СТАН ГЛОБАЛЬНОГО РИНКУ КІБЕРФАХІВЦІВ У 2024 РОЦІ: ОСНОВНІ ЦИФРИ ТА ТЕНДЕНЦІЇ

ЗМІСТ

ВСТУП

Людський фактор у традиційній кібербезпековій тріаді технології, процеси, люди залишається домінуючим, адже його слабкість може нівелювати будь-який з двох інших. Добре навчені, підготовлені та мотивовані кіберфахівці є запорукою кібербезпеки будь-якої організації, а в ширшому контексті – однією з запорук безпеки країн у сучасному цифровому світі.

Між тим загрози від кібератак зростають і стають все більше вартісними за наслідками для організацій. Середня пряма вартість злому у 2024 році становила 4,88 мільйона доларів США, а середня вартість інсайдерської зловмисної атаки ще вище – 4,99 мільйона доларів. Середнє збільшення поточних витрат після порушення становить приблизно 830 000 доларів США. Ці цифри ілюструють фінансові ризики, які можуть бути пом'якшені завдяки поліпшенню ситуації з кіберперсоналом в організаціях.

Аналітичні організації по всьому світу роблять регулярні дослідження ринку кіберфахівців та формулюють тренди розвитку для цієї сфери, а також рекомендації, які можуть використати як приватні компанії так і державні органи аби поліпшити ситуацію в цій сфері. Все частіше ці дослідження звертаються і до суміжних тем, таких як залученість до сфери кібербезпеки вразливих груп чи глобальних факторів, які впливають на динаміку цього ринку. Частиною питання є і те, кого взагалі варто віднести до когорти кіберфахівців - все частіше в якості основи таких досліджень виступає NICE Framework який пропонує 52 робочі ролі для визначення того, хто відноситься до спеціалістів у сфері кібербезпеки. Водночас Національний науковий фонд США (NSF) спільно з Національним центром науки та інженерної статистики (NCSES) пропонують дивитись на це питання ширше, виокремлюючи щонайменше три великі категорії працівників:

- ядро кіберфахівців, що включає в себе як безпосередньо кіберфахівців чиї обов'язки відповідають NICE Framework, так і первинних та вторинних кіберфахівців (посади, де кібербезпека не є центром діяльності, але імманентно їй притаманна: юристи в сфері кібербезпеки, IT фахівці, менеджери баз даних тощо)
- працівники залучені до сфери кібербезпеки (посади, де кібербезпека має істотне значення для діяльності, але не є її фокусом: бізнес та фінансові операції, захисні служби, різноманітні інженери)
- суміжна робоча сила (кібербезпека не є предметом діяльності, або для ефективного виконання завдань потрібні окремі навички з NICE Framework)

В 2024 році з'явилось щонайменше чотири великих дослідження, які стосуються сфери кіберпраці та які дають нам краще уявлення про те, яким був цей ринок у 2024 році, з

якими викликами світ стикнеться у наступні періоди та що організації та країни можуть зробити аби поліпшити тут ситуацію.

- ISC2 "Cybersecurity Workforce Study"[1]
- Worl Economic Forum "Strategic Cybersecurity Talent Framework" (White Paper)[2]
- Global Cybersecurity Forum. "Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap"[3]
- ISC2 Women in Cybersecurity Report (звіт базується на даних 2023 року)[4]

Мета цього огляду – дати узагальнений погляд на ринок кіберфахівців у 2024 році, з акцентом на ключові тенденції та окремо описати фактор жінок в кібербезпеці.

Слід враховувати, що ключовий індикатор всіх звітів – показник дефіциту робочої сили . Під дефіцитом мається на увазі різниця між кількістю кіберфахівців які потрібні організації для належного кіберзахисту та фактичній доступності кіберфахівців на ринку праці. Однак варто враховувати, що дефіцит кадрів у сфері кібербезпеки часто обговорюють у таких термінах, як дефіцит навичок або дефіцит робочої сили , які використовуються як синоніми, незважаючи на їхні відмінні нюанси. Ця неточність іноді призводить до плутанини щодо конкретного типу дефіциту, з яким стикається галузь, і тих дій, які необхідних для вирішення проблем. Нестача робочої сили підкреслює загальний дефіцит професіоналів, кваліфікованих для будь-яких кіберпосад, тоді як розрив у навичках стосується розриву між навичками, які потрібні організаціям, і тими, якими зараз володіє робоча сила.

КІЛЬКІСТЬ АКТИВНОЇ РОБОЧОЇ СИЛИ

Загальна оцінка ринку кіберфахівців (тобто їх поточної кількості) у 2024 році істотно різниться. Нижче наведено оцінки двох різних звітів - ISC2 та Global Cybersecurity Forum з цього питання:

1. https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen
2. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf
3. https://web-assets.bcg.com/61/d3/705fbd684d70b0e5f98cdcf7cf47/2024-cybersecurity-work-force-report.pdf
4. https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Inclusion-Advance-ment-Pay-Equity

Регіон	ISC2	Global Cybersecurity Forum
Азіатсько-Тихоокеанський регіон	997 068[5]	2 932 534
Північна та Південна Америка	2 728 780	2 423 654
Європа	1 300 023	1 449 458
Африка	431 302	297 667
Всього	**5 457 173**	**7 103 313**

Оцінки ISC2 вказують на те, що розмір активної робочої сили з кібербезпеки у порівнянні з 2023 рік зріс неістотно – на 0,1%. Загальна ж кількість робочої сили, необхідної для задоволення попиту становить близько 10,2 мільйонів кіберфахівців в усьому світі – за останній рік цей показник зріс на 8,1% порівняно з попереднім роком.

Зростання Глобальних центрів можливостей (GCC)/Спільних сервісних центрів (SSC) також змінює глобальну робочу силу з кібербезпеки. Такі центри, які відіграють важливу роль у визначенні стратегічного напряму, покращенні управління та впровадженні принципу безпека за замовчуванням (security and safety by design). Особливо такі центри популярні в таких країнах як Індія, Мексика та Бразилія, що дозволило їм залучити більшу кількість кіберфахівців.

ДЕФІЦИТ КІБЕРФАХІВЦІВ

У 2024 році фахівці з кібербезпеки зіткнулися з низкою проблем, які вплинули на ролі та обов'язки в організаціях усіх типів. Економічний тиск, глобальні геополітичні проблеми, збої в ланцюжку постачання, невдалі оновлення програмного забезпечення та підвищення рівня автоматизації та цифровізації завдань кібербезпеки привернули увагу до критично важливої для бізнесу природи кібербезпеки та дозволили професіоналам продемонструвати свої навички та досвід із захисту організацій. Однак, незважаючи як на очевидну потребу, так і на визнання цінності, яку кібербезпека додає організаціям, глобальна активна робоча сила в кіберпространстві зупинилася на рівні 5,5 мільйонів людей. У таких країнах як Німеччина, США, Канада, та Великобританія кількість кіберфахівців навіть зменшилась – в середньому на 3%, в т.ч. як Саудівська Аравія, Південна Африка, Нідерланди демонструють зростання на 8-10%.

При цьому фактичний дефіцит робочої сили зростає, але дані щодо обсягів цього зростання відрізняються. Global Cybersecurity Forum вважає, що у сфері кібербезпеки у всьому світі не вистачає 2,8 мільйона спеціалістів (при чому найбільше – у Азіатсько-

5. Методологія ICS2 прямо вказує на те, що Китай та Індія були виключені з дослідження оцінки робочої сили через відсутність надійних вторинних джерел, однак були враховані при оцінці дефіциту робочої сили.

Тихоокеанський регіон на який припадає більше ніж 1,6 млн. такої нестачі або 56% від загального дефіциту), в т.ч. як ISC2 дає істотно більшу цифру - 4,8 мільйона в усьому світі (зростання на 19% порівняно з минулим роком). Цей розрив характерний майже для всіх країн, особливо тих, де економіки розвиваються – Південна Корея (за останній рік розрив зріс на 77,9%), Австралія (71,3%), Індія (35,9%).

У розрізі галузей дефіцит найбільше стосується чотирьох з них: фінансові послуги, матеріали та промисловість, споживчі товари та технології. Це логічно, зважаючи на те, що вони є ціллю приблизно 70% усіх глобальних кібератак.

СУПЕРЕЧЛИВІ РЕАКЦІЇ ОРГАНІЗАЦІЙ НА ПРОБЛЕМУ

Організації усвідомлюють цю проблему, намагаючись збільшити витрати на кібербезпеку – наприклад у 2024 році організації по всьому світу інвестували майже 200 мільярдів доларів на рік у продукти та послуги кібербезпеки. При цьому 39% кіберфахівців вказують на брак бюджетів на кібербезпеку, 25% спостерігали збільшення кількості звільнень фахівців (на 3% більше, ніж у 2023 році), а більше третини (37%) відзначили додаткове скорочення бюджетів на кібербезпеку (+7% порівняно з 2023 роком). Близько 64% респондентів опитування вказали, що основною проблемою при заповненні посад у сфері кібербезпеки є відсутність кваліфікованих кандидатів, а 47% респондентів вказали на високий попит на фахівців (а відтак і конкуренцію з боку інших організацій) як фактор із слабкими заповненням вакансій.

Все це позначається і на чинних працівниках: традиційно високий рівень задоволеності роботою в секторі кібербезпеки знизився на 4% по відношенню до попереднього року, проте все ще залишається на відмітці 66% задоволення своєю роллю.

При цьому спостерігається і інша тенденція - кількість нових оголошень про роботу в сфері кібербезпеки скорочується. Так, в порівнянні з минулим роком, у США кількість таких оголошень скоротилася на 5,4%, в Сінгапурі на 4,9%, у Франції на 4,5%, в Канаді на 3,5% і в Бразилії на 2,5%. Зменшення кількості оголошень про роботу підтверджується різними дослідженнями (в т.ч. ISC2), які також показують, що за останній рік команди з кібербезпеки спостерігали скорочення можливостей найму та просування по службі. Це парадоксальна ситуація, коли усвідомлення проблеми веде до протилежних практичних кроків з боку компаній. Ця ситуація може бути додатково пояснена одним з факторів, який прямо не згадується в звітах але часто визначається кіберфахівцями – керівництво організацій часто надає перевагу вкладенню коштів у технології кібербезпеки, аніж в фахівців, вважаючи, що закупка та встановлення

сучасних технологічних рішень саме по собі збільшує захист організацій, що в багатьох випадках має діаметрально протилежні наслідки.

ЕФЕКТИВНІСТЬ КОМАНД ТА ЗАТРЕБУВАНІ НАВИЧКИ: ЧИ ГОТОВІ ОРГАНІЗАЦІЇ ТА КІБЕРФАХІВЦІ?

74% респондентів відмітили, що поточний ландшафт загроз є найскладнішим за останні п'ять років – зростають самі загрози, їх види, з'являються нові фактори, які істотно змінюють ситуацію. Наприклад, новітні технології, такі як GenAI, пропонують одночасно і величезні переваги, і становлять нові серйозні ризики для організацій. Організації, які ефективно використовують GenAI, можуть отримати до 30% збільшення операційної ефективності, звільняючи людські ресурси для зосередження на більш складних і стратегічних викликах безпеки. Однак ті самі функції, які роблять GenAI потужним інструментом захисту, також становлять серйозні ризики, якщо їх використовують зловмисники.

При цьому більше третини (34%) респондентів назвали навички в сфері ШІ найбільшим недоліком навичок у командах. Далі йдуть хмарні обчислення (30%), нульова довіра (27%), реагування на інциденти (25%), безпека додатків і тестування на проникнення (по 24%).

Опитування намагались виявити і сфери, де спостерігаються найбільш складна ситуація з кіберфахівцями. Майже абсолютним лідером виявилась сфера освіти - 96% респондентів повідомляли про недоліки в навичках їх служби безпеки. Далі йдуть 94% у будівництві та охороні здоров'я, 93% у сфері нерухомості, 92% у некомерційних, аерокосмічних, телекомунікаційних і науково-дослідних секторах, а також у готельному секторі, подорожах та державному секторі (92%). Однак загалом цей показник для більшості сфер не опускається нижче 83% тобто це не означає, що в цих галузях ситуація катастрофічна по відношенню до інших (що не відміняє загальну проблему з високими показниками).

Дискусійною є ситуація і з навичками. Все ще спостерігається значна відмінність у розумінні важливості тих чи інших навичок з боку самих кіберфахівців та HR служб які здійснюють залучення цих фахівців. Наприклад, хоча професіонали приділяють значну увагу комунікаційним навичкам (31%), навичкам хмарних обчислень (30%), ШІ (23%) і GRC (19%), менеджери з найму не так високо цінують ці навички – для них важливішими виявляються комунікаційні навички та в сфері хмарних обчислень (25%), в т.ч. як навички ШІ мають лише 12% пріоритетності, а GRC (Governance, Risk Management та Compliance) – 13%.

Однак це не лише проблема невірного розуміння HR службами кібербезпекових пріоритетів організацій – це більш загальна тенденція характерна для всього ринку. Опитані керівники кіберпідрозділів різних організацій вказують на те, що найбільш значні прогалини є в навичках у таких сферах, як лідерство в кібербезпеці (є проблеми з конвергенцію навичок кібербезпеки та ділової хватки яку важко знайти серед наявних кадрів), мережева безпека (попит на ці навички підвищується через потребу в кандидатах із попереднім досвідом IT, що робить цю прогалину особливо складною), архітектура безпеки та хмарна безпека (витрати на хмарні технології становитимуть 58% витрат на IT у 2027 році, однак 44% організацій вже зараз повідомляють, що їм важко знайти потрібну експертизу) – всі ці тенденції будуть зберігатись актуальними протягом наступних 5 років.

ВІДСУТНІСТЬ СИСТЕМНОГО НАВЧАННЯ ТА МОЛОДИХ ФАХІВЦІВ

Майже одна третина (31%) учасників заявили, що в їхніх командах безпеки немає професіоналів початкового рівня, а 15% сказали, що не мають професіоналів молодшого рівня (1-3 роки досвіду). Хоча присутність професіоналів початкового та молодшого рівня в службах кібербезпеки дійсно збільшується з розміром організації, однак загалом це означає, що існує значна частка організацій, які не мають у своєму штаті професіоналів наступного покоління, яких можна розвивати відповідно до конкретних потреб організації в кібербезпеці та які можуть вчитися у своїх більш досвідчених колег, перш ніж вийти на пенсію або перейти.

Але і процес інвестування в освіту теж стикається із суперечливими баченням керівництва організацій.

Загалом є розуміння того, що інвестування в культуру безперервного є стратегічно важливим. Більше половини респондентів заявили, що підвищення кваліфікації кіберфахівців для їх більшої готовності до викликів майбутнього, вимагає сприяння культурі безперервного, а не просто періодичного, навчання. Організації все частіше віддають пріоритет професійному розвитку співробітників, надаючи час для навчання в робочий час (51%) і відшкодовуючи витрати на сторонні курси (50%). Однак одночасно з цим виникає парадокс сертифікації - незважаючи на те, що 91% організацій вважають, що галузеві сертифікації є важливими для подолання розриву в навичках кібербезпеки, лише 43% пропонують спонсорство сертифікації своїм співробітникам, що свідчить про значний розрив між вірою в постійне навчання та дії організацій в цьому напрямку.

ЖІНКИ В КІБЕРБЕЗПЕЦІ

Майже всі звіти, тією чи іншою мірою, приділяють увагу темі залучення жінок до сфери кібербезпеки. Ключові аргументи на користь цього, які наводить звіт Global Cybersecurity Forum:

- нові резерви кадрів можуть принести різноманітні перспективи та унікальні підходи до вирішення проблем та інновацій.
- компанії з ґендерно різноманітною базою співробітників, як правило, мають фінансові прибутки, які перевищують середні показники по національній галузі.
- заохочення жінок до кар'єри в сфері кібербезпеки може допомогти зміцнити добре оплачувану, високопродуктивну та перспективну галузь.

Кількість жінок, які працюють у сфері кібербезпеки, залишається майже незмінною з року в рік. ISC2 підрахував, що відсоток жінок у галузі, ймовірно, коливається від 20% до 25%. Хоча немає жодної організації, яка б спеціально відстежувала цей показник, цифри ISC2 узгоджуються з аналогічними звітами та оцінками інших організацій. Схожі дані дає звіт Global Cybersecurity Forum - станом на 2024 рік жінки становили близько 24% від всіх фахівців в сфері кібербезпеки (і 36% для всього технологічного сектору). Ці показники відрізняються за регіонами:

Регіон	Global Cybersecurity Forum
Азіатсько-Тихоокеанський регіон	24,8%
Північна та Південна Америка	25,4%
Європа	22,4%
Африка	13,5%

При цьому лише 16% від усіх CISO (Chief Information Security Officer) це жінки. Позитивна тенденція – з кожним роком жінок стає більше і вони охочіше йдуть у сферу кібербезпеки. Наприклад, статистика по віковим групам жінок в кібербезпеці виглядає наступним чином:

Вікова група	Відсоток у загальній кількості кіберфахівців
До 30 років	26%
30 – 34	25%
35-38	20%
39 – 44	16%
45 – 49	13%
50 – 54	14%
55 – 59	15%
60 – 64	14%
65+	13%

Ці данні підкріплюються іншим результатом опитування – лише 11% опитаних вказали на те, що в їх командах кібербезпеки взагалі немає жінок. Найбільше жінок-кіберфахівців в командах безпеки які працюють в сфері хмарних сервісів, автомобільних компаніях та будівництві (28% команди), а найменше – військові та енергетика (20%).

Також дослідження ICS2 показує, що жінки значно частіше ніж чоловіки мають вчені ступені (кваліфікації магістра та доктора) з профільних дисциплін, мають однакову кількість сертифікатів з чоловіками, але при цьому більше з них планують отримати нові сертифікати ніж чоловіки (27 відсотків проти 24).

Гендерні упередження впливають і на дії зловмисників. Наприклад, до жінок в організаціях майже в два рази частіше звертаються зловмисники які прагнуть залучити їх до зловмисної діяльності в якості інсайдера (35% жінок проти 21% чоловіків до яких звертались з аналогічними проханнями).

Дослідження також вказує на те, що жінки які працюють в сфері кібербезпеки частіше задоволені своєю роботою ніж чоловіки (76% проти 70%) і ця тенденція спостерігається щонайменше протягом 5 останніх років.

Організації приділяють все більше уваги саме цьому напрямку, намагаючись розширити свої стратегії залучення кіберфахівців збільшивши базу для найму. Так, 56% організацій проводять навчальні програми для створення інклюзивної культури та зміни сприйняття кібербезпеки як індустрії лише для чоловіків. 51% організацій прийняли цільові ініціативи (наприклад, активно шукаючи жінок-кандидатів і заохочуючи їх подавати заявки на посади в галузі) щодо найму персоналу, щоб залучити більше жінок до посад у сфері кібербезпеки. 62% організацій запровадили спеціальні політики підтримки для жінок, які заохочують їх йти в сферу кібербезпеки: гнучкі умови праці, відпустку по догляду за дитиною тощо. 36% організацій

запровадили програми наставництва, які особливо впливають на підтримку розвитку кар'єри жінок у сфері кібербезпеки.

РЕКОМЕНДАЦІЇ

Всі звіти так чи інакше пропонують численні тактичні чи стратегічні рекомендації, мета яких – зменшити дефіцит робочої сили та поліпшити кібербезпеку принаймні на рівні організацій. Ці рекомендації включають:

- ***Розширення програм залучення кіберфахівців не лише middle та senior рівнів, але і junior.*** Наймання різних людей, від професіоналів початкового рівня до найдосвідченіших, не лише створює можливості для залучення наступного покоління до робочої сили, але й забезпечує зростання можливостей роботи в сфері кібербезпеки. Цей підхід дає змогу найняти більшу кількість спеціалістів у межах доступного бюджету (адже зарплати молодших фахівців істотно нижчі) і створює стійкий довгостроковий канал для передачі знань від досвідчених спеціалістів наступному поколінню спеціалістів із кібербезпеки.

- ***Більше уваги навчанню вже найнятого персоналу.*** Спроба покладатися виключно на наймання попередньо кваліфікованих осіб може виявитись економічно затратним та стратегічно не ефективним. Крім того, підхід за якого організація сама формує програми навчання дозволяє їй навчати персоналу відповідно до унікальних поточних і майбутніх потреб самої організації.

- ***Зменшення розриву між тим, що шукають HR, і тим, що, на думку професіоналів, має попит на ринку.*** Роботодавці мають чіткіше формулювати свої очікування від майбутніх кандидатів, не покладаючись виключно на розуміння цих потреб з боку HR служб (або тісніше співпрацювати з ними в цьому питанні). Слід точніше оцінювати реальну потребу організації у фахівцях, не очікуючи, що професіонали вже мають недосяжний багаторічний досвід і галузеві сертифікати в нещодавно актуальній дисципліні, як, наприклад, штучний інтелект.

- ***Впроваджуйте цільові ініціативи з найму, спрямовані на недостатньо представлені групи, особливо жінок та інші меншини.*** В цьому може допомогти глибока співпраця з навчальними закладами, секторальними органами та громадськими організаціями. Слід розглядати можливість надання спеціальних стипендій, програм наставництва та пом'якшення потенційних бар'єрів у кар'єрі, з якими стикаються ці групи при вході в сферу кібербезпеки.

- ***Долучатись до національних ініціатив які популяризують кібербезпеку як найкращий вибір кар'єри.*** Значна кількість організацій може показати власні приклади з реального світу та відповідні рольові моделі які можуть збільшити зацікавленість в опануванні кіберпрофесій. Це включає розширення доступу до стажування, учнівства та раннього кар'єрного досвіду, що плавно переводить студентів у робочу силу.

- ***Інтеграція кібербезпеки в освітнеі програми від самого початку.*** Важливо, аби кібербезпекові дисципліни стали частиною навчальних програм початкової та середньої школи – це сприятиме розвитку зацікавленості щодо такої кар'єри (дослідження показують, що саме жінки частіше за чоловіків приймають рішення про кар'єру в сфері кібербезпеки якщо стикнулись з цим ще в школі).

- ***Адаптація навчальних програм відповідно до потреб промисловості.*** Освітні заклади мають тісніше взаємодіяти із промисловістю та приватним сектором аби краще розуміти їх потреби у фахівцях.

- ***Розвиток культури навчання впродовж життя.*** Як держави, так і приватні компанії мають бути орієнтованими на створення платформ безперервного навчання, які надають фахівцям з кібербезпеки постійний доступ до найновіших знань та відповідних інструментів. За можливості - централізуйте ці ресурси в легкодоступному навчальному просторі для підтримки професіоналів на всіх етапах кар'єри.

- ***Методи найму на основі навичок.*** Всі зацікавлені у залучення кіберфахівців мають більше орієнтуватись на рамки навичок кібербезпеки (NICE Cybersecurity Workforce Framework, ECSF, SCyWF14 чи підтверджені кваліфікації) замість спиратись на формальні академічні/освітні показники чи вимоги.

- ***Чітке розуміння кар'єрних шляхів.*** Кібербезпекові фахівці, які будь-які інші, потребують чіткого розуміння можливостей для свого зростання, навчання та просування. Це включає необхідність формування планів професійного розвитку та доступ до тренінгів.