцінки розміру ринку та екосистеми

	**Джерела та дані**	• **Розмір ринку кібербезпеки України**: Statista • **Розмір сегменту кіберрішень в Україні:** Statista • **Розмір сегменту безпекових послуг в Україні:** Statista • **Розмір світового ринку кібербезпеки:** Statista • **Розмір ринку кібербезпеки Польщі:** Statista
	**Методологія**	• **Оцінка розміру ринку:** – **Вибірка даних**: враховує компанії з B2B, B2C, та B2G сегментів. Дані базуються на витратах на компаній на кібербезпеку (без урахування ПДВ та кількості кібератак). – **Моделювання розміру ринку**: top-down підхід – оцінюється загальний розмір ринку, починаючи з макрорівня, використовуючи дані з світового ринку, які подальшому проектуються на місцевий ринок; bottom-up підхід – будується розмір ринку, агрегуючи дані від окремих компаній та сегментів місцевого ринку. Основні джерела включають фінансову звітність провідних компаній, національну статистику та дані організацій, що займаються питаннями безпеки, а також специфічні для країни показники, такі як ВВП та рівень проникнення Інтернету. – **Прогнозування:** застосовуються різноманітні методи прогнозування (наприклад експоненційне згладжування, ARIMA) з використання таких показників, як ВВП, кількість користувачів Інтернету та рівень цифровізації. – **Валюта:** використовується поточний обмінний курс згідно з НБУ. • **Оцінка екосистеми:** – **Українські вендори:** компанії в сфері кібербезпеки у разі наявності офіційної юридичної реєстрації в Україні або наявності українських бенефіціарів. – **Міжнародні вендори:** компанії в сфері кібербезпеки, які не підпадають під вищезазначені критерії, але надають власті послуги в Україні за посередництва дистриб'юторів чи системних інтеграторів.

Це дослідження підготовлене виключно з метою ознайомлення із ринком кібербезпеки в Україні і не є інвестиційною порадою або рекомендацією до прийняття будь-яких фінансових чи інвестиційних рішень. Інформація, представлена у звіті, може бути неповною або змінюватися з часом. Перед прийняттям будь-яких інвестиційних рішень ми рекомендуємо звернутися до професійних інвестиційних або фінансових експертів для отримання більш детальних порад і оцінки ризиків.

office@datadriven.group

DataDriven | Research & Consulting

Kyiv Paris London