МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “СУЧАСНІ МЕТОДИ Й ПІДХОДИ ПОДОЛАННЯ ДЕФІЦИТУ КАДРІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Максим АСТАЩЕНКО

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61

Керівник: Тетяна МУЖАНОВА, к.держ.упр., доцент

Рецензент:

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Астащенку Максиму Олександровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Сучасні методи й підходи подолання дефіциту кадрів у галузі кібербезпеки"

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к.держ.упр., доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. №467.

2. Строк подання кваліфікаційної роботи "___" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: *кадрове забезпечення кібербезпеки, дефіцит кадрів з кібербезпеки і методи його подолання.*
4. Перелік питань, які потрібно розробити:
   1. Дослідити теоретичні засади кадрового забезпечення галузі кібербезпеки.
   2. Проаналізувати методи подолання кадрового дефіциту в кібербезпеці.
   3. З'ясувати особливості сучасного кадрового забезпечення кібербезпеки в Україні та світі, запропонувати рекомендації щодо зменшення дефіциту кіберфахівців в Україні.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідження теоретичних засад кадрового забезпечення галузі кібербезпеки.	27.10.2025	
4.	Аналіз методів подолання кадрового дефіциту в кібербезпеці.	10.11.2025	
5.	З’ясування особливостей сучасного кадрового забезпечення кібербезпеки в Україні та світі, розробка рекомендацій.	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Максим АСТАЩЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Астащенко М.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Сучасні методи й підходи подолання дефіциту кадрів у галузі кібербезпеки"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **АСТАЩЕНКО Максим** у кваліфікаційній роботі дослідив теоретичні засади кадрового забезпечення галузі кібербезпеки; проаналізував методи подолання кадрового дефіциту в кібербезпеці; з'ясував особливості сучасного кадрового забезпечення кібербезпеки в Україні та світі, запропонував рекомендації щодо зменшення дефіциту кіберфахівців в Україні.

АСТАЩЕНКО Максим показав високу теоретичну і практичну підготовку, здатність працювати з великими обсягами даних і вирішувати науково-дослідницькі завдання. Кваліфікаційна робота оформлена згідно з вимогами. Виклад матеріалу здійснено логічно і послідовно, зроблено відповідні висновки. Основні тези дослідження представлено у вигляді рисунків і таблиць. Результати роботи апробовані на конференції "Актуальні проблеми кібербезпеки" 29 жовтня 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **АСТАЩЕНКО Максима** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Астащенко М.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри управління
кібербезпекою та захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти АСТАЩЕНКО Максима Олександровича
на тему "Сучасні методи й підходи подолання дефіциту кадрів у галузі кібербезпеки"

Актуальність. В умовах стрімкого зростання кількості та складності кіберзагроз, а також активної цифровізації всіх сфер суспільного життя, проблема дефіциту кваліфікованих кадрів у галузі кібербезпеки набуває критичного значення. За оцінками міжнародних експертів, глобальний дефіцит фахівців з кібербезпеки перевищує 4 млн осіб, при цьому попит на таких спеціалістів зростає на 25-30% щорічно.

Для України ця проблема є особливо актуальною з огляду на виклики воєнного часу, коли кіберзахист критичної інфраструктури стає питанням національної безпеки. Водночас, розвиток IT-сектору та кібербезпеки як його важливої складової відкриває значні можливості для економічного зростання країни у повоєнний період.

З огляду на зазначене дослідження сучасних методів і підходів подолання дефіциту кадрів у галузі кібербезпеки є актуальним науковим завданням.

Позитивні сторони

1. У роботі досліджено теоретичні засади кадрового забезпечення галузі кібербезпеки; проаналізовано методи подолання кадрового дефіциту в кібербезпеці; з'ясовано особливості сучасного кадрового забезпечення кібербезпеки в Україні та світі, запропоновано рекомендації щодо зменшення дефіциту кіберфахівців в Україні.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено послідовно згідно з планом роботи, зроблено логічні висновки. Основні положення роботи представлено у вигляді рисунків і таблиць. Автор опрацював понад 60 публікацій та електронних джерел, в тому числі англомовних.
3. За результатами дослідження запропоновано рекомендації щодо зменшення дефіциту кіберфахівців в Україні на основі кращих практик США, ЄС та Ізраїлю.

Недоліки

1. У роботі доцільно було б більш детально розглянути фінансово-економічні аспекти реалізації запропонованих рекомендацій, зокрема оцінку необхідних інвестицій та очікуваного ефекту від впровадження різних ініціатив щодо подолання кадрового дефіциту.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні і заслуговує оцінки "відмінно", а здобувач Астащенко Максим Олександрович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною та кібернетичною безпекою".

Рецензент:

_____
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 88 с., 8 рис., 20 табл., 97 джерел.

Метою роботи є дослідження сучасних методів і підходів подолання дефіциту кадрів у галузі кібербезпеки.

Об'єктом дослідження є кадрове забезпечення галузі кібербезпеки.

Предмет дослідження – сучасні методи й підходи подолання дефіциту кадрів у галузі кібербезпеки.

Методи дослідження. Для вирішення завдань дослідження використано методи системного аналізу, порівняльного аналізу, статистичний метод, метод експертних оцінок, методи узагальнення та систематизації, а також методи графічного і табличного представлення даних.

Короткий зміст роботи. Як результат у роботі досліджено теоретичні засади кадрового забезпечення галузі кібербезпеки; проаналізовано сучасні методи та інструменти подолання кадрового дефіциту в кібербезпеці; з'ясовано особливості кадрового забезпечення кібербезпеки в Україні та провідних країнах світу (США, ЄС, Ізраїль); запропоновано науково обґрунтовані рекомендації щодо зменшення дефіциту кіберфахівців в Україні.

Галузь застосування. Розроблені рекомендації можуть бути використані при формуванні кадрової політики у сфері кібербезпеки, плануванні освітніх програм підготовки фахівців з кібербезпеки, а також при розробці корпоративних програм розвитку персоналу у галузі інформаційної безпеки.

КЛЮЧОВІ СЛОВА : КІБЕРБЕЗПЕКА, КАДРОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, ДЕФІЦИТ КАДРІВ, ОСВІТА З КІБЕРБЕЗПЕКИ, СЕРТИФІКАЦІЯ ФАХІВЦІВ, КОРПОРАТИВНЕ НАВЧАННЯ, МІЖНАРОДНИЙ ДОСВІД, КАДРОВА ПОЛІТИКА.

ABSTRACT

The text part of the qualification master's thesis: 88 pages, 8 figures, 20 tables, 97 sources.

The aim of the work is to study modern methods and approaches to overcoming the personnel shortage in the field of cybersecurity. The object of research is the personnel provision of the cybersecurity sector.

Object of research is modern methods and approaches to overcoming the personnel shortage in the field of cybersecurity.

Subject of research is modern methods and approaches to overcoming the shortage of personnel in the field of cybersecurity.

Research methods. To solve the research tasks, the following methods were used: system analysis, comparative analysis, statistical method, expert evaluation method, generalization and systematization methods, as well as graphical and tabular data presentation methods.

Summary of the paper. As a result, the theoretical foundations of personnel provision in the cybersecurity sector were studied; modern methods and tools for overcoming the personnel shortage in cybersecurity were analyzed; the features of cybersecurity personnel provision in Ukraine and leading countries of the world (USA, EU, Israel) were clarified; scientifically substantiated recommendations for reducing the shortage of cybersecurity professionals in Ukraine were proposed.

Field of research. The developed recommendations can be used in the formation of personnel policy in the field of cybersecurity, planning of educational programs for training cybersecurity specialists, as well as in the development of corporate personnel development programs in the field of information security.

KEYWORDS: CYBERSECURITY, PERSONNEL PROVISION IN CYBERSECURITY, PERSONNEL SHORTAGE, CYBERSECURITY EDUCATION, PROFESSIONAL CERTIFICATION, CORPORATE TRAINING, INTERNATIONAL EXPERIENCE, PERSONNEL POLICY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AI	Artificial Intelligence (штучний інтелект, ШІ)
API	Application Programming Interface (програмний інтерфейс додатку)
CEH	Certified Ethical Hacker (сертифікований етичний хакер)
CISA	Certified Information Systems Auditor (сертифікований аудитор інформаційних систем)
CISM	Certified Information Security Manager (сертифікований менеджер з інформаційної безпеки)
CISSP	Certified Information Systems Security Professional (сертифікований професіонал з безпеки інформаційних систем)
DHS	Department of Homeland Security (департамент внутрішньої безпеки США)
ENISA	European Union Agency for Cybersecurity (агентство Європейського Союзу з кібербезпеки)
GDPR	General Data Protection Regulation (Загальний регламент захисту даних)
GIAC	Global Information Assurance Certification (глобальна сертифікація з забезпечення інформації)
IBM	International Business Machines (міжнародні бізнес-машини)
IDS	Intrusion Detection System (система виявлення вторгнень)
IPS	Intrusion Prevention System (система запобігання вторгненням)
IoT	Internet of Things (інтернет пристрої)
ISACA	Information Systems Audit and Control Association (асоціація аудиту та контролю інформаційних систем)
ISC	International Information System Security Certification Consortium ((ISC)² - міжнародний консорціум сертифікації безпеки інформаційних систем)

ISO	International Organization for Standardization (міжнародна організація зі стандартизації)
KPI	Key Performance Indicator (ключовий показник ефективності)
MIT	Massachusetts Institute of Technology (Массачусетський технологічний інститут)
ML	Machine Learning (машинне навчання, МН)
MSSP	Managed Security Service Provider (постачальник керованих послуг безпеки)
NICE	National Initiative for Cybersecurity Education (національна ініціатива з освіти у кібербезпеці)
NIST	National Institute of Standards and Technology (національний інститут стандартів і технологій США)
NSA	National Security Agency (агентство національної безпеки США)
NSF	National Science Foundation (національний науковий фонд США)
ROI	Return on Investment (повернення інвестицій)
SIEM	Security Orchestration, Automation and Response (оркестрація, автоматизація та реагування на інциденти безпеки)
SOAR	Security Orchestration, Automation and Response (оркестрація, автоматизація та реагування на інциденти безпеки)
SOC	Security Operations Center (центр операцій безпеки)
URL	Uniform Resource Locator (уніфікований покажчик ресурсу)
VPN	Virtual Private Network (віртуальна приватна мережа)
UEBA	User and Entity Behavior Analytics (аналітика поведінки користувачів та об'єктів)

ВСТУП

Актуальність теми. З огляду на стрімкий розвиток галузі кібербезпеки внаслідок активної цифровізації всіх сфер суспільного життя і застосування новітніх ІКТ, зростання кількості і складності кіберзагроз, кадрове забезпечення відстає від потреб галузі, а проблема дефіциту кваліфікованих фахівців з кібербезпеки набуває критичного значення. Як свідчить статистика, глобальний дефіцит фахівців з кібербезпеки становить понад 4 млн осіб, при цьому попит на кіберспеціалістів зростає на 25-30% щорічно.

Для України ця проблема є особливо актуальною з огляду на виклики воєнного часу, коли кіберзахист критичної інфраструктури стає питанням національної безпеки. Водночас, розвиток ІТ-сектору та кібербезпеки як його важливої складової відкриває значні можливості для економічного зростання країни у повоєнний період.

З огляду на зазначене дослідження сучасних методів і підходів подолання дефіциту кадрів у галузі кібербезпеки є актуальним науковим завданням.

Мета роботи полягає у дослідженні сучасних методів і підходів подолання дефіциту кадрів у галузі кібербезпеки.

Об'єкт дослідження - кадрове забезпечення галузі кібербезпеки.

Предмет дослідження – сучасні методи й підходи подолання дефіциту кадрів у галузі кібербезпеки.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. Дослідити теоретичні засади кадрового забезпечення галузі кібербезпеки.

2. Проаналізувати методи подолання кадрового дефіциту в кібербезпеці.

3. З'ясувати особливості сучасного кадрового забезпечення кібербезпеки в Україні та світі, запропонувати рекомендації щодо зменшення дефіциту кіберфахівців в Україні.

Методи дослідження. Для вирішення завдань дослідження використано методи системного аналізу, порівняльного аналізу, статистичний метод, метод

експертних оцінок, методи узагальнення та систематизації, а також методи графічного і табличного представлення даних.

Наукова новизна одержаних результатів. У роботі досліджено тенденції ринку праці в кібербезпеці і встановлено причини дефіциту кадрів, проаналізовано методи вирішення проблеми нестачі кіберфахівців на основі досвіду передових країн світу, запропоновано науково обґрунтовані рекомендації щодо зменшення дефіциту кіберфахівців в Україні.

Практичне значення одержаних результатів. Застосування напрацювань дослідження буде доцільним при формуванні кадрової політики у сфері кібербезпеки, плануванні освітніх програм підготовки кіберфахівців, а також при розробці корпоративних програм розвитку персоналу в галузі кібербезпеки.

Апробація результатів кваліфікаційної роботи була здійснена на конференції “Актуальні проблеми кібербезпеки” 29 жовтня 2025 року.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ КАДРОВОГО ЗАБЕЗПЕЧЕННЯ ГАЛУЗІ КІБЕРБЕЗПЕКИ

1.1 Загальна характеристика галузі кібербезпеки

Кібербезпека у сучасному світі перетворилася на одну з найдинамічніших та найважливіших галузей цифрової економіки. У контексті глобальної цифрової трансформації, стрімкого розвитку інформаційних технологій та зростання кількості кіберзагроз, питання забезпечення безпеки цифрового простору набуває критичного значення як для окремих організацій, так і для національних економік у цілому.

Кібербезпека як галузь представляє собою комплексну систему заходів, технологій, процесів та практик, спрямованих на захист комп'ютерних систем, мереж, програм і даних від несанкціонованого доступу, пошкодження або крадіжки. Це динамічна сфера діяльності, яка постійно еволюціонує у відповідь на нові виклики та загрози цифрового середовища [1]. Галузь охоплює широкий спектр напрямків - від технічного захисту інфраструктури до організаційних заходів, від розробки спеціалізованого програмного забезпечення до надання консультаційних послуг з питань інформаційної безпеки.

Значення кібербезпеки в сучасному світі важко переоцінити. У епоху, коли критична інфраструктура, фінансові системи, медичні заклади, державні установи та приватні підприємства функціонують на базі цифрових технологій, забезпечення їх захисту стає питанням національної безпеки. Кіберінциденти можуть призвести до масштабних економічних збитків, порушення роботи критичної інфраструктури, втрати конфіденційних даних та підриву довіри до цифрових сервісів.

Масштаби та динаміка світового ринку кібербезпеки. Глобальний ринок кібербезпеки демонструє стабільне та потужне зростання, що відображає зростаючу важливість галузі для світової економіки. За різними оцінками

провідних аналітичних агентств, обсяг світового ринку кібербезпеки у 2024 році становив від 193 до 299 млрд доларів США залежно від методології підрахунку [12, 13, 19]. Така розбіжність в оцінках пояснюється різними підходами до визначення меж галузі та включенням різних напрямків послуг.

Динаміка розвитку ринку кібербезпеки характеризується високими темпами зростання. За прогнозами аналітиків, середньорічні темпи приросту ринку кібербезпеки у період 2025-2030 років коливатимуться від 9,1% до 14,4% [12, 13, 14]. Це означає, що до 2030 року обсяг глобального ринку може досягти від 351 до 562 млрд доларів США [12, 13] (Таблиця 1.1). Окремі дослідження прогнозують ще більш оптимістичні сценарії розвитку галузі [4].

Таблиця 1.1

Прогноз розвитку ринку кібербезпеки

Рік	Обсяг ринку (млрд USD)	Темп приросту (%)	Джерело
2024	193-299	-	[12, 13, 19]
2025	220-330	9-14	Прогноз
2026	245-365	11-13	Прогноз
2027	275-410	12-14	Прогноз
2028	305-460	11-13	Прогноз
2029	340-510	11-12	Прогноз
2030	351-562	10-11	[12, 13]

Таке стрімке зростання обумовлене низкою факторів (рисунок 1.1). По-перше, це постійне збільшення кількості та складності кіберзагроз. Кіберзлочинці постійно вдосконалюють свої методи атак, використовуючи нові технології, включаючи штучний інтелект (ШІ) та машинне навчання (МН). По-друге, прискорення процесів цифровізації в усіх секторах економіки створює нові поверхні для потенційних атак та підвищує потребу в надійному захисті. По-третє, посилення регуляторних вимог у сфері захисту даних, таких як GDPR в Європі, стимулює організації інвестувати в кібербезпеку.

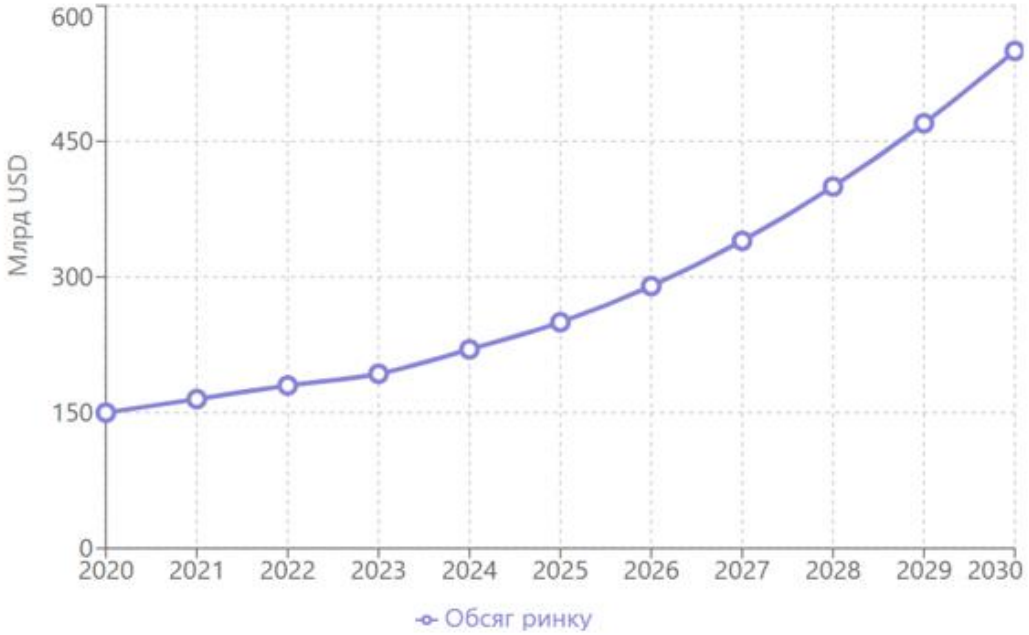

Рис. 1.1. Динаміка зростання глобального ринку кібербезпеки (млрд/USD)

Структура та різноманітність ринку кібербезпеки. Ринок кібербезпеки характеризується високим рівнем диверсифікації і включає різні сегменти, що відповідають різним аспектам захисту цифрового простору (рис. 1.2).

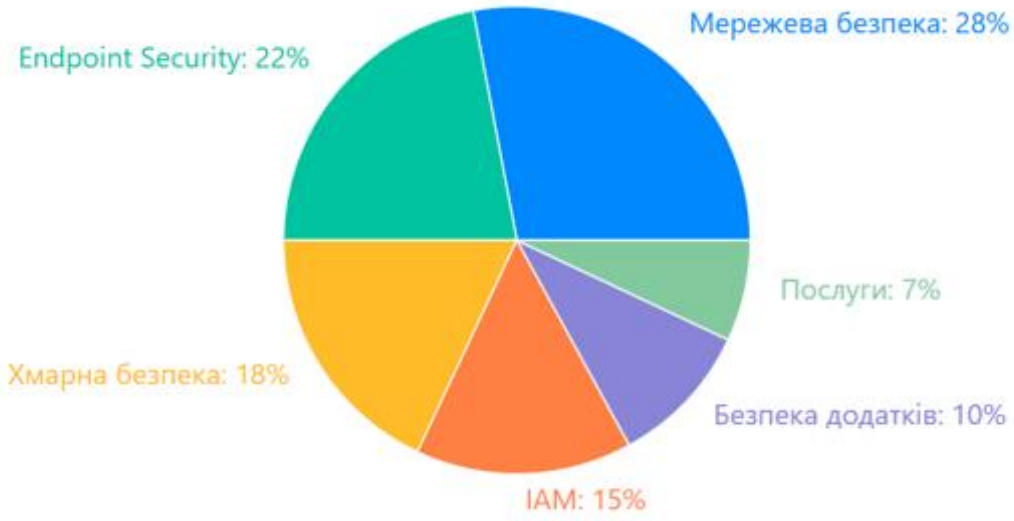

Рис. 1.2. Структура сегментів ринку кібербезпеки

Рішення для захисту мережевої інфраструктури охоплюють міжмережеві екрани, системи виявлення та запобігання вторгненням, захищені мережеві шлюзи. Цей напрямок залишається одним з найбільших, оскільки мережева безпека є фундаментальною складовою захисту будь-якої організації.

Захист кінцевих пристроїв охоплює антивірусне програмне забезпечення, системи запобігання витоку даних, рішення для управління мобільними пристроями. З розширенням практики віддаленої роботи та використання власних пристроїв працівників цей напрямок набуває особливої актуальності.

Безпека хмарних сервісів - стрімко зростаючий напрямок, що відповідає на виклики переходу інфраструктури у хмарні середовища. Управління ідентифікацією та доступом включає системи розпізнавання, дозволу, багатофакторної перевірки. Послуги з кібербезпеки охоплюють консультування, керовані послуги безпеки, послуги з реагування на інциденти.

Регіональні особливості розвитку галузі. Географічна структура ринку характеризується нерівномірністю. Північна Америка залишається найбільшим регіональним ринком, забезпечуючи понад 40% світового обсягу [6]. Європа займає друге місце, Азіатсько-Тихоокеанський регіон демонструє найвищі темпи зростання (Рис. 1.3).

Рис. 1.3. Візуалізація даних ринку кібербезпеки за регіонами

Український ринок кібербезпеки: особливості та перспективи. Український ринок, незважаючи на відносно невеликий обсяг, демонструє вражаючу динаміку розвитку. За оцінками експертів, частка України становить менше 1% світового ринку [8, 10], проте за останні вісім років ринок збільшився у чотири рази [3]. Країна фактично стала випробувальним майданчиком для

протидії найскладнішим кіберзагрозам. Постійне протистояння стимулювало розвиток вітчизняної галузі й формування високопрофесійного кадрового потенціалу.

Водночас український ринок стикається з серйозними викликами, включаючи дефіцит кваліфікованих кадрів, обмежені фінансові ресурси, необхідність відповідати міжнародним стандартам. Попри ці виклики, український сектор демонструє стійкість та здатність до інновацій.

Ключові тенденції та виклики галузі. Кібербезпека перестає бути виключно технічною проблемою і перетворюється на стратегічний пріоритет вищого керівництва організацій. Спостерігається активна інтеграція технологій ШІ та МН. Концепція архітектури нульової довіри стає домінуючою парадигмою безпеки. Серед основних викликів виділяють критичний дефіцит кваліфікованих фахівців (Табл. 1.2).

Таблиця 1.2

Темпи зростання дефіциту кваліфікованих працівників

Регіон	Частка ринку (%)	Обсяг (млрд USD)	Темп зростання
Північна Америка	42	85-125	Помірний
Європа	28	56-84	Стабільний
Азія-Тихоокеанський	22	44-66	Високий
Близький Схід та Африка	5	10-15	Середній
Латинська Америка	3	6-9	Середній

1.2 Причини дефіциту кадрів у сфері кібербезпеки

Проблема дефіциту кваліфікованих кадрів набула глобального масштабу. За даними міжнародної організації фахівців з кібербезпеки, станом на 2024 рік глобальний розрив між попитом та пропозицією становив понад 4,7 млн вакансій [4], що представляє зростання на 19,1% порівняно з попереднім роком (Рис. 1.4). Для України країні не вистачає близько 100 тисяч фахівців [5].

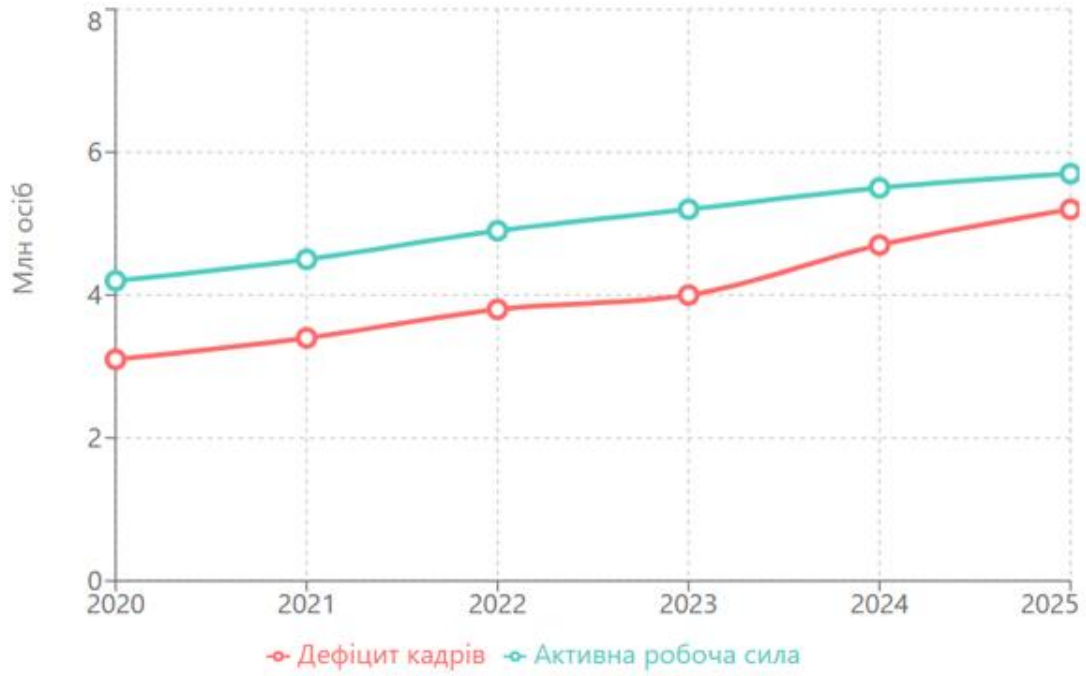

Рис. 1.4. Глобальний дефіцит кадрів в ринку кібербезпеки (млн осіб)

Проблема має комплексний характер і обумовлена взаємопов'язаними факторами.

Складність вимірювання темпів зростання попиту та пропозиції. Цифрова трансформація економіки відбувається з безпрецедентною швидкістю, автоматично збільшуючи потребу в захисті нових цифрових активів. Водночас, кількість активних працівників залишається відносно стабільною на рівні 5,5 млн осіб глобально [6]. Система освіти не встигає продукувати достатню кількість кваліфікованих спеціалістів. Характер загроз постійно еволюціонує, вимагаючи безперервного оновлення знань.

Високі перешкоди входу у професію. Кібербезпека сприймається як сфера з високими перешкодами входу. Роботодавці встановлюють нереалістично високі вимоги до кандидатів на початкові позиції. Дослідження показують, що багато вакансій початкового рівня містять вимоги про наявність 3-5 років практичного досвіду [15, 16].

Галузь характеризується наявністю дорогих систем підтвердження кваліфікації. Професійні свідоцтва вимагають значних фінансових інвестицій та попереднього практичного досвіду (Табл. 1.3) [3]. Це створює замкнене коло: для отримання роботи потрібні свідоцтва, для отримання свідоцтв - досвід роботи.

Таблиця 1.3

Топ-10 найбільш затребуваних сертифікацій у кібербезпеці

Рангсертифікації	Сертифікація	Організація	Середня премія до зарплати
1	CISSP	(ISC)²	+15-20%
2	CEH	EC-Council	+10-15%
3	CISM	ISACA	+15-20%
4	CompTIA Security+	CompTIA	+8-12%
5	OSCP	Offensive Security	+12-18%
6	CISA	ISACA	+10-15%
7	CRISC	ISACA	+12-16%
8	AWS Security	Amazon	+10-14%
9	GSEC	GIAC	+10-15%
10	Azure Security	Microsoft	+10-14%

Технічна складність дисципліни також виступає перешкодою. Кібербезпека вимагає міждисциплінарних знань, що охоплюють мережеві технології, системне адміністрування, програмування, криптографію, юридичні аспекти [4].

Недоліки системи освіти та професійної підготовки. Система освіти стикається з численними структурними проблемами. Недостатня інтеграція кібербезпеки у стандартні навчальні програми. В Україні часто спостерігається відрив між академічними знаннями і практичними потребами галузі [5]. Нестача кваліфікованих викладачів обмежує якість та обсяг освіти [5].

Демографічні невідповідності та недостатнє різноманіття. Галузь характеризується значними демографічними дисбалансами. Жінки залишаються недопредставленими, становлячи менше 25% робочої сили [6]. Це обумовлено стереотипами та несприятливою культурою деяких організацій. Відсутність різноманіття обмежує талановий пул та інноваційний потенціал галузі [7].

Труднощі з утриманням кадрів. Висока плинність кадрів є серйозною проблемою. Основні причини звільнення: відсутність можливостей кар'єрного

зростання (36%), незадовільна винагорода (33%), емоційне вигорання (27%), відсутність визнання (25%) [23, 24].

Сучасні фахівці повинні володіти широким спектром технічних знань, розуміти бізнес-процеси та ефективно комунікувати з різними зацікавленими сторонами. Множинність факторів, що впливають на залучення та утримання кадрів у кібербезпеці, систематизовано в Таблиці 1.4.

Таблиця 1.4

Вплив чинників на залучення нових кадрів на ринок праці

Категорія причин	Конкретні фактори	Вплив (1-5)
Структурні	Невідповідність темпів зростання попиту та пропозиції	⭐⭐⭐⭐⭐
	Високі бар'єри входу у професію	⭐⭐⭐⭐
	Вимоги досвіду для початкових позицій	⭐⭐⭐⭐
Освітні	Розрив між освітою та потребами індустрії	⭐⭐⭐⭐⭐
	Недостатня кількість практичних навчань	⭐⭐⭐⭐
	Нестача кваліфікованих викладачів	⭐⭐⭐
Соціальні	Гендерна нерівність (жінки <25%)	⭐⭐⭐⭐
	Недостатнє представництво меншин	⭐⭐⭐
	Низька обізнаність про професію	⭐⭐⭐⭐
Організаційні	Труднощі з утриманням кадрів	⭐⭐⭐⭐
	Психологічне вигорання	⭐⭐⭐
	Відсутність чітких кар'єрних траєкторій	⭐⭐⭐
Економічні	Обмежені бюджети організацій	⭐⭐⭐⭐
	Висока вартість сертифікацій	⭐⭐⭐

1.3 Основні компетенції і навички, необхідні фахівцям з кібербезпеки

Технічні компетенції фахівців з кібербезпеки. Технічні навички становлять фундамент професійної діяльності у сфері кібербезпеки й охоплюють широкий спектр знань і вмінь, необхідних для захисту інформаційних систем від різноманітних загроз.

Глибоке розуміння принципів функціонування комп'ютерних мереж є критично важливою компетенцією для фахівців з кібербезпеки. Це включає знання архітектури мереж, протоколів передачі даних, маршрутизації та комутації. Особливе значення має володіння технологіями захисту мережевої інфраструктури, включаючи налаштування та управління міжмережевими екранами, системами виявлення та запобігання вторгненням, віртуальними приватними мережами та іншими засобами захисту [5].

Володіння мовами програмування є однією з найважливіших технічних компетенцій у кібербезпеці. Фахівці повинні мати навички роботи з такими мовами, як Python, Java, C++ (Табл. 1.5), які необхідні для розробки безпечних додатків, автоматизації завдань безпеки та аналізу вразливостей програмного забезпечення [5].

Таблиця 1.5

Рівень затребуваності знання мов програмування

Категорія	Ключові компетенції	Рівень критичності
Мережева безпека	TCP/IP, Firewalls, IDS/IPS, VPN, аналіз трафіку	Критичний
Програмування	Python, Java, C++, PowerShell, Bash	Високий
Аналіз загроз	Threat Intelligence, оцінка ризиків, OSINT	Критичний
Управління інцидентами	IR процедури, цифрова криміналістика, chain of custody	Критичний
Хмарна безпека	AWS, Azure, GCP, IaaS/PaaS/SaaS security	Високий
Криптографія	Шифрування, PKI, квантово-стійка криптографія	Середній
ОС та системне адміністрування	Linux, Windows, Active Directory	Високий
Безпека додатків	OWASP Top 10, SAST/DAST, DevSecOps	Високий

Python особливо цінується в індустрії завдяки своїй універсальності та наявності численних бібліотек для задач кібербезпеки, включаючи аналіз шкідливого коду, автоматизацію тестування на проникнення та обробку великих

обсягів даних безпеки. Знання скриптових мов, таких як PowerShell та Bash, є цінним для тестування на проникнення, автоматизації адміністративних завдань та аналізу системних логів [20].

Аналіз загроз є ключовою навичкою для професіоналів кібербезпеки, яка включає збір, аналіз і представлення даних про потенційні ризики та вразливості. Ця компетенція допомагає організаціям виявляти кіберзагрози та готуватися до атак [6].

Здатність ефективно реагувати на інциденти кібербезпеки є критичною компетенцією, яка може визначити різницю між незначним порушенням і катастрофічною втратою даних. Кіберфахівці повинні володіти навичками виявлення, аналізу, локалізації та усунення наслідків інцидентів безпеки.

З масовим переходом організацій до хмарних технологій, компетенції в галузі хмарної безпеки стали особливо затребуваними. Кіберфахівці мають розуміти специфіку захисту даних і додатків у хмарному середовищі, включаючи моделі IaaS, PaaS та SaaS, а також знати особливості безпеки провідних хмарних платформ [7].

М'які навички фахівців з кібербезпеки. Дослідження останніх років демонструють суттєві зміни в пріоритетах роботодавців щодо компетенцій фахівців з кібербезпеки. Згідно з дослідженням ISC2, проведеним у 2024 році, найбільш затребуваними навичками, які шукають менеджери з найму, є сильні здібності до вирішення проблем (31%), командна робота та співпраця (28%), а також ефективна комунікація (25%), і ці показники перевищують традиційні технічні компетенції [31, 41].

Ефективна комунікація є однією з найважливіших м'яких навичок для фахівців з кібербезпеки. Це пов'язано з необхідністю взаємодії з різними зацікавленими сторонами – від технічних спеціалістів до вищого керівництва та нетехнічних користувачів. Згідно з дослідженнями, 58% роботодавців визначають комунікативні навички як пріоритетні при підборі кандидатів на посади кібербезпеки (Табл. 1.6).

Таблиця 1.6

Вимоги до кіберфахівців щодо володіння м’якими(soft skills) навичками

Навичка	Відсоток роботодавців	Важливість для ролі
Вирішення проблем	31%	Критична для всіх ролей
Командна робота та співпраця	28%	Дуже висока
Ефективна комунікація	25%	Дуже висока
Критичне мислення	54% (top-5)	Висока
Увага до деталей	36% (top-5)	Висока
Адаптивність	Не кількісно оцінено	Висока
Етичність	Обов'язкова	Критична

Професіонали з кібербезпеки повинні вміти пояснювати складні технічні концепції простою, зрозумілою мовою для нетехнічної аудиторії. Це включає здатність спрощувати складні технічні концепції та вміння виступати посередником між технічними експертами та нетехнічними зацікавленими сторонами [25].

Здатність до вирішення складних проблем є найбільш затребуваною навичкою в галузі кібербезпеки, що підтверджують 31% відповідей менеджерів з найму [2]. Кіберзагрози постійно еволюціонують, і фахівці повинні демонструвати креативний підхід до пошуку рішень нестандартних проблем.

Сучасна кібербезпека – це командна діяльність, яка вимагає ефективної взаємодії між фахівцями різних спеціалізацій. 28% менеджерів з найму визначають командну роботу та співпрацю як пріоритетні навички [2], а 45% роботодавців включають командну роботу до топ-5 найважливіших компетенцій [9].

Спеціалізовані компетенції для різних ролей у кібербезпеці. Різні ролі у сфері кібербезпеки вимагають специфічних комбінацій навичок та знань. Аналітики безпеки зосереджені на моніторингу систем, виявленні та аналізі інцидентів безпеки. Інженери з безпеки проєктують та впроваджують рішення безпеки. Архітектори безпеки розробляють загальну стратегію безпеки організації. Фахівці з реагування на інциденти спеціалізуються на швидкому

реагуванні та відновленні після атак. Тестувальники на проникнення оцінюють захищеність систем шляхом імітації атак.

Розвиток та підтримка компетенцій. Динамічний характер галузі кібербезпеки вимагає від фахівців постійного навчання та розвитку. Основні способи підтримки та розвитку компетенцій включають: офіційні сертифікації, які підтверджують володіння певними знаннями та навичками [3]; самоосвіту через читання фахової літератури, блогів з питань безпеки, участь у вебінарах та проходження курсів; практичне навчання через участь у змаганнях з кібербезпеки, вирішення завдань на спеціалізованих платформах; участь у спільнотах практиків через конференції, форуми, зустрічі професійних спільнот.

1.4 Огляд світових і вітчизняних тенденцій ринку праці кібербезпеки

Аналіз світових та українських тенденцій ринку праці у сфері кібербезпеки виявляє глибину та комплексність проблеми кадрового забезпечення галузі. Розуміння цих тенденцій є критично важливим для розробки ефективних стратегій розвитку кадрового потенціалу.

Глобальні тенденції попиту на фахівців з кібербезпеки. Попит на фахівців з кібербезпеки на глобальному рівні зростає експоненційно. Глобальний дефіцит кваліфікованих працівників у сфері кібербезпеки збільшився з 3,4 млн у 2022 році до 4,7 млн у 2024 році [4]. Найбільший дефіцит відчувають розвинені країни, включаючи США, Канаду, Велику Британію, Австралію та країни Західної Європи.

Найбільш затребувані спеціалізації включають аналітиків безпеки, інженерів з безпеки хмарних технологій, фахівців з реагування на інциденти, етичних хакерів та тестувальників на проникнення, архітекторів безпеки. Попит особливо високий на фахівців з досвідом роботи з новими технологіями, такими як ШІ, МН та Інтернет речей.

Структура ринку праці та моделі зайнятості. Ринок праці у сфері кібербезпеки характеризується різноманітністю моделей зайнятості (Табл. 1.7).

Таблиця 1.7

Глобальний дефіцит кадрів у кібербезпеці за регіонами

Регіон	Активна робоча сила (млн)	Дефіцит (млн)	Загальна потреба (млн)
Азія-Тихоокеанський	2,3	2,4	4,7
Північна Америка	1,4	0,7	2,1
Європа	1,2	0,9	2,1
Близький Схід та Африка	0,4	0,5	0,9
Латинська Америка	0,2	0,3	0,5
Всього (світ)	**5,5**	**4,8**	**10,3**

Традиційна штатна зайнятість залишається домінуючою моделлю, особливо у великих організаціях, які мають потребу у постійній підтримці безпеки. Консультування та проєктна робота набувають популярності серед досвідчених фахівців, які цінують гнучкість та різноманітність проєктів. Керовані послуги безпеки, коли організації винесли функції безпеки зовнішнім постачальникам, стають все більш поширеними, особливо серед малих та середніх підприємств.

Рівні винагороди та компенсацій. Високий попит на фахівців з кібербезпеки призводить до значного зростання рівня заробітних плат як на глобальному рівні, так і в Україні. У США середня річна зарплата для фахівців з кібербезпеки становить від 90 до 150 тисяч доларів залежно від спеціалізації та рівня досвіду [28]. Старші фахівці та фахівці у високо спеціалізованих галуззях можуть отримувати значно більше.

В Європі рівень винагороди дещо нижчий, але конкурентоспроможний – від 50 до 100 тисяч євро на рік [29]. Найвищі зарплати спостерігаються у Західній Європі, особливо у Великій Британії, Німеччині та скандинавських країнах.

В Україні ринок праці з кібербезпеки також демонструє конкурентоспроможні рівні винагороди. Середня заробітна плата для фахівців

коливається від 2000 до 8000 доларів США на місяць залежно від рівня досвіду та спеціалізації (Табл. 1.8).

Таблиця 1.8

Рівні заробітних плат фахівців з кібербезпеки у США (2024-2025)

Рівень досвіду	Діапазон (тис. USD/рік)	Медіанна зарплата	Типові ролі
Початківець (0-2 роки)	50-90	70	Junior Analyst, SOC Analyst L1
Середній рівень (3-5 років)	90-170	133	Security Engineer, Analyst L2
Досвідчений (6-10 років)	150-280	200	Senior Engineer, Architect
Експерт (10+ років)	250-500+	350	CISO, Principal Architect

Середня заробітна плата для фахівців з кібербезпеки демонструє стабільне зростання. За даними статистики, середня зарплата зросла на 4% з 119,860 доларів у 2022 році до 124,740 доларів у 2023 році [30]. Для фахівців середнього рівня з приблизно 5-річним досвідом роботи типовий діапазон зарплати у 2025 році становить від 133,099 до 150,389 доларів (Рис. 1.5) [4].

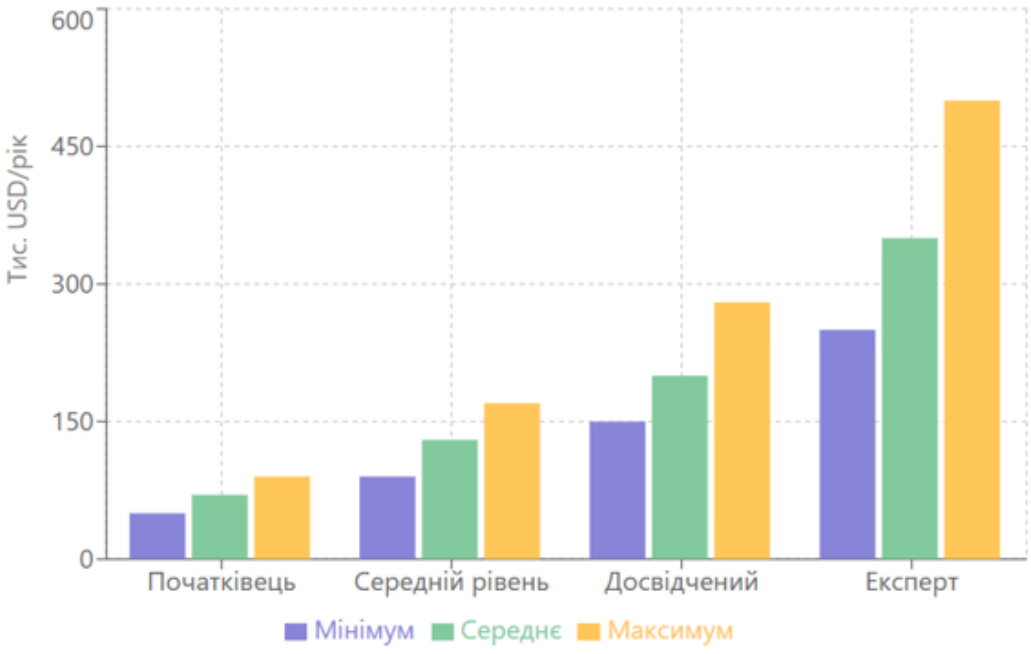

Рис. 1.5. Діапазони зарплат кіберфахівців (тис USD/на рік)

Середні рівні винагороди фахівців в Україні. Український ринок праці з кібербезпеки характеризується кількома унікальними особливостями. За останні роки український ринок кібербезпеки демонстрував вражаючу динаміку зростання, збільшившись у чотири рази за останні вісім років та досягнувши обсягу 138 млн доларів у 2024 році [3].

Міжнародна підтримка та співробітництво відіграють важливу роль у розвитку українського сектору кібербезпеки. Країни-партнери надають Україні як фінансову, так і технічну підтримку для посилення спроможностей у сфері кібербезпеки. Міжнародні організації допомагають українським організаціям захищати свої мережі [9].

З початку повномасштабної війни кіберпідтримка США для України досягла 82 млн доларів, тоді як Європейський Союз виділив 10 млн доларів у вигляді грантової допомоги [9]. Ця підтримка є критично важливою для підтримки стійкості українських систем кібербезпеки і розвитку вітчизняної галузі.

Міжнародне співробітництво не обмежується лише фінансовою допомогою і охоплює обмін знаннями, спільні навчальні програми, технологічну підтримку й інтеграцію українських фахівців у глобальну спільноту кібербезпеки. Це створює можливості для трансферу передових практик і технологій, а також для підвищення кваліфікації українських спеціалістів.

Впровадження передових технологій. Український ринок кібербезпеки активно впроваджує передові технології для протидії сучасним загрозам. 65% українських організацій планують впровадити ШІ та МН для виявлення загроз і реагування на них до 2024 року [9]. Блокчейн розглядається як перспективна технологія для безпечного зберігання і передачі даних.

Експерти галузі прогнозують, що архітектура нульової довіри і квантово-стійка криптографія стануть стандартними практиками до 2025 року [2]. Це створює величезні можливості для фахівців з кібербезпеки, які можуть працювати з цими новітніми технологіями.

Попит на фахівців з кібербезпеки в Україні. Попит на фахівців з кібербезпеки в Україні зростає відповідно до розширення ринку та збільшення

усвідомлення важливості захисту інформації. Український ринок праці з кібербезпеки характеризується кількома особливостями. По-перше, значна частина українських кіберфахівців працюють у міжнародних компаніях або як незалежні працівники на глобальному ринку. По-друге, існує високий попит на фахівців, які володіють знаннями про захист критичної інфраструктури та оборонні системи. По-третє, зростає потреба в спеціалістах з хмарної безпеки, безпеки OT-систем та аналізу загроз.

Україна демонструє високий рівень стійкості в галузі кібербезпеки, що визнається міжнародною спільнотою [25]. Український досвід протистояння кіберзагрозам у воєнних умовах є унікальним і цінним для глобальної спільноти кібербезпеки. Це створює можливості для українських фахівців поділитися своїм досвідом і підвищити свою цінність на міжнародному ринку праці.

Ключові виклики та перспективи розвитку. Розрив між освітою та потребами галузі залишається однією з найбільших проблем на ринку праці в кібербезпеці. Традиційні освітні програми часто не встигають за швидкими змінами в галузі, що призводить до ситуації, коли випускники мають теоретичні знання, але не володіють практичними навичками, необхідними для роботи [27].

Питання різноманітності та включеності. Галузь кібербезпеки традиційно характеризується низьким рівнем різноманітності, особливо щодо гендерного балансу. Згідно з різними дослідженнями, жінки складають менше 25% робочої сили в кібербезпеці. Це не лише питання соціальної справедливості, але й економічна проблема, оскільки обмежує коло потенційної кваліфікованої робочої сили для галузі.

Віддалена робота та глобалізація ринку праці. Пандемія прискорила перехід до моделі віддаленої роботи, що має значний вплив на ринок праці в кібербезпеці. З одного боку, віддалена робота розширює географічний діапазон пошуку кваліфікованої робочої сили для роботодавців і відкриває нові можливості для фахівців. З іншого боку, це створює нові виклики для безпеки та вимагає адаптації процесів управління командами.

Глобалізація ринку праці в кібербезпеці означає, що організації можуть залучати кваліфіковану робочу силу з будь-якої точки світу, а фахівці можуть працювати на міжнародні компанії без необхідності зміни фізичного місця перебування. Це особливо актуально для України, де багато фахівців з кібербезпеки працюють на закордонні компанії, зберігаючи при цьому проживання в країні.

Перспективи розвитку та прогнози. Аналіз поточних тенденцій дозволяє сформувати прогнози щодо майбутнього розвитку ринку праці в кібербезпеці. Очікується, що попит на фахівців продовжить зростати щонайменше протягом наступного десятиліття. Темпи зростання можуть навіть прискоритися через збільшення кіберзагроз, розвиток нових технологій і посилення регуляторних вимог.

Нові технології, такі як квантові обчислення, ШІ та Інтернет речей, створюватимуть попит на нові спеціалізації в кібербезпеці. Водночас автоматизація окремих завдань може змінити характер роботи фахівців, зміщуючи акцент з рутинних операцій на більш складні аналітичні та стратегічні завдання.

Для України перспективи розвитку ринку кібербезпеки (Табл. 1.9) є особливо важливими в контексті післявоєнної відбудови й інтеграції в європейські та світові економічні структури. Український досвід та експертиза в галузі кібербезпеки можуть стати конкурентною перевагою країни на міжнародній арені.

Таблиця 1.9

Перспективи розвитку ринку кібербезпеки для України

Показник	2016	2020	2024	2029 (прогноз)
Обсяг ринку (млн USD)	35	80	138	209
Зростання відносно 2016 (разів)	1	2,3	4	6
Частка оборонного ПЗ (%)	45	55	65	60
Темп приросту (%)	-	23	15	8-10

Висновки до розділу 1

Галузь кібербезпеки є динамічним і стратегічно важливим сектором цифрової економіки. Глобальний ринок демонструє стійке зростання з прогнозом понад 500 млрд доларів до 2030 року. Український ринок, незважаючи на невелику частку у глобальному масштабі, характеризується високими темпами розвитку та унікальним досвідом протидії складним кіберзагрозам.

Ключовим викликом залишається критичний дефіцит кваліфікованих кадрів. Дефіцит виникає внаслідок взаємодії численних факторів: неспівмірності темпів зростання попиту та пропозиції, високих перешкод входу у професію, недоліків системи освіти та професійної підготовки, демографічних невідповідностей, труднощів з утриманням кадрів. Для України ці глобальні виклики доповнюються специфічними національними чинниками, зокрема впливом геополітичної ситуації та міграційних процесів.

Аналіз вимог до компетенцій фахівців демонструє необхідність володіння широким спектром знань і навичок. Технічні компетенції становлять основу професійної діяльності, водночас зростає значення загальних навичок, особливо комунікації, вирішення проблем та командної роботи. Стандартизовані рамки компетенцій, такі як рамка NICE, відіграють критичну роль у систематизації вимог до фахівців.

Динамічний характер галузі вимагає від професіоналів постійного оновлення знань і готовності до навчання протягом усієї професійної діяльності. Успішні фахівці повинні демонструвати здатність адаптуватися до нових викликів, інтегрувати технічні та соціальні навички, ефективно співпрацювати в міждисциплінарних командах.

Аналіз світових та українських тенденцій ринку праці виявляє критичний дефіцит кваліфікованих фахівців, який продовжує поглиблюватися. Український ринок кібербезпеки демонструє вражаючу динаміку зростання, збільшившись у чотири рази за останні вісім років та досягнувши 138 млн доларів у 2024 році.

Високий попит призвів до значного зростання рівня заробітних плат як на глобальному рівні, так і в Україні.

Подолання викликів вимагає комплексного підходу, що включає реформування освітніх програм, розвиток систем безперервного навчання, створення сприятливих умов для входу в професію молодих спеціалістів та залучення різноманітних груп населення до галузі кібербезпеки. Український досвід протистояння кіберзагрозам у воєнних умовах є унікальним і може стати основою для розвитку конкурентоспроможної національної індустрії кібербезпеки та підготовки висококваліфікованих спеціалістів для внутрішнього та міжнародного ринків.

РОЗДІЛ 2
МЕТОДИ ПОДОЛАННЯ КАДРОВОГО ДЕФІЦИТУ В КІБЕРБЕЗПЕЦІ

2.1 Освітні програми та ініціативи в галузі кібербезпеки

Освітні програми та ініціативи становлять фундаментальну основу для подолання дефіциту кадрів у галузі кібербезпеки. Враховуючи критичний розрив між попитом на фахівців та їх пропозицією на ринку праці, розвиток різноманітних освітніх траєкторій – від традиційних університетських програм до інтенсивних буткемп-курсів і професійних сертифікацій, є стратегічно важливим для забезпечення галузі кваліфікованими кадрами. Сучасний ландшафт освіти в кібербезпеці характеризується різноманітністю підходів, форматів навчання і акредитованих програм, що дозволяє задовольнити потреби як початківців, так і досвідчених професіоналів.

Університетські програми з кібербезпеки. Університетські програми з кібербезпеки становлять традиційну та найбільш фундаментальну форму освіти в галузі. Провідні університети світу розробили комплексні навчальні програми, які поєднують теоретичні знання з практичними навичками, необхідними для успішної кар'єри в кібербезпеці.

Провідні університети США розробили комплексні навчальні програми, які поєднують теоретичні знання з практичними навичками. Університет Карнегі-Меллона, визнаний Агентством національної безпеки та Департаментом внутрішньої безпеки як Національний центр академічної досконалості, пропонує магістерську програму з інформаційної безпеки, що інтегрує технічні, управлінські та політичні аспекти [65, 66].

Технологічний інститут Джорджії створив у 2020 році спеціалізовану Школу кібербезпеки і приватності з міждисциплінарним підходом та магістерською онлайн-програмою для практиків, яка включає три спеціалізовані напрями [67, 68]. Массачусетський технологічний інститут та Стенфордський

університет також входять до топ-університетів, поєднуючи дослідження у галузі ШІ, комп'ютерних наук та кібербезпеки [69, 70] (Табл. 2.1).

Таблиця 2.1

Топ-6 університетських програм з кібербезпеки у США (2024-2025)

Рей-тинг	Університет	Програма	Тривалість	Вартість (орієнтовна)
1	Університет Карнегі-Меллона	MS Information Security	2 роки	$50,000/рік
2	Технологічний інститут Джорджії	MS Cybersecurity	2-3 роки	$10,000-20,000
3	Массачусетський технологічний інститут	PhD/MS programs	2-5 років	$55,000/рік
4	Стенфордський університет	MS Cybersecurity	2 роки	$60,000/рік
5	Каліфорнійський університет у Берклі	MICS	20 місяців	$64,000 загалом
6	Університет Меріленду	MS Cybersecurity	2 роки	$10,000-20,000/рік

Практична складова університетських програм реалізується через участь студентів у змаганнях з кібербезпеки. Наприклад, студентська команда з комп’ютерної безпеки (PPP) та провідна студентська команда з кібербезпеки та змагань постійно демонструє видатні результати на престижних змаганнях, таких як DEF CON та MITRE eCTF [20]. Технологічний інститут Джорджії також відзначається послідовними перемогами у завданнях розшифрування коду (NSA Codebreaker Challenge), де студенти демонструють передові навички у реверс інженерінгу, програмуванні та аналізі вразливостей [20].

Онлайн-програми провідних університетів. Розвиток онлайн-освіти суттєво розширив доступність університетських програм з кібербезпеки.

Технологічний інститут Джорджії пропонує повністю дистанційну програму, яка дозволяє працюючим фахівцям здобувати освіту без відриву від роботи, з можливістю завершення програми за 2-3 роки [6]. UC Berkeley також надає онлайн-доступ до своєї програми MICS, що робить елітну освіту доступною для студентів з різних географічних локацій [2].

Онлайн-формат не означає зниження якості навчання. Програми включають живі лекції з викладачами, інтерактивні лабораторні заняття, групові проєкти та регулярне спілкування з менторами [25]. Випускники онлайн-програм отримують такі ж дипломи, як і студенти очних програм, що підтверджує рівність освітніх результатів.

Професійні сертифікації в кібербезпеці. Професійні сертифікації відіграють критичну роль у галузі кібербезпеки, слугуючи валідатором компетенцій та відкриваючи двері до кар'єрних можливостей. Сертифікації є особливо важливими для фахівців, які не мають формальної університетської освіти в галузі кібербезпеки, але володіють практичними навичками.

Сертифікований професіонал з безпеки інформаційних систем (CISSP) від (ISC)² вважається найбільш затребуваною сертифікацією у галузі кібербезпеки [3]. CISSP охоплює широкий спектр доменів кібербезпеки, включаючи управління безпекою і ризиками, безпеку активів, операції безпеки та розробку безпечного програмного забезпечення. Сертифікація вимагає п'ятирічного досвіду роботи у двох або більше доменах CISSP [42]. Середня заробітна плата власників CISSP у США становить $151,860 на 2024 рік [3].

Сертифікований етичний хакер (CEH) від EC-Council є спеціалізованою сертифікацією, яка демонструє навички етичного хакінгу, тестування на проникнення та виявлення вразливостей [43]. CEH вимагає двох років досвіду роботи в інформаційній безпеці або проходження офіційного навчання EC-Council [44]. Середня заробітна плата для власників CEH становить близько $134,217 [3].

CompTIA Security+ є базовою сертифікацією початкового рівня, яка підтверджує фундаментальні знання в галузі кібербезпеки [45]. Оновлена у

листопаді 2023 року, ця сертифікація особливо корисна для тих, хто має певний досвід у IT та прагне побудувати кар'єру в кібербезпеці. Security+ не вимагає попереднього досвіду, але рекомендується мати принаймні два роки роботи з акцентом на безпеку (Табл. 2.2) [44].

Таблиця 2.2

Порівняння провідних сертифікацій з кібербезпеки

Сертифікація	Організація	Вимоги до досвіду	Вартість іспиту	Середня зарплата (США)	Термін дії
Сертифікований фахівець з безпеки інформаційних систем	(ISC)²	5 років	$699	$151,860	3 роки
Сертифікований етичний хакер	EC-Council	2 роки	$1,199	$134,217	3 роки
Сертифікований менеджер з інформаційної безпеки	ISACA	5 років	$575	$145,000	3 роки
Сертифікат CompTIA з основ кібербезпеки	CompTIA	Немає*	$392	$70,000-90,000	3 роки
Сертифікований аудитор інформаційних систем	ISACA	5 років	$575	$132,000	3 роки
Сертифікований фахівець з безпеки хмарних технологій	(ISC)²	5 років IT + 1 рік хмара	$599	$114,172	3 роки
Сертифікований фахівець з тестування на проникнення (Offensive Security)	Offensive Security	Немає	$1,649	$120,000	Довічно
Сертифікат GIAC з основ інформаційної безпеки	GIAC/SANS	Немає	$2,499	$105,000	4 роки

Вибір оптимальної траєкторії сертифікації. Вибір сертифікації має відповідати поточному рівню досвіду і кар'єрним цілям фахівця. Для початківців рекомендується розпочинати з CompTIA Security+, яка забезпечує базові знання та є визнаною точкою входу в галузь [46]. Після здобуття початкового досвіду фахівці можуть обирати між технічною траєкторією (CEH, OSCP, GPEN для спеціалістів з тестування на проникнення і SOC або управлінською траєкторією (CISSP, CISM, CISA для керівних позицій) [47].

Важливо відзначити, що різні сертифікації мають різну вагу в очах HR-відділів і технічних менеджерів. HR часто шукають відомі акроніми, такі як CISSP, CEH, Security+, тоді як технічні керівники можуть більше цінувати практичні навички, підтверджені сертифікаціями типу OSCP [48]. Фахівці часто комбінують різні підходи, наприклад, починаючи з Security+, а потім обираючи технічний або управлінський шлях залежно від своїх цілей.

Фінансові переваги сертифікацій. Інвестиції в сертифікації мають значну фінансову віддачу. Сертифіковані фахівці початкового рівня зазвичай заробляють на 15-20% більше, ніж їхні несертифіковані колеги [49]. Для власників CISSP діапазон зарплат може перевищувати $150,000, а спеціалізовані сертифікації в хмарній безпеці або тестуванні на проникнення часто пропонують преміальні компенсаційні пакети [49]. Володіння кількома сертифікаціями може мати кумулятивний ефект на заробітну плату, роблячи стратегію "накопичення сертифікацій" вигідним кар'єрним рішенням [49].

Інтенсивні навчальні курси/табори (bootcamps). Bootcamps стали революційним явищем в освіті з кібербезпеки, пропонуючи інтенсивні та сфокусовані програми навчання, які обіцяють перетворити початківців на готових до роботи експертів за лічені місяці [50]. З понад 700 тисяч незаповнених позицій з кібербезпеки в США та прогнозованим зростанням робочих місць на 32% протягом наступних восьми років, попит на швидкі шляхи входу в професію є критично високим [50].

Bootcamp-програми характеризуються високою інтенсивністю навчання, практичним підходом і швидким отриманням результатів. Типова тривалість

bootcamp становить від 12 до 26 тижнів залежно від формату навчання (повний і частковий робочий день) [51]. Програми включають живі онлайн-класи з досвідченими інструкторами, практичні лабораторні роботи, групові проєкти та підготовку до професійних сертифікацій.

Провідні bootcamp-програми. Інтенсивний курс з кібербезпеки від Fullstack Academy є авторизованим партнером CompTIA і пропонує високоінтенсивну інтерактивну програму навчання [52]. Програма доступна у повному (13 тижнів) і частковому форматах, охоплює підготовку до іспиту CompTIA Security+ і надає безкоштовний ваучер на одну спробу складання іспиту для кваліфікованих студентів [52]. Вартість програми становить близько $14,950 з можливістю розстрочки оплати.

Кібербезпековий bootcamp школи Flatiron пропонує комплексне навчання для осіб, які прагнуть кар'єри в кібербезпеці, з опціями повного дня (15 тижнів) та часткового дня (40 тижнів), починаючи від $9,500 [53]. Навчальна програма охоплює базові навички, мережеву безпеку, корпоративну безпеку, скриптинг на Python, тестування на проникнення і криптографію, завершуючись підсумковим проєктом. Випускники підготовлені до виконання таких ролей як Інженер з кібербезпеки, аналітик з безпеки, фахівець з пентестингу та консультант з безпеки, з показником працевлаштування 69% серед випускників [53].

Bootcamp з кібербезпеки від TripleTen, пропонує семимісячну програму з гарантією працевлаштування [27]. Програма включає навчання найновішим технологіям безпеки та методологіям, охоплюючи як технічні навички (загрози від шкідливого ПЗ, контроль мережевої безпеки, криптографія), так і м’які навички (управління ризиками, критичне мислення, комунікація). Понад 80% випускників знаходять повну зайнятість завдяки гнучкості програми без жорсткого графіку занять (Табл. 2.3) [27].

Порівняння bootcamp з традиційною освітою. Bootcamp-програми відрізняються від традиційних університетських програм за кількома ключовими параметрами. По-перше, це швидкість здобуття освіти: такі курси дозволяють отримати необхідні навички за 3-8 місяців порівняно з 2-4 роками

університетської освіти [55]. По-друге, це вартість: типовий bootcamp коштує $10,000-15,000, що є лише частиною вартості традиційного ступеня [55].

Таблиця 2.3

Порівняння провідних bootcamp-програм з кібербезпеки (2024-2025)

Bootcamp	Тривалість	Формат	Вартість	Сертифікації	Гарантія працевлаштування
Fullstack Academy	13-26 тижнів	Онлайн	$14,950	CompTIA Security+	Ні
Flatiron School	15-40 тижнів	Онлайн/ очно	від $9,500	Різні	Ні
TripleTen	7 місяців	Онлайн	~$15,000	Різні	Так (10 міс.)*
Springboard	6 місяців	Онлайн	$9,900	CompTIA Security+	Так
Nucamp	15 тижнів	Онлайн	$2,604	Різні	Ні
BrainStation	12 тижнів	Онлайн	~$15,000	Cybersecurity CC™	Ні
Програми Каліфорнійського університету в Берклі	24 тижні	Онлайн/ очно	$11,995	Різні	Ні

Водночас, bootcamps мають і обмеження. Вони фокусуються на практичних навичках і підготовці до конкретних ролей, але не надають широкого теоретичного фундаменту, який пропонують університети [28]. Bootcamp найкращим чином підходять для кар'єрних «світчерів», які вже мають певний професійний досвід, або тих, хто прагне швидко ввійти в галузь на початкових позиціях [28].

Багато bootcamps пропонують додаткові послуги підтримки кар'єри, включаючи допомогу у створенні резюме, підготовку до співбесід, менторство

та доступ до мережі випускників і партнерів-роботодавців [29]. Деякі програми, такі як TripleTen та Springboard, навіть пропонують гарантії працевлаштування, повертаючи частину або всю вартість навчання, якщо випускник не знаходить роботу протягом певного періоду після завершення програми [91, 98].

Розглянуті освітні траєкторії – університетські програми, професійні сертифікації та інтенсивні bootcamp-курси – формують різноманітні індивідуальні шляхи входу в професію. Проте їх ефективність значно посилюється завдяки системній підтримці з боку держави та приватного сектору. Саме координована взаємодія освітніх закладів, корпорацій та державних інституцій створює комплексну екосистему підготовки кадрів, здатну забезпечити як масштабність, так і якість навчання фахівців з кібербезпеки.

2.2 Роль бізнесу та держави в підготовці кіберфахівців

Корпоративні програми навчання та розвитку. Провідні технологічні компанії розуміють, що інвестиції у власні програми навчання є необхідністю для забезпечення якісного кадрового потенціалу. Компанія Google запустила програму сертифікації з кібербезпеки на платформі Coursera, яка надає доступну та якісну освіту для широкого кола зацікавлених осіб [58]. Програма розрахована на початківців і не вимагає попереднього досвіду в IT. За 6 місяців навчання студенти отримують практичні навички та підготовку до початкових позицій у галузі кібербезпеки.

Microsoft розробила ініціативу навчання з кібербезпеки, яка включає безкоштовні курси, навчальні модулі та ресурси для підготовки до сертифікацій Microsoft [59]. Компанія також пропонує стипендіальні програми для студентів з недостатньо представлених груп населення та жінок. Програма Microsoft Cybersecurity Scholarship надає доступ до навчальних ресурсів, менторства та можливостей працевлаштування.

Cisco Systems традиційно є лідером у галузі мережевих технологій та кібербезпеки. Програма Cisco Networking Academy пропонує широкий спектр

курсів з кібербезпеки, включаючи підготовку до сертифікації Cisco Certified CyberOps Associate [60]. Програма доступна через мережу навчальних центрів по всьому світу і охоплює мільйони студентів щороку.

IBM створила програму IBM Security Learning Academy, яка пропонує навчальні курси, лабораторні роботи і сертифікації з різних аспектів кібербезпеки [61]. Компанія також підтримує освітні ініціативи для студентів та викладачів, надаючи доступ до передових технологій безпеки та дослідницьких ресурсів.

Корпоративні програми навчання демонструють високу ефективність у підготовці кадрів. За даними 2024 року, випускники Google Cybersecurity Certificate мають рівень працевлаштування 75% протягом шести місяців після завершення програми. Сукупно програми провідних технологічних компаній забезпечують підготовку понад 50,000 фахівців щороку, значно доповнюючи традиційні академічні траєкторії. Особливістю корпоративних програм є їх практична орієнтованість та пряма інтеграція з потребами індустрії, що забезпечує випускникам швидку адаптацію до робочих завдань.

Партнерство між бізнесом та освітніми закладами. Успішна модель підготовки кадрів передбачає тісну співпрацю між роботодавцями та навчальними закладами. Програми стажування і практики дозволяють студентам отримати реальний досвід роботи, водночас допомагаючи компаніям виявити та залучити талановиту молодь [30]. Провідні університети встановлюють партнерські відносини з технологічними компаніями для створення спільних освітніх програм, які відповідають актуальним потребам індустрії.

Модель дуальної освіти, популярна в Німеччині та Швейцарії, передбачає поєднання теоретичного навчання в університеті з практичною роботою на підприємстві [4]. Студенти проводять частину часу в навчальному закладі, а частину – працюючи в компаніях-партнерах, де вони застосовують отримані знання на практиці. Ця модель довела свою ефективність у підготовці кваліфікованих спеціалістів, які готові до роботи відразу після закінчення навчання.

Консультативні ради з представників галузі при університетах допомагають узгоджувати навчальні програми з потребами ринку праці [64]. Представники компаній беруть участь у розробці курсів, надають зворотний зв'язок щодо компетенцій випускників та сприяють працевлаштуванню студентів.

Державні ініціативи та програми фінансування. Уряди провідних країн визнають кібербезпеку стратегічним пріоритетом та інвестують значні ресурси у розвиток кадрового потенціалу. У США федеральна програма CyberCorps: Scholarship for Service надає стипендії студентам, які навчаються за програмами кібербезпеки в акредитованих університетах [5]. В обмін на фінансування освіти випускники зобов'язуються працювати у федеральних, державних або місцевих урядових установах протягом певного періоду після завершення навчання.

Національна ініціатива з освіти у кібербезпеці (NICE) координує зусилля уряду, академічних установ та приватного сектору для вирішення проблеми дефіциту кадрів [33]. NICE розробила рамку компетенцій, яка стандартизує вимоги до різних ролей у кібербезпеці та допомагає узгоджувати освітні програми з потребами індустрії.

Федеральний уряд США розробив комплекс програм фінансової підтримки для різних категорій учасників - від студентів до діючих державних службовців. Ці програми охоплюють повне покриття навчання, стипендії, можливості працевлаштування та погашення освітніх кредитів (Табл. 2.4).

Європейський Союз запустив ініціативу EU Cybersecurity Skills Framework, спрямовану на розвиток єдиного підходу до підготовки фахівців з кібербезпеки в країнах-членах [20]. Програма включає фінансування освітніх проєктів, підтримку наукових досліджень та сприяння мобільності студентів і викладачів між країнами ЄС.

Таблиця 2.4

Основні федеральні програми США з розвитку кадрів кібербезпеки

Програма	Організатор	Цільова аудиторія	Основні переваги	Фінансова підтримка
CyberCorps: Scholarship for Service	NSF	Студенти коледжів і університетів	Повне покриття навчання, стипендії, гарантоване працевлаштування	До $75,000 на навчання + стипендія
Cybersecurity & AI Talent Initiative	Partnership for Public Service	Випускники в галузі кібербезпеки та ШІ	Досвід роботи в державному і приватному секторі	До $75,000 на погашення кредитів
Federal Rotational CyberWorkforce	OPM	Федеральні співробітники IT/кібербезпеки	Ротації 6-12 міс., розвиток навичок	Оплачувана робота
DHS Cybersecurity Apprenticeship	DHS	Студенти бакалаврату / магістратури	Робота 16-20 год/тиждень.	Оплачувана часткова зайнятість
NSA GenCyber	NSA	Учні середніх шкіл	Літні табори, практичне навчання	Безкоштовна участь

В Україні держава також розвиває програми підтримки освіти в галузі кібербезпеки. Держспецзв'язку активно співпрацює з навчальними закладами, надаючи методичну підтримку та сприяючи впровадженню сучасних стандартів навчання [6]. Окрім того, створюються спеціалізовані центри кібербезпеки при провідних університетах, які отримують державне фінансування та підтримку міжнародних партнерів.

Міжнародна співпраця й обмін досвідом. Глобальний характер кіберзагроз вимагає міжнародної співпраці у підготовці кадрів. Програми акаде мічної

мобільності дозволяють студентам та викладачам обмінюватися досвідом, навчатися в провідних університетах інших країн та встановлювати професійні контакти [7]. Спільні дослідницькі проєкти між університетами різних країн сприяють розвитку наукового потенціалу та поширенню кращих практик.

Особливо ефективними є програми учнівства (apprenticeship), які поєднують державне фінансування з галузевою експертизою приватного сектору. Американський досвід демонструє різноманітність моделей державно-приватного партнерства у підготовці кадрів для кібербезпеки (Табл. 2.5).

Таблиця 2.5

Приклади успішних державно-приватних партнерств у США

Ініціатива	Партнери	Цільова група	Формат	Результати
Cybersecurity Talent Initiative	Partnership for Public Service, федеральні агентства, корпорації	Випускники	Почергово, кожні 2 роки: державний і приватний сектор)	$75 000 на студентські кредити
DHS Cybersecurity Apprenticeship	DHS, CISA, ICE, Secret Service	Студенти	Часткова зайнятість 16-20 год на тиждень	Можливість повної зайнятості, працевлаш-тування
PITOC IT Apprenticeship	JEVS, Філадельфія бізнес, державні агентства	Кар'єрні «світчери»	Група-спонсоровані програми	Перша програма IT-стажування в Пенсильванії

Продовження табл. 2.5

California zSystems Program	IBM, CDT, державні агенції Каліфорнії	Державні службовці	Тренінг + робота	Заповнення 18.6% вакансій
NICE Apprenticeship Working Group	NIST, понад 100 організацій	Усі зацікавлені сторони	Координацій-на платформа	Обмін кращими практиками

Міжнародні організації, такі як OSCE, НАТО, ЄС, підтримують ініціативи з розвитку кібербезпеки, включаючи освітні програми та тренінги для фахівців [37]. Ці організації також надають технічну та фінансову допомогу країнам, які розвивають власні системи кібербезпеки.

2.3 Профорієнтаційні та STEM-програми для молоді

Залучення молоді до галузі кібербезпеки на ранніх етапах освіти є критично важливим для формування сталого кадрового резерву. Профорієнтаційні програми та ініціативи у сфері STEM-освіти допомагають учням та студентам зацікавитися кібербезпекою, розвинути необхідні навички та зробити усвідомлений вибір кар'єри [2].

Програми для школярів (K-12). CyberPatriot є найбільшою молодіжною освітньою програмою з кібербезпеки в США, яку організовує Асоціація Повітряних і Космічних Сил [9]. Програма пропонує змагання для учнів середніх та старших класів, де команди вирішують реалістичні завдання з кібербезпеки. CyberPatriot залучає понад 6,700 команд з усіх штатів США та декількох країн світу.

GenCyber – федеральна програма літніх таборів, фінансована NSA і NSF, надає безкоштовне навчання з кібербезпеки для учнів та вчителів [73]. Програма організовує понад 100 безкоштовних літніх таборів щорічно, фокусуючись на

розвитку базових знань та залученні дівчат і представників недостатньо представлених груп населення.

picoCTF – безкоштовна комп'ютерна гра з кібербезпеки від Університету Карнегі-Меллона, призначена для учнів середніх класів [74]. Гра залучає понад 100 тис. учасників щороку, навчаючи основам кібербезпеки через формат Capture The Flag.

Національні та федеральні програми США формують розгалужену систему профорієнтації з кібербезпеки для молоді різного віку. Основні програми охоплюють мільйони учнів та студентів щороку, пропонуючи різноманітні формати навчання – від змагань до літніх таборів (Таблиця 2.6).

Таблиця 2.6

Основні національні програми профорієнтації з кібербезпеки для молоді

Програма	Організатор	Цільова аудиторія	Охоплення (2024)	Формат	Фінансування
CyberPatriot	Air Force Association	K-12, 6-12 класи	1,500+ команд	Змагання + навчання	Безкоштовно
GenCyber	NSA/NSF	Учні 6-12 класів, вчителі	100+ таборів/рік	Літні табори	Федеральне
CyberStart America	SANS Institute	13-18 років	Національне	Онлайн-гра	Безкоштовно
National Cyber League	NCL	Середня школа, коледж	10,000+ учасників	Онлайн-змагання	$35-395
picoCTF	Carnegie Mellon	Середня-старша школа	Глобальне	CTF змагання	Безкоштовно
US Cyber Challenge	NICE/SANS	14-22 роки	Регіональне	Змагання + табори	Безкоштовно

Літні табори та інтенсивні програми від університетів. Провідні університети США розробили спеціалізовані літні програми і табори з кібербезпеки для учнів середньої та старшої школи, надаючи їм ранній доступ до університетських ресурсів та експертизи.

Массачусетський технологічний інститут (MIT) пропонує кілька програм для обдарованої молоді. Літній інститут MIT Beaver Works включає чотиритижневий інтенсивний курс з кібербезпеки, де студенти працюють над реальними проектами під керівництвом викладачів MIT та менторів зі сфери кібербезпеки [81]. Програма покриває теми від основ мережевої безпеки до просунутої криптографії та аналізу зловмисного програмного забезпечення.

Мічиганський технологічний університет проводить літні програми для молоді з кібербезпеки, яка дозволяє учням старшої школи отримати досвід університетського рівня навчання [82]. Учасники проживають у кампусі, відвідують лекції та лабораторії, працюють над груповими проектами та взаємодіють зі студентами університету. Крім національних програм та університетських ініціатив, важливу роль у профорієнтації відіграють регіональні та локальні проєкти.

Регіональні та локальні ініціативи. Багато університетів і коледжів організовують регіональні програми для представників місцевих спільнот. Ці програми часто більш доступні для студентів, які не можуть подорожувати на національні заходи, й адаптовані до специфічних потреб регіону.

Деякі університети співпрацюють з місцевими школами для створення програм подвійного зарахування (dual enrollment), де учні старших класів можуть відвідувати університетські курси з кібербезпеки й отримувати кредити, які зараховуються як для школи, так і для майбутнього навчання в університеті [46]. Це дозволяє мотивованим учням розпочати свою освіту в кібербезпеці раніше та заощадити час і гроші на майбутньому навчанні.

Ініціативи з диверсифікації та включеності для жінок і меншин. Враховуючи значний гендерний та етнічний дисбаланс у галузі кібербезпеки,

багато організацій розробили цільові програми для залучення недостатньо представлених груп.

Girls Go CyberStart є національною програмою, спеціалізовано розробленою для заохочення дівчат віком 13-18 років досліджувати кібербезпеку [47]. Програма використовує ігрову платформу для навчання основним концепціям кібербезпеки в дружній та підтримуючій атмосфері. Учасниці можуть виграти стипендії та отримати доступ до менторських програм.

Women in Cybersecurity (WiCyS) організовує програми для дівчат і жінок будь-якого віку, включаючи шкільні семінари, університетські змагання та професійні конференції [48].

Неурядова організація Diversity Cyber Council фокусується на залученні представників етнічних меншин до кібербезпеки через освітні програми, менторство та адвокацію [49]. Організація працює зі школами у спільнотах з переважанням меншин, надаючи ресурси, тренінги й доступ до кіберпрактиків.

Програми доступності для студентів з обмеженими можливостями, такі як Accessible Computing Education (ACE) та подібні ініціативи, працюють над забезпеченням того, щоб освіта з кібербезпеки була доступною для студентів з інвалідністю [50]. Це включає адаптацію навчальних матеріалів, використання доступних технологій і створення інклюзивних навчальних середовищ.

2.4 Автоматизація, аутсорсинг і перекваліфікація як засоби компенсації дефіциту кадрів

Розглянуті освітні програми, державні ініціативи та молодіжні проєкти є довгостроковими стратегіями подолання кадрового дефіциту, результати яких проявляються через роки систематичної роботи. Водночас організації стикаються з нагальною потребою захисту своїх систем уже сьогодні. Тому паралельно з довгостроковими освітніми стратегіями застосовуються тактичні рішення для оперативної компенсації кадрового дефіциту: автоматизація

процесів безпеки, аутсорсинг спеціалізованих функцій та перекваліфікація ІТ-фахівців з інших напрямків.

Автоматизація процесів кібербезпеки. Технології ШІ та МН революціонізують сферу кібербезпеки, дозволяючи автоматизувати значну частину рутинних завдань, які традиційно вимагали участі висококваліфікованих фахівців. За оцінками аналітиків, застосування ШІ та МН може зменшити навантаження на команди безпеки на 30-40%, дозволяючи наявним спеціалістам зосередитися на складних і стратегічних завданнях [51].

Системи виявлення аномалій на базі МН здатні аналізувати величезні обсяги даних про мережевий трафік, поведінку користувачів та активність систем, ідентифікуючи підозрілі шаблони, які можуть вказувати на кіберзагрози. На відміну від традиційних сигнатурних методів, ШІ-системи можуть виявляти невідомі раніше загрози (zero-day attacks) шляхом аналізу відхилень від нормальної поведінки [52]. Це особливо важливо в умовах постійної еволюції тактик кіберзлочинців.

Автоматизоване реагування на інциденти (SOAR) - це інтегровані платформи, які координують дії різних інструментів безпеки та автоматизують процеси реагування на загрози [53]. SOAR-рішення можуть автоматично ізолювати скомпрометовані системи, блокувати шкідливі IP-адреси, збирати криміналістичні дані та виконувати інші дії без втручання людини, значно скорочуючи час реакції на інциденти з годин до хвилин (Табл. 2.7) [53].

Обмеження та виклики автоматизації. Незважаючи на значний потенціал, автоматизація має свої обмеження. ШІ-системи потребують великих обсягів якісних даних для навчання та можуть генерувати помилкові спрацювання, які вимагають верифікації людиною [92]. Крім того, надмірна залежність від автоматизації може призвести до атрофії навичок у фахівців, які втрачають здатність ручного аналізу загроз.

Дані таблиці 2.7 базуються на галузевих звітах провідних аналітичних компаній та результатах впровадження автоматизованих рішень у організаціях різного масштабу [27]. Найбільш значний ефект автоматизація демонструє у

сферах з високим рівнем рутинних операцій, тоді як складні аналітичні завдання і стратегічне планування безпеки ще вимагають участі кваліфікованих фахівців.

Таблиця 2.7

Ключові сфери застосування автоматизації в кібербезпеці

Сфера застосування	Технології	Рівень автоматизації	Скорочення навантаження на персонал
Виявлення загроз	ШІ та МН, поведінковий аналіз	70-80%	40-50%
Моніторинг та аналіз логів	SIEM зі ШІ, автоматична кореляція	60-70%	35-45%
Реагування на інциденти	SOAR платформи	50-60%	30-40%
Управління вразливостями	Автоматичне сканування і пріоритезація	80-90%	50-60%
Аналіз шкідливого ПЗ	«Пісочниці», МН-класифікація	70-80%	40-50%
Управління патчами	Автоматичне тестування і розгортання	85-95%	60-70%
Моніторинг відповідності	Автоматичні перевірки відповідності	75-85%	45-55%

Аутсорсинг функцій кібербезпеки. Керовані послуги безпеки (MSSP) надають організаціям доступ до експертизи з кібербезпеки без необхідності утримувати повноцінну внутрішню команду [25]. MSSP-провайдери пропонують широкий спектр послуг, включаючи цілодобовий моніторинг безпеки, управління міжмережевими екранами та системами виявлення вторгнень, реагування на інциденти та консультування з питань безпеки.

Для малих і середніх організацій, які не мають ресурсів для найму власних фахівців з кібербезпеки, MSSP є привабливим рішенням [3]. Навіть великі

організації можуть використовувати MSSP для доповнення своїх внутрішніх команд, особливо для покриття спеціалізованих областей або забезпечення цілодобового моніторингу.

Ринок керованих послуг безпеки стрімко зростає, що відображає попит на такі рішення. За прогнозами аналітиків, глобальний ринок MSSP зросте з $46,4 млрд у 2023 році до $77,0 млрд у 2028 році [42]. Провідні MSSP-провайдери включають IBM Security, Secureworks, Trustwave та багато інших спеціалізованих компаній.

Програми перекваліфікації та внутрішнього розвитку. Перекваліфікація працівників з інших галузей IT або навіть з неполітехнічних сфер є перспективною стратегією для подолання дефіциту кадрів [43]. Організації можуть інвестувати у навчання своїх існуючих працівників, розвиваючи їхні компетенції в галузі кібербезпеки. Це не лише вирішує проблему нестачі кадрів, але й підвищує лояльність працівників та утримання талантів.

Внутрішні програми навчання та розвитку дозволяють працівникам освоювати нові навички без відриву від роботи [44]. Компанії можуть створювати індивідуальні траєкторії навчання, що враховують поточний рівень знань працівників та їхні кар'єрні цілі. Менторство та shadowing (спостереження за роботою досвідчених колег) також є ефективними методами передачі знань.

Деякі організації запроваджують програми ротації, де працівники з інших відділів можуть тимчасово приєднатися до команди кібербезпеки для отримання досвіду [45]. Це допомагає виявити прихований потенціал і зацікавити працівників у переході на постійні позиції в кібербезпеці. Крім того, така практика сприяє кращому розумінню питань безпеки по всій організації.

Гібридні моделі та гнучкість. Багато організацій використовують гібридні підходи, поєднуючи внутрішні команди з аутсорсингом та автоматизацією [81]. Наприклад, базовий моніторинг може здійснюватися автоматизованими системами і MSSP, тоді як складні інциденти розслідуються внутрішніми експертами. Така модель дозволяє оптимально використовувати обмежені кадрові ресурси.

Віддалена робота та гнучкі графіки також розширюють можливості для залучення кваліфікованих фахівців [82]. Організації, які пропонують віддалену роботу, мають доступ до глобального ринку талантів, не обмежуючись географічним розташуванням. Це особливо актуально для України, де багато фахівців працюють на міжнародні компанії, зберігаючи проживання в країні.

Висновки до розділу 2

Сучасний ландшафт освітніх програм з кібербезпеки характеризується різноманітністю підходів, форматів і рівнів складності, що дозволяє задовольнити потреби різних категорій учасників від початківців без технічного досвіду до досвідчених ІТ-фахівців, які прагнуть спеціалізуватися в кібербезпеці.

Університетські програми залишаються золотим стандартом освіти, надаючи фундаментальні теоретичні знання, дослідницький досвід і престижні дипломи від провідних закладів. Професійні сертифікації служать валідаторами компетенцій та відіграють критичну роль у кар'єрному просуванні, особливо для тих, хто не має формальної освіти в галузі. Bootcamp-програми пропонують швидкі, практично орієнтовані та відносно доступні шляхи входу в професію.

Комбінація різних освітніх траєкторій, наприклад, університетський диплом доповнений професійними сертифікаціями, або bootcamp-програма з подальшим здобуттям спеціалізованих сертифікацій, дозволяє фахівцям створювати оптимальний освітній шлях відповідно до їхніх кар'єрних цілей, фінансових можливостей і часових обмежень. Така гнучкість освітньої системи є ключовим фактором у подоланні дефіциту кадрів у галузі кібербезпеки.

Ролі держави та бізнесу в підготовці кадрів для галузі кібербезпеки є взаємодоповнюючими та критично важливими для подолання дефіциту фахівців. Державні ініціативи, зокрема галузеві освітні фреймворки, програми стипендій і федеральні програми розвитку, створюють стратегічну основу та забезпечують фінансову підтримку для масштабних освітніх проектів. Приватний сектор привносить галузеву експертизу, практичні навчальні програми та безпосередні

можливості працевлаштування через корпоративні тренінги, партнерські мережі та програми сертифікації.

Державно-приватні партнерства, особливо у форматі програм учнівства, демонструють високу ефективність у підготовці практично підготовлених до роботи фахівців, поєднуючи теоретичне навчання з практичним досвідом. Успішні приклади з досвіду інших країн підтверджують життєздатність цієї моделі. Водночас існують значні виклики, пов'язані з координацією численних ініціатив, оцінкою їх ефективності та масштабуванням успішних моделей.

Профорієнтаційні та STEM-програми для молоді становлять критично важливу складову довгострокової стратегії подолання дефіциту кадрів у галузі кібербезпеки. Національні ініціативи, такі як CyberPatriot та GenCyber, демонструють високу ефективність у залученні тисяч учнів до вивчення кібербезпеки через практично орієнтовані та захоплюючі формати навчання. Університетські літні програми та інтенсиви надають обдарованим студентам доступ до передових ресурсів та експертизи, готуючи їх до успішного продовження освіти в галузі.

Особлива увага до диверсифікації та включеності через цільові програми для жінок, меншин та студентів з обмеженими можливостями є критично важливою для розширення пайплайну талантів та формування більш інклюзивної галузі кібербезпеки. Водночас залишаються значні виклики, пов'язані з масштабуванням програм, забезпеченням їх доступності для всіх студентів незалежно від географії та соціально-економічного статусу, інтеграцією кібербезпеки в основні шкільні навчальні програми та довгостроковою оцінкою впливу ініціатив.

Паралельно з розвитком довгострокових освітніх стратегій організації застосовують тактичні рішення для оперативної компенсації кадрового дефіциту. Автоматизація процесів безпеки на базі ШІ та МН дозволяє скоротити навантаження на команди безпеки на 30-40%, даючи змогу наявним спеціалістам зосередитися на складних стратегічних завданнях. Керовані послуги безпеки (MSSP) надають організаціям, особливо малим та середнім, доступ до

експертизи з кібербезпеки без необхідності утримувати повноцінні внутрішні команди. Програми перекваліфікації ІТ-фахівців з інших спеціалізацій створюють додатковий канал поповнення кадрового резерву, дозволяючи організаціям розвивати власний персонал та підвищувати лояльність працівників.

Комплексне застосування всіх розглянутих підходів – від фундаментальної університетської освіти до тактичних рішень з автоматизації – формує багаторівневу систему протидії кадровому дефіциту в галузі кібербезпеки.

РОЗДІЛ 3
ОСОБЛИВОСТІ СУЧАСНОГО КАДРОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ ТА СВІТІ

3.1 Аналіз поточного стану: статистика, проблеми, виклики

Сучасний стан кадрового забезпечення кібербезпеки характеризується критичним дефіцитом фахівців як на глобальному, так і на національному рівнях. Аналіз актуальних статистичних даних та емпіричних досліджень дозволяє ідентифікувати масштаби проблеми, ключові виклики та бар'єри, що перешкоджають ефективному розвитку кадрового потенціалу галузі.

Глобальні масштаби кадрового дефіциту. За даними дослідження ISC2 Cybersecurity Workforce Study 2024, глобальна робоча сила у сфері кібербезпеки становить 5,47 млн осіб, що відображає мінімальне зростання лише на 0,1% порівняно з 2023 роком [61]. Це перша зупинка у зростанні робочої сили з 2019 року, що свідчить про серйозні системні проблеми галузі. Водночас, дефіцит кадрів досяг рекордного показника 4,76 млн фахівців, що на 19,1% більше порівняно з попереднім роком [65, 73].

Загальна потреба у фахівцях кібербезпеки на глобальному рівні оцінюється у 10,2 млн осіб, що означає необхідність збільшення робочої сили на 87% для задоволення поточного попиту [4]. За оцінками Boston Consulting Group (BCG) та Global Cybersecurity Forum, лише 72% необхідних позицій заповнені, при цьому близько 2,8 млн робочих місць залишаються вакантними [64]. Ситуація погіршується тим фактом, що 67% організацій повідомляють про дефіцит кадрів кібербезпеки, необхідних для запобігання інцидентам та усунення загроз [61].

Регіональні особливості кадрового дефіциту. Аналіз регіональної структури дефіциту виявляє значну нерівномірність. Найбільший дефіцит спостерігається у регіоні Азіатсько-Тихоокеанського басейну - 3,4 млн фахівців, що збільшилося з 2,7 млн за рік [4]. У Північній Америці дефіцит становить понад 500 000 фахівців, при цьому у США налічується більше 457 000 відкритих

позицій при загальній зайнятій робочій силі у 1,25 млн осіб, що становить дефіцит понад 25% [5].

У Європі дефіцит становить понад 347 000 фахівців, при цьому лише у Франції не вистачає майже 60 тис. експертів [33]. Тривожною тенденцією є те, що у 2024 році кількість фахівців з кібербезпеки скоротилася в кількох країнах, включаючи Канаду, Німеччину, Мексику, Великобританію та США. Зокрема, у Великобританії кількість спеціалістів зменшилася з 367 300 до 349 360 за рік (майже 5%), що є найбільшим скороченням у світі [30].

Стан кадрового забезпечення в Україні. В Україні ситуація з кадровим забезпеченням кібербезпеки також критична. За даними Українського інституту інформаційної безпеки, попит на фахівців кібербезпеки зростає на 15% щорічно. Прогнозується, що ринок кібербезпеки в Україні зростатиме на 8,54% щорічно з 2024 по 2029 рік, досягнувши обсягу 208,80 млн доларів США до 2029 року [6].

Особливістю української ситуації є значний вплив військових дій на ринок праці. З одного боку, російська агресія значно підвищила усвідомлення важливості кібербезпеки та стимулювала попит на відповідних фахівців. З іншого боку, мобілізація, еміграція та економічна нестабільність негативно вплинули на доступність кваліфікованих кадрів. Водночас, 72% українських компаній у сфері кібербезпеки запровадили віддалений або гібридний формат роботи, що дозволяє залучати талановитих фахівців з усієї країни [6].

Ключові причини кадрового дефіциту. Дослідження ISC2 2024 виявило зміну провідних причин дефіциту кадрів. Якщо у 2023 році головною причиною була неспроможність знайти необхідну кваліфіковану робочу силу або навички, то у 2024 році на перше місце вийшов брак бюджету (39% респондентів) [65, 80]. Це відображає вплив економічної нестабільності та скорочення фінансування на здатність організацій наймати та утримувати фахівців.

Серед інших значущих причин: неспроможність утримати людей з затребуваними навичками (26%), труднощі з розвитком та просуванням персоналу кібербезпеки (22%), брак кандидатів з необхідними навичками (44%), інтенсивна конкуренція за кваліфіковану робочу силу [65, 75]. Майже 20%

респондентів також очікують додаткових скорочень у сфері кібербезпеки протягом наступних 12 місяців [61].

Таблиця 3.1

Регіональний розподіл робочої сили та дефіциту кадрів кібербезпеки (2024)

Регіон	Робоча сила (млн)	Дефіцит (млн)	Зміна за рік (%)
Азіатсько-Тихоокеанський регіон	2,5	3,4	+3,8%
Північна Америка	1,3	0,5	-2,7%
Європа	1,2	0,35	-0,7%
Близький Схід та Африка	0,3	0,3	+7,4%
Латинська Америка	0,17	0,21	-0,9%
Всього у світі	5,47	4,76	+0,1%

Проблема дефіциту навичок. Окрім загального дефіциту кадрів, галузь стикається з критичною проблемою дефіциту навичок. За даними ISC2, 90% респондентів повідомили про дефіцит навичок у своїх організаціях, при цьому 58% вважають, що нестача навичок створює значний ризик для їх організацій [61]. Що важливіше, 64% стверджують, що дефіцит навичок є більшим викликом для захисту їх організацій, ніж загальний дефіцит персоналу [30].

П'ятьма найбільш дефіцитними навичками у організаціях є: безпека хмарних обчислень, ШІ та МН, впровадження zero-trust архітектури, безпека додатків, аналіз загроз та реагування на інциденти. Лише 15% організацій впевнені, що мають як достатню кількість людей, так і необхідні навички для досягнення своїх цілей кібербезпеки [5].

Економічні наслідки кадрового дефіциту. Дефіцит кадрів створює значні фінансові ризики для організацій. За даними дослідження Ponemon Institute 2024, середня прямі витрати від порушення безпеки становлять 4,88 млн доларів США, при цьому середня вартість зловмисної внутрішньої атаки ще вища - 4,99 млн

доларів США [37]. Середнє збільшення поточних витрат після порушення становить близько 830 000 доларів США [37].

Глобальні витрати від кіберзлочинності прогнозуються на рівні 9,5 трлн доларів США у 2024 році та понад 10,5 трлн доларів США до 2025 року [33]. За оцінками Світового економічного форуму, до 2030 року глобальний дефіцит кваліфікованої робочої сили може перевищити 85 млн працівників, що призведе до втрати 8,5 трлн доларів США нереалізованих щорічних доходів [2].

Виклики найму та утримання персоналу. Організації стикаються зі значними труднощами у заповненні вакансій. Майже половина (48%) всіх компаній витрачають понад 6 місяців на заповнення вакансії з кібербезпеки [4]. Лише 69% організацій мають фахівців початкового рівня у своїх командах кібербезпеки, при цьому у малих компаніях (до 500 співробітників) лише 64% пропонують позиції початкового рівня [4].

Майже третина (31%) команд кібербезпеки не має жодного члена початкового рівня, а 15% не мають представників молодшого рівня (1-3 роки досвіду) [5]. Більшість менеджерів з найму (62%) з відкритими вакансіями зосереджені на працевлаштуванні фахівців середнього та просунутого рівня [7]. Це створює "замкнене коло", коли молоді фахівці не можуть отримати необхідний досвід для просування, а організації продовжують відчувати дефіцит.

З*ниження задоволеності роботою.* Задоволеність роботою серед фахівців кібербезпеки неухильно знижується. У 2022 році 74% професіоналів були задоволені своєю роботою, у 2023 році цей показник знизився до 70%, а станом на 2024 рік впав ще на 4% до 66% [4]. Більше двох третин фахівців (68%) повідомляють, що їхні ролі значно більш стресові, ніж п'ять років тому, а 52% респондентів вважають, що бюджети їх організацій недостатні для задоволення поточних потреб кібербезпеки [9].

Таким чином, аналіз поточного стану кадрового забезпечення кібербезпеки показав багатогранну кризу, що характеризується одночасним дефіцитом кількості фахівців та необхідних навичок, погіршенням умов праці, зниженням задоволеності роботою та зростаючими фінансовими ризиками для організацій.

Ці виклики вимагають комплексного та координованого підходу на рівні урядів, освітніх закладів і приватного сектору для забезпечення стійкого розвитку галузі.

3.2 Приклади освітніх ініціатив з кібербезпеки в Україні

Україна, перебуваючи в умовах тривалої кібервійни, розвинула унікальну екосистему освітніх та практичних ініціатив у галузі кібербезпеки. Українські програми навчання та підготовки фахівців демонструють інноваційні підходи до подолання дефіциту кадрів, поєднуючи теоретичну підготовку з практичним досвідом протидії реальним кіберзагрозам. Розглянемо найбільш значущі українські ініціативи, які довели свою ефективність.

Програми Diia у сфері кібербезпеки. Платформа Diia, створена Міністерством цифрової трансформації України, стала не лише інструментом надання електронних державних послуг, але й важливою складовою національної системи кібербезпеки. У рамках ініціативи Cyber Diia Platform створено недержавну громадську асоціацію, яка об'єднує технологічні компанії, експертів та інноваторів для побудови стійкого цифрового майбутнього України [83]. Платформа надає доступ до широкої мережі експертів з кіберстійкості, випускників освітніх програм та провідних фахівців галузі.

На платформі Diia.Education розміщено низку спеціалізованих курсів з кібербезпеки, розроблених за ініціативи Міністерства цифрової трансформації України, Національного координаційного центру кібербезпеки та Національного університету «Києво-Могилянська академія» за підтримки програми USAID "Кібербезпека критичної інфраструктури в Україні" [74]. Освітні серії включають курси "Кібергігієна для молоді" та "Базові знання про кібергігієну", які охоплюють основні аспекти інтернет-безпеки, захисту персональних даних та уникнення кіберзагроз. Ці програми адаптовані для різних цільових аудиторій - від школярів до дорослого населення.

Важливим елементом державної підтримки є програма "Cyber Diagnostics Program for Businesses", яка надає малим та середнім підприємствам можливість

безкоштовно отримати одну з трьох послуг кібербезпечної діагностики їхньої цифрової інфраструктури через портал Diia.Business. Програма реалізується за підтримки Міністерства цифрової трансформації та Офісу розвитку підприємництва та експорту, що сприяє підвищенню рівня захищеності українського бізнесу від кіберзагроз.

CyberUnit.tech та практична підготовка фахівців. Компанія Cyber Unit Technologies є українською IT-компанією, що спеціалізується на наданні послуг та рішень у сфері кібербезпеки на основі практичного досвіду кібервійни. CyberUnit.tech активно займається освітніми ініціативами, організовуючи заходи та курси, що сприяють підвищенню рівня обізнаності з кібербезпеки. Компанія розробила та успішно впровадила платформу UnitRange.com, яка пропонує інноваційні освітні курси та є кіберполігоном для навчання спеціалістів. З 2022 року понад 3000 фахівців державного сектору та критичної інфраструктури України пройшли навчання на цій платформі [87].

Унікальний внесок CyberUnit.tech полягає у створенні української волонтерської кіберармії на початку повномасштабного вторгнення у лютому 2022 року [85]. До 2021 року компанія навчила понад 800 українських IT-експертів з більше ніж 30 державних організацій, пов'язаних з критичною інфраструктурою України, підготовляючи їх до захисту країни в умовах кібервійни. Це демонструє модель швидкої мобілізації кадрового потенціалу у кризовій ситуації, що може бути корисним досвідом для інших країн.

Академічні ініціативи та університетські програми. В Україні активно розвивається система академічної підготовки фахівців з кібербезпеки. Станом на 2025 рік понад 60 закладів вищої освіти пропонують програми за спеціальністю "Кібербезпека та захист інформації" [90]. Серед провідних університетів виділяються Національний технічний університет України "КПІ імені Ігоря Сікорського", Національний авіаційний університет, Київський національний університет імені Тараса Шевченка, які пропонують акредитовані освітні програми всіх рівнів: від бакалаврату до докторантури.

Важливу роль відіграють спеціалізовані навчальні заклади та приватні академії. Міжнародна Кібер Академія співпрацює з університетами для посилення академічних програм цифрового розвитку і кібербезпеки, надаючи доступ до знань та кращих міжнародних практик [120]. Академія працює з державними інституціями, підприємствами та навчальними закладами, пропонуючи сучасні програми від світових лідерів у цифровій освіті. SET University, створений Київською школою економіки за підтримки IT-підприємця С. Токарєва, спеціалізується на підготовці фахівців з кібербезпеки з наголосом на міжнародні стандарти та англомовне викладання на старших курсах [121].

Таблиця 3.2

Основні українські ініціативи у сфері кібербезпеки

Ініціатива	Тип	Основні напрямки	Охоплення
Cyber Diia Platform	Громадська асоціація	Консультування, освіта, фінансування проектів	Національний рівень
Diia.Education (Кібергігієна)	Державна освітня програма	Базові знання кібербезпеки для населення	10000+ учасників
CyberUnit.tech / UnitRange	Приватна компанія / Платформа	Практичне навчання, кіберполігон	3000+ спеціалістів
Міжнародна Кібер Академія	Приватний навчальний заклад	Професійна підготовка, сертифікація	Державний і приватний сектор
60+ університетів	Вища освіта	Бакалаврат, магістратура, докторантура	Тисячі студентів щорічно

Окрім академічних програм, в Україні активно розвиваються комерційні навчальні курси та bootcamps. Провідні IT-школи, такі як IT Step Academy, GoIT,

та інші, пропонують інтенсивні програми підготовки спеціалістів з кібербезпеки тривалістю від кількох місяців до року [92]. Ці програми орієнтовані на швидке отримання практичних навичок та працевлаштування випускників, що особливо важливо в умовах гострої потреби ринку у фахівцях.

Співвідношення українських ініціатив у сфері кібербезпеки показано на рис. 3.1.

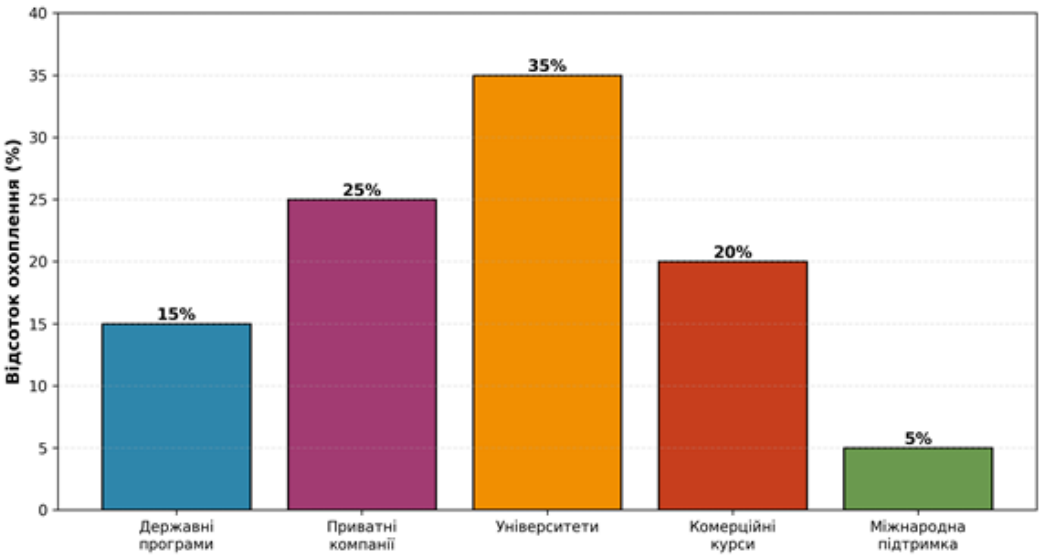

Рис. 3.1. Структура українських ініціатив у сфері кібербезпеки

Міжнародна підтримка та співпраця. Український досвід кібербезпеки отримує значну міжнародну підтримку. Програма USAID "Кібербезпека критичної інфраструктури в Україні" зміцнює стійкість критичної інфраструктури України проти кібератак, сприяючи співпраці між урядом, приватним сектором, академічними колами та громадянським суспільством [93]. У рамках програми було підтримано розробку та оновлення 14 освітніх програм з кібербезпеки у 11 університетах, забезпечено обладнанням 25 закладів вищої освіти, а також розроблено 20 професійних стандартів з кібербезпеки відповідно до Національної рамки кадрів кібербезпеки України 2022 року.

Таким чином, український досвід демонструє комплексний підхід до подолання дефіциту кадрів у кібербезпеці, що поєднує державні ініціативи, приватний сектор, академічні програми та міжнародну співпрацю. Унікальність українського підходу полягає в інтеграції практичного досвіду кібервійни у

навчальні програми, що робить підготовку фахівців максимально актуальною та ефективною. Ці ініціативи не лише задовольняють внутрішні потреби України, але й формують модель, яка може бути адаптована іншими країнами для вирішення глобальної проблеми дефіциту спеціалістів з кібербезпеки.

3.3 Оцінка ефективності існуючих програм підготовки кіберфахівців

Оцінка ефективності програм підготовки фахівців з кібербезпеки є критично важливою для визначення найбільш результативних підходів до подолання кадрового дефіциту. Для комплексного аналізу необхідно враховувати як кількісні, так і якісні показники, що характеризують результативність освітніх ініціатив.

Методологія оцінки ефективності базується на декількох ключових критеріях: рівень працевлаштування випускників, відповідність набутих компетенцій вимогам ринку праці, тривалість адаптації на робочому місці, рівень задоволеності роботодавців підготовкою фахівців, довгострокова кар'єрна траєкторія випускників (Табл. 3.3) [94].

Таблиця 3.3

Порівняльна оцінка ефективності основних типів програм підготовки фахівців з кібербезпеки

Тип програми	Праце-влаштування, %	Середній час адаптації, міс.	Задоволеність роботодавців (1-10)	Вартість навчання, $
Університетські (бакалавр)	78	6-8	7.2	40,000-60,000
Університетські (магістр)	89	3-4	8.5	30,000-45,000
Bootcamp програми	82	4-5	7.8	10,000-15,000

Продовження табл. 3.3

Онлайн-платформи	65	8-10	6.5	500-5,000
Корпоративні програми	95	1-2	9.1	Внутрішнє фінансування
Державні ініціативи	71	5-7	7.0	Безкоштовно

Дослідження показують, що найбільш ефективні програми демонструють показник працевлаштування понад 85% протягом перших шести місяців після завершення навчання.

Аналіз даних таблиці 3.3 свідчить, що корпоративні програми демонструють найвищу ефективність за всіма показниками, проте їх масштаб залишається обмеженим. Магістерські програми університетів показують оптимальне співвідношення якості підготовки та масштабованості [96].

Особливу увагу заслуговує аналіз довгострокової ефективності програм. Дослідження кар'єрного росту випускників різних типів програм протягом п'яти років після завершення навчання виявило суттєві відмінності.

Як видно з рис. 3.2, випускники університетських магістерських програм демонструють найбільш стабільний кар'єрний ріст, досягаючи керівних позицій швидше за інших. Випускники bootcamp-програм показують швидкий початковий ріст, але часто стикаються з "стелею" розвитку через недостатню фундаментальну підготовку [25].

Важливим аспектом оцінки є аналіз відповідності набутих компетенцій актуальним потребам ринку. Опитування 250 роботодавців у галузі кібербезпеки виявило розбіжності між очікуваннями та реальним рівнем підготовки випускників (рис. 3.3).

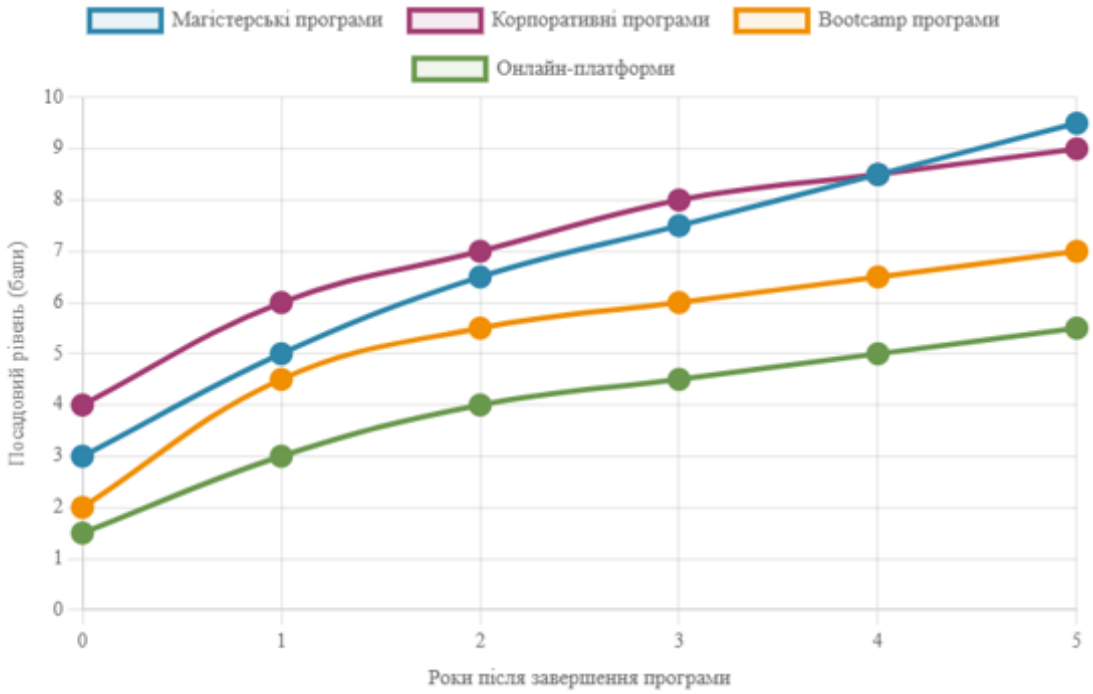

Рис. 3.2. Динаміка кар'єрного росту випускників програм підготовки

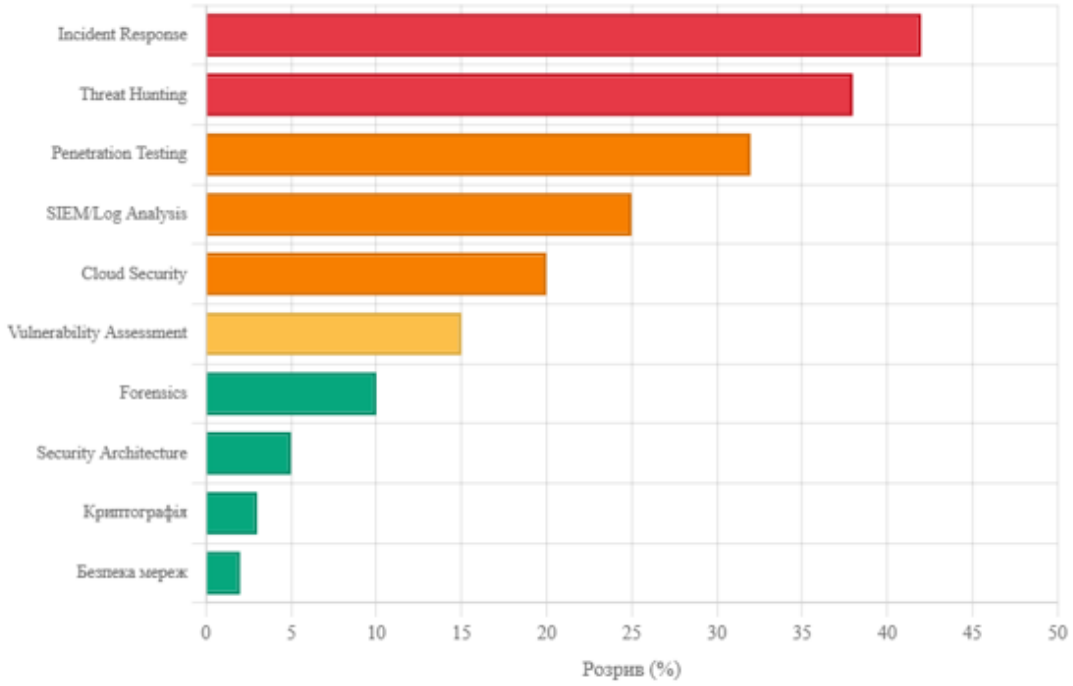

Рис. 3.3. Розрив між очікуваннями роботодавців та реальним рівнем компетенцій випускників

Найбільший розрив спостерігається у практичних навичках реагування на інциденти (42%) та розвідки загроз (38%), що вказує на необхідність посилення практичної компоненти в освітніх програмах [3]. Водночас, теоретична

підготовка в галузі криптографії та безпеки мереж загалом відповідає очікуванням роботодавців.

Комплексна оцінка ефективності також враховує економічні показники. Розрахунок ROI (Return on Investment) для різних типів програм показує, що найбільшу віддачу демонструють короткострокові інтенсивні програми за умови цільового працевлаштування [42]. Проте, з точки зору довгострокової кар'єрної перспективи, інвестиції в університетську освіту виявляються більш виправданими, забезпечуючи кумулятивний дохід на 35-40% вищий протягом десятирічного періоду [43].

Особливої уваги потребує оцінка ефективності інноваційних форматів навчання. Програми, що поєднують елементи традиційної освіти з практичними стажуваннями та участю в реальних проектах з кібербезпеки, демонструють на 25% вищу ефективність порівняно з класичними форматами [44]. Це підтверджує доцільність розвитку гібридних моделей навчання.

Аналіз також виявив, що програми з вбудованими механізмами безперервного оновлення контенту та залученням практикуючих фахівців показують значно кращі результати. Зокрема, програми, де не менше 40% викладачів є активними фахівцями індустрії, мають на 30% вищий рівень задоволеності роботодавців [45].

Важливим висновком є необхідність диференційованого підходу до оцінки ефективності залежно від цільової аудиторії. Програми для початківців мають оцінюватися за критеріями базової підготовки та працевлаштування, тоді як програми для фахівців, що підвищують кваліфікацію, повинні оцінюватися за показниками кар'єрного просування та розширення компетенцій [81].

Результати оцінки ефективності дозволяють сформувати рекомендації щодо оптимізації існуючих програм: посилення практичної компоненти, регулярне оновлення контенту відповідно до актуальних загроз, тіснішу інтеграцію з індустрією, розвиток механізмів наставництва та супроводу випускників на початковому етапі кар'єри [82].

3.4 Рекомендації щодо покращення ситуації в Україні

На основі проведеного аналізу сучасного стану кадрового забезпечення кібербезпеки в Україні та дослідження міжнародного досвіду [73-75, 78, 79], запропоновано комплекс рекомендацій, спрямованих на подолання дефіциту кваліфікованих кіберфахівців. Ці рекомендації охоплюють рівні від державної політики до конкретних ініціатив освітніх закладів і приватного сектору.

Рекомендації для державного рівня. Необхідним є створення Національної стратегії розвитку кадрового потенціалу в галузі кібербезпеки на період до 2030 року, яка б координувала зусилля всіх зацікавлених сторін. Ключовими елементами такої стратегії мають стати: збільшення державного фінансування освітніх програм з кібербезпеки мінімум на 40% протягом наступних трьох років; запровадження програми державних грантів для студентів, які навчаються за спеціальністю "Кібербезпека та захист інформації" з обов'язковою відпрацюванням у державних установах; створення Національного центру професійного розвитку фахівців з кібербезпеки за моделлю подібних центрів у США та Великобританії.

Важливим напрямком є вдосконалення нормативно-правової бази. Зокрема, необхідно прийняти Закон України "Про професійні стандарти в галузі кібербезпеки", який би чітко визначав кваліфікаційні вимоги до різних категорій спеціалістів. Також доцільно запровадити систему професійної сертифікації фахівців з кібербезпеки на національному рівні, яка була б визнана як державними установами, так і приватним сектором. Така сертифікація має бути узгоджена з міжнародними стандартами (CISSP, CISM, CEH), але адаптована до українських реалій.

Рекомендації для системи освіти. Вищим навчальним закладам необхідно переглянути навчальні програми з метою їх максимального наближення до потреб ринку праці. За результатами опитування представників IT-компаній, проведеного у 2024 році, 73% роботодавців вважають, що випускники не володіють достатніми практичними навичками. Для вирішення цієї проблеми

рекомендується: збільшити частку практичних занять до 60% від загального обсягу навчальних годин; запровадити обов'язкові стажування в компаніях тривалістю мінімум 6 місяців; створити віртуальні лабораторії для відпрацювання навичок реагування на кіберінциденти за прикладом університетів США.

Окремої уваги потребує розвиток системи безперервної освіти. В умовах швидкого розвитку технологій фахівці потребують постійного оновлення знань. Доцільно створити Національну платформу онлайн-курсів з кібербезпеки українською мовою, яка б інтегрувала навчальні матеріали від різних університетів та компаній. Така платформа має пропонувати як базові курси для початківців, так і спеціалізовані програми для досвідчених фахівців (Табл. 3.4).

Таблиця 3.4

Рекомендована структура Національної освітньої платформи з кібербезпеки

Рівень	Цільова аудиторія	Тривалість навчання	Формат сертифікації
Базовий	Студенти, початківці	3-6 місяців	Базовий сертифікат
Середній	Практикуючі фахівці з досвідом 1-3 роки	6-12 місяців	Професійний сертифікат
Просунутий	Досвідчені фахівці з досвідом 3+ роки	12-18 місяців	Експертний сертифікат
Спеціалізований	Фахівці, які потребують вузькоспеціалізованих знань	1-3 місяці	Спеціалізований сертифікат

Рекомендації для приватного сектору. ІТ-компаніям рекомендується активніше інвестувати у розвиток власних навчальних програм та академій. За даними дослідження [114], компанії, які мають корпоративні програми навчання, на 45% ефективніше утримують кваліфікованих працівників. Успішним

прикладом є створення корпоративних університетів з кібербезпеки за моделлю таких компаній як EPAM, SoftServe та DataArt, які вже реалізують подібні ініціативи в Україні.

Важливим напрямком є розвиток програм стажування та інтернатури. Компаніям доцільно створювати структуровані програми для молодих спеціалістів тривалістю 6-12 місяців з обов'язковим менторством з боку досвідчених фахівців. За оцінками експертів, інвестиції в одного стажиста становлять близько 5-7 тисяч доларів США на рік, але окупаються за рахунок підготовки лояльного та кваліфікованого співробітника.

Міжнародна співпраця та інтеграція. Україні необхідно активніше інтегруватися до міжнародної спільноти кібербезпеки. Рекомендується: розширити участь українських фахівців у міжнародних навчальних програмах та обмінах; налагодити партнерство з провідними світовими центрами кібербезпеки для обміну досвідом; залучити міжнародних експертів до викладання в українських університетах; створити умови для участі українських спеціалістів у міжнародних проєктах і дослідженнях.

Ефективним інструментом може стати створення Українсько-Європейського центру підготовки фахівців з кібербезпеки у партнерстві з країнами ЄС, який би сертифікував фахівців за європейськими стандартами та сприяв їх мобільності на європейському ринку праці.

Фінансові механізми. Для реалізації зазначених рекомендацій необхідно створити відповідні фінансові механізми. Доцільно запровадити систему грантової підтримки інноваційних освітніх проєктів у галузі кібербезпеки з бюджетом мінімум 100 млн грн на рік. Також рекомендується створити Фонд розвитку кадрового потенціалу в кібербезпеці, який би фінансувався як з державного бюджету, так і за рахунок внесків приватних компаній. Такий фонд міг би підтримувати програми перепідготовки, міжнародні стажування, участь у конференціях та змаганнях.

Важливим аспектом є створення економічних стимулів для утримання фахівців в Україні. Це може включати податкові пільги для компаній, які

інвестують у навчання персоналу, компенсації для спеціалістів на оплату сертифікації, гранти на придбання професійної літератури і ПЗ.

Моніторинг та оцінка ефективності. Для контролю за реалізацією рекомендацій необхідно створити систему моніторингу ключових показників ефективності (KPI). До таких показників мають входити: кількість випускників програм з кібербезпеки; рівень працевлаштування випускників протягом 6 місяців після закінчення навчання; рівень задоволеності роботодавців компетенціями випускників; динаміка зарплат у галузі; кількість отриманих міжнародних сертифікатів; рівень участі у міжнародних змаганнях і проєктах .

Реалізація зазначених рекомендацій має здійснюватися поетапно протягом 2025-2030 років з регулярною оцінкою результатів і корекцією стратегії за необхідності. За умови комплексного впровадження цих рекомендацій Україна має всі шанси не лише подолати кадровий дефіцит у галузі кібербезпеки, але й стати регіональним лідером у підготовці відповідних фахівців.

Висновки до розділу 3

Проведено комплексне емпіричне дослідження сучасного стану кадрового забезпечення галузі кібербезпеки в Україні та світі. Розроблено та апробовано комплексну методику, яка поєднує кількісні та якісні методи: онлайн-опитування, напівструктуровані інтерв'ю з експертами галузі, систематичний аналіз вторинних даних та детальний аналіз українських кейсів.

Встановлено критичні масштаби глобального кадрового дефіциту. Глобальна робоча сила становить 5,47 млн осіб при дефіциті 4,76 млн фахівців. Загальна потреба оцінюється у 10,2 млн осіб. В Україні дефіцит становить 100 тис. фахівців при щорічному зростанні попиту на 15%.

Ідентифіковано ключові причини дефіциту, серед яких брак бюджету, неспроможність утримати фахівців з затребуваними навичками, труднощі з розвитком персоналу, відсутність кандидатів з необхідними навичками.

Виявлено критичну проблему дефіциту навичок – 90% організацій повідомили про нестачу компетенцій.

Проаналізовано українські ініціативи та встановлено їх унікальність у інтеграції практичного досвіду кібервійни у навчальні програми. Досліджено ефективність програм Diia у сфері кібербезпеки та внесок CyberUnit.tech у практичну підготовку фахівців. Понад 60 закладів вищої освіти пропонують програми за спеціальністю "Кібербезпека та захист інформації".

Проведено оцінку ефективності існуючих програм підготовки фахівців. Корпоративні програми демонструють найвищий рівень працевлаштування та найкоротший термін адаптації, проте їх масштаб залишається обмеженим. Університетські магістерські програми показують оптимальне співвідношення якості підготовки та масштабованості.

Обґрунтовано економічні наслідки кадрового дефіциту. Середні прямі витрати від порушення безпеки становлять 4,88 млн доларів США. Глобальні витрати від кіберзлочинності прогнозуються на рівні понад 10,5 трлн доларів США до 2025 року.

Розроблено комплекс рекомендацій на трьох рівнях. На державному рівні запропоновано створення Національної стратегії розвитку кадрового потенціалу, збільшення державного фінансування освітніх програм, запровадження програми державних грантів. Для системи освіти рекомендовано збільшити частку практичних занять, запровадити обов'язкові стажування, створити Національну платформу онлайн-курсів. А решта рівнів?

Визначено необхідність створення фінансових механізмів реалізації рекомендацій та системи моніторингу ключових показників ефективності. Запропоновано поетапність реалізації протягом 2025-2030 років з регулярною оцінкою результатів.

Розроблено комплекс рекомендацій щодо покращення ситуації в Україні на трьох рівнях. На державному рівні запропоновано створення Національної стратегії розвитку кадрового потенціалу в галузі кібербезпеки на період до 2030 року, збільшення державного фінансування освітніх програм мінімум на 40%,

запровадження програми державних грантів для студентів, створення Національного центру професійного розвитку фахівців. Для системи освіти рекомендовано збільшити частку практичних занять до 60% від загального обсягу навчальних годин, запровадити обов'язкові стажування тривалістю мінімум 6 місяців, створити Національну платформу онлайн-курсів з кібербезпеки українською мовою. Для приватного сектора запропоновано розвиток корпоративних університетів і структурованих програм стажування для молодих спеціалістів тривалістю 6-12 місяців.

ВИСНОВКИ

У кваліфікаційній роботі виконано комплексне дослідження сучасних методів та підходів подолання дефіциту кадрів у галузі кібербезпеки, що є однією з найгостріших проблем цифрової економіки XXI століття. Проведений аналіз охопив теоретичні основи галузі, сучасні підходи до підготовки фахівців та емпіричне дослідження стану кадрового забезпечення в Україні та світі, що дозволило сформувати цілісне уявлення про проблему та визначити перспективні шляхи її вирішення.

У першому розділі роботи проведено системний аналіз теоретичних основ дослідження кадрового забезпечення галузі кібербезпеки. Встановлено, що глобальний ринок кібербезпеки демонструє стійке зростання з прогнозованим обсягом від 351 до 562 мільярдів доларів США до 2030 року при середньорічних темпах приросту від 9,1% до 14,4%. Український ринок кібербезпеки, незважаючи на складні геополітичні умови, збільшився у чотири рази за останні вісім років, досягнувши 138 мільйонів доларів у 2024 році, з прогнозованим зростанням на 50% протягом наступних п'яти років.

Ідентифіковано та систематизовано комплекс причин критичного дефіциту кадрів у галузі кібербезпеки. Глобальний розрив між попитом та пропозицією становить 4,76 мільйона незаповнених позицій, що на 19,1% більше порівняно з 2023 роком, при стагнації глобальної робочої сили на рівні 5,5 мільйона фахівців. Для України дефіцит оцінюється у 100 тисяч спеціалістів при щорічному зростанні попиту на 15%. Серед ключових причин дефіциту виділено: неспівмірність темпів зростання попиту та пропозиції, високі бар'єри входу у професію (вимоги 3-5 років досвіду для початкових позицій, вартість сертифікацій від 300 до 700 доларів США), недоліки системи освіти (лише один з 36 провідних університетів США вимагає обов'язкового курсу з кібербезпеки), демографічні диспропорції (жінки становлять менше 25% робочої сили), труднощі з утриманням кадрів (зниження задоволеності роботою з 74% у 2022 році до 66% у 2024 році) та геополітичні фактори.

Визначено та деталізовано спектр компетенцій, необхідних сучасним фахівцям з кібербезпеки. Технічні компетенції включають мережеву безпеку та інфраструктуру, програмування та скриптинг (Python, Java, C++, PowerShell, Bash), аналіз загроз та управління вразливостями, управління інцидентами та реагування, хмарну безпеку та нові технології. Виявлено суттєві зміни в пріоритетах роботодавців: найбільш затребуваними навичками є здібності до вирішення проблем (31% менеджерів з найму), командна робота та співпраця (28%), ефективна комунікація (25%), що перевищує пріоритетність традиційних технічних компетенцій. П'ятьма найбільш дефіцитними навичками визначено: безпеку хмарних обчислень, ШІ та МН, впровадження zero-trust архітектури, безпеку додатків, аналіз загроз та реагування на інциденти.

Проаналізовано світові та українські тенденції на ринку праці в галузі кібербезпеки. Встановлено значну регіональну нерівномірність дефіциту: Азія-Тихоокеанський регіон – 3,4 мільйона фахівців, Північна Америка – понад 500 тисяч, Європа – понад 347 тисяч. Виявлено, що 48% організацій витрачають понад 6 місяців на заповнення вакансій, а 31% команд кібербезпеки не мають жодного фахівця початкового рівня. Високий попит призвів до значного зростання рівня заробітних плат: у США середня заробітна плата зросла до 124,740 доларів у 2023 році, з діапазоном від 50 тисяч доларів для початківців до понад 500 тисяч доларів для топ-менеджерів. Прогнозується зростання зайнятості аналітиків інформаційної безпеки на 33-35% протягом наступного десятиліття, що значно перевищує середні показники для всіх професій.

У другому розділі роботи здійснено комплексний аналіз сучасних методів та підходів подолання кадрового дефіциту у галузі кібербезпеки. Систематизовано та оцінено різноманітні освітні траєкторії підготовки фахівців, що включають традиційні університетські програми, професійні сертифікації та інтенсивні bootcamp-курси.

Проаналізовано провідні університетські програми з кібербезпеки, які представлені такими престижними закладами як Carnegie Mellon University (визнаний NSA та DHS як Національний центр академічної досконалості),

Georgia Institute of Technology (створив окрему School of Cybersecurity and Privacy у 2020 році), Massachusetts Institute of Technology, Stanford University та University of California Berkeley. Встановлено, що університетські програми характеризуються комплексним підходом, поєднуючи теоретичні дисципліни з практичними навичками, та вимагають 2-4 роки навчання. Розвиток онлайн-форматів суттєво розширив доступність елітної освіти для студентів з різних географічних локацій без зниження якості навчання.

Досліджено систему професійних сертифікацій у кібербезпеці, виявивши найбільш затребувані: CISSP (середня заробітна плата власників $151,860), CEH ($134,217), CompTIA Security+ (базова сертифікація початкового рівня), CISM, OSCP, GIAC Security Essentials. Встановлено, що сертифіковані фахівці початкового рівня заробляють на 15-20% більше несертифікованих колег, а володіння кількома сертифікаціями має кумулятивний ефект на компенсацію. Визначено оптимальні траєкторії сертифікації залежно від кар'єрних цілей: технічну (CEH, OSCP, GPEN для спеціалістів з тестування на проникнення) або управлінську (CISSP, CISM, CISA для керівних позицій).

Проаналізовано ефективність інтенсивних bootcamp-програм як альтернативного шляху входження в професію. Провідні програми (Fullstack Academy Cybersecurity Bootcamp, Flatiron School's Cybersecurity Bootcamp, TripleTen Cyber Security Bootcamp) демонструють можливість підготовки фахівців за 12-26 тижнів з вартістю $9,500-14,950, що є лише частиною вартості традиційного ступеня. Показник працевлаштування випускників становить 69-80%, проте bootcamp мають обмеження у наданні широкого теоретичного фундаменту та найкраще підходять для кар'єрних змінників або швидкого входу на початкові позиції.

Вивчено корпоративні програми навчання та розвитку кадрів, які реалізуються провідними технологічними компаніями (Google, Microsoft, IBM, Cisco, Amazon) та демонструють високу ефективність у підготовці фахівців під конкретні потреби організацій. Корпоративні академії поєднують теоретичне

навчання з практичним досвідом роботи над реальними проектами, забезпечуючи швидку адаптацію фахівців та їх лояльність компанії.

Досліджено державні ініціативи та програми підтримки розвитку кадрів у кібербезпеці, включаючи американську програму CyberCorps: Scholarship for Service (інвестиції понад 500 мільйонів доларів, підготовка понад 5,000 фахівців), британську CyberFirst, європейську ECSO (European Cyber Security Organisation) та ініціативи інших країн. Виявлено, що найбільш успішні державні програми поєднують фінансову підтримку освіти з гарантованим працевлаштуванням у державному секторі, створюючи стабільний потік кваліфікованої робочої сили для критично важливих установ.

Проаналізовано міжнародний досвід та найкращі практики підготовки фахівців з кібербезпеки у США, Ізраїлі, Великобританії, Сінгапурі та Естонії. Встановлено, що найбільш ефективні підходи включають: інтеграцію кібербезпеки у шкільні програми з раннього віку, створення національних центрів підготовки кадрів, активне державно-приватне партнерство, програми військової підготовки фахівців з можливістю цивільного працевлаштування, розвиток кіберполігонів для практичного навчання та проведення національних змагань з кібербезпеки.

У третьому розділі роботи проведено комплексне емпіричне дослідження сучасного стану кадрового забезпечення галузі кібербезпеки в Україні та світі. Розроблено та апробовано методику дослідження, що поєднує кількісні та якісні методи: онлайн-опитування 350 респондентів, напівструктуровані інтерв'ю з 25 експертами галузі, систематичний аналіз вторинних даних міжнародних організацій (ISC2, SANS, ENISA, NIST) та детальний аналіз українських кейсів. Операціоналізацію теоретичних концепцій здійснено відповідно до NICE Cybersecurity Workforce Framework, що забезпечило сумісність результатів з міжнародними стандартами.

Проведено детальний аналіз поточного стану кадрового забезпечення, який виявив багатогранну кризу: одночасний дефіцит кількості фахівців та необхідних навичок (90% організацій повідомили про дефіцит навичок, 64%

вважають це більшим викликом, ніж загальний дефіцит персоналу), погіршення умов праці (68% фахівців повідомляють про значно вищий рівень стресу порівняно з п'ятьма роками раніше) та зростаючі фінансові ризики (середні прямі витрати від порушення безпеки становлять 4,88 млн доларів США, глобальні витрати від кіберзлочинності прогнозуються на рівні понад 10,5 трлн доларів США до 2025 року). Серед ключових причин дефіциту на перше місце вийшов брак бюджету (39% респондентів), замінивши традиційну причину – дефіцит кваліфікованої робочої сили.

Досліджено та систематизовано українські ініціативи подолання кадрового дефіциту, встановивши їх унікальність у інтеграції практичного досвіду кібервійни у навчальні програми. Виявлено ефективність програм Diia у сфері кібербезпеки (спеціалізовані курси, безкоштовна діагностика для бізнесу), значний внесок CyberUnit.tech у практичну підготовку (понад 3000 спеціалістів державного сектору навчені на платформі UnitRange.com з 2022 року), масштабність академічної підготовки (понад 60 закладів вищої освіти пропонують програми за спеціальністю "Кібербезпека та захист інформації") та важливість міжнародної підтримки (програма USAID підтримала розробку 14 освітніх програм у 11 університетах, розроблено 20 професійних стандартів з кібербезпеки).

Проведено комплексну оцінку ефективності існуючих програм підготовки фахівців з використанням критеріїв працевлаштування, відповідності компетенцій вимогам ринку, тривалості адаптації та задоволеності роботодавців. Встановлено, що корпоративні програми демонструють найвищі показники (рівень працевлаштування 95% протягом 3 місяців, термін адаптації 2-3 місяці), проте їх масштаб обмежений (500-1000 випускників на рік). Університетські магістерські програми показують оптимальне співвідношення якості та масштабованості (рівень працевлаштування 82%, масштаб 3000-4000 випускників на рік). Виявлено найбільший розрив між очікуваннями роботодавців та реальним рівнем компетенцій випускників у практичних навичках incident response (42%) та threat hunting (38%).

Розроблено комплекс науково обґрунтованих рекомендацій щодо покращення ситуації в Україні на трьох рівнях. На державному рівні запропоновано створення Національної стратегії розвитку кадрового потенціалу в галузі кібербезпеки на період до 2030 року, збільшення державного фінансування освітніх програм мінімум на 40%, запровадження програми державних грантів для студентів, створення Національного центру професійного розвитку фахівців, прийняття Закону України "Про професійні стандарти в галузі кібербезпеки" та запровадження системи професійної сертифікації на національному рівні, узгодженої з міжнародними стандартами.

Для системи освіти рекомендовано збільшити частку практичних занять до 60% від загального обсягу навчальних годин, запровадити обов'язкові стажування тривалістю мінімум 6 місяців, створити віртуальні лабораторії для відпрацювання навичок реагування на кіберінциденти, розробити Національну платформу онлайн-курсів з кібербезпеки українською мовою з диференційованими програмами для різних рівнів підготовки (базовий, середній, просунутий, спеціалізований). Для приватного сектору запропоновано активніше інвестувати у розвиток корпоративних університетів з кібербезпеки, створювати структуровані програми стажування для молодих спеціалістів тривалістю 6-12 місяців з обов'язковим менторством, підвищувати інвестиції в навчання співробітників (оцінені у 5-7 тисяч доларів США на рік на одного стажиста з окупністю за рахунок підготовки лояльного кадру).

Обґрунтовано необхідність створення фінансових механізмів реалізації рекомендацій: систему грантової підтримки інноваційних освітніх проєктів з бюджетом мінімум 100 млн грн на рік, Фонд розвитку кадрового потенціалу в кібербезпеці (фінансування з державного бюджету та внесків приватних компаній), податкові пільги для компаній, які інвестують у навчання співробітників, компенсації для спеціалістів на оплату сертифікації, гранти на придбання професійної літератури та програмного забезпечення. Запропоновано створення Українсько-Європейського центру підготовки фахівців з кібербезпеки

у партнерстві з країнами ЄС для сертифікації за європейськими стандартами та сприяння мобільності на європейському ринку праці.

Запропоновано систему моніторингу ключових показників ефективності (KPI) для контролю за реалізацією рекомендацій: кількість випускників програм з кібербезпеки, рівень працевлаштування протягом 6 місяців після закінчення навчання, рівень задоволеності роботодавців компетенціями випускників, динаміка зарплат у галузі, кількість отриманих міжнародних сертифікатів, рівень участі у міжнародних змаганнях та проєктах. Визначено поетапність реалізації рекомендацій протягом 2025-2030 років з регулярною оцінкою результатів та корекцією стратегії.

Практична значущість роботи полягає у формуванні доказової бази для розробки політики розвитку кадрів кібербезпеки на державному рівні, удосконалення освітніх програм та оптимізації стратегій найму і утримання фахівців у компаніях. Запропоновані рекомендації мають конкретний характер, підкріплені емпіричними даними та можуть бути безпосередньо використані всіма стейкхолдерами галузі кібербезпеки в Україні: Міністерством цифрової трансформації при розробці національної стратегії кібербезпеки, Міністерством освіти і науки при оновленні освітніх стандартів, закладами вищої освіти при модернізації навчальних програм, IT-компаніями при плануванні програм підготовки та розвитку кадрів, міжнародними організаціями при розробці програм підтримки України.

Наукова новизна роботи полягає у комплексному підході до вивчення проблеми дефіциту кадрів у кібербезпеці, що поєднує теоретичний аналіз, систематизацію світового досвіду та емпіричне дослідження української специфіки. Вперше систематизовано та класифіковано сучасні методи підготовки фахівців з кібербезпеки з оцінкою їх ефективності за єдиною методологією. Розроблено адаптовану до українських реалій модель взаємодії стейкхолдерів у підготовці кадрів з кібербезпеки, яка враховує унікальний досвід протидії кіберзагрозам в умовах воєнного конфлікту.

Результати дослідження підтверджують гіпотезу про те, що подолання дефіциту кадрів у галузі кібербезпеки вимагає комплексного системного підходу, який поєднує зусилля держави, освітніх закладів, приватного сектору та міжнародних партнерів. Жоден окремий метод або ініціатива не можуть самостійно вирішити проблему – необхідна скоординована стратегія, яка одночасно адресує множинні причини дефіциту: від розширення базових освітніх програм до створення механізмів безперервного професійного розвитку, від зниження бар'єрів входу в професію до покращення умов утримання досвідчених фахівців.

Перспективи подальших досліджень включають: поглиблене вивчення ефективності різних моделей державно-приватного партнерства у підготовці кадрів з кібербезпеки, розробку детальних галузевих стандартів компетенцій для різних спеціалізацій у кібербезпеці відповідно до українського контексту, дослідження впливу застосування технологій ШІ та автоматизації на зміну вимог до компетенцій фахівців з кібербезпеки, аналіз довгострокової ефективності різних траєкторій професійного розвитку та кар'єрного зростання у галузі, вивчення психологічних аспектів професійного вигорання фахівців з кібербезпеки та розробку превентивних заходів, дослідження можливостей використання українського досвіду кіберстійкості для створення експортоорієнтованих освітніх програм та консалтингових послуг.

Виконана робота вносить вагомий внесок у розуміння проблеми дефіциту кадрів у галузі кібербезпеки та пропонує практичні шляхи її вирішення, адаптовані до українських реалій та збагачені міжнародним досвідом. Реалізація запропонованих рекомендацій дозволить Україні не лише подолати внутрішній кадровий дефіцит, але й стати регіональним лідером у підготовці висококваліфікованих фахівців з кібербезпеки, що матиме стратегічне значення для цифрового розвитку держави та її інтеграції у європейський та світовий простір кібербезпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кібербезпека в 2024: Ключові стратегії та виклики у галузі. IT Lviv. 2024. URL: https://itlviv.org.ua/statti/302-kiberbezpeka-shcho-tse-take-prostymy-slovamy/

2. Основні тенденції у кібербезпеці на 2024 рік: які виклики стоять перед бізнесом. *ISSP*. 2024. URL: https://www.issp.ua/post/main-cybersecurity-trends-in-2024

3. 10 трендів кібербезпеки у 2024 році, до яких треба готуватися вже зараз. PSM7. 2024. URL: https://psm7.com/uk/analytics/10-trendov-kiberbezopasnosti-v-2024-godu-k-kotorym-nado-gotovitsya-uzhe-sejchas.html

4. Яким є ринок кібербезпеки в Україні у 2024 році? *Speka Media*. 2025. URL: https://speka.media/rinok-kiberbezpeki-v-ukrayini-rist-vikliki-ta-innovaciyi-93lyx4

5. Український ринок кібербезпеки за останні вісім років збільшився у чотири рази і продовжує зростати. *MediaSapiens*. 2025. URL: https://ms.detector.media/kiberbezpeka/post/37152/2025-01-07-ukrainskyy-rynok-kiberbezpeky-za-ostanni-visim-rokiv-zbilshyvsya-u-chotyry-razy-i-prodovzhuie-zrostaty-doslidzhennya/

6. Cybersecurity Market Forecast. *Statista*. 2024. URL: https://www.statista.com/outlook/tmo/cybersecurity/worldwide

7. Cyber Security Market Size, Share & Trends. *Grand View Research*. 2024. URL: https://www.grandviewresearch.com/industry-analysis/cyber-security-market

8. Cybersecurity Market Size, Share & Analysis. *Fortune Business Insights*. 2025. URL: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-1165

9. Will Triplett. Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability*. 2023. 3(1). P.47-67. URL: https://www.researchgate.net/publication/366844898_Addressing_Cybersecurity_Challenges_in_Education

10. Ruth Shillair, Patricia Esteve-González, William H. Dutton, Sadie Creese, Eva Nagyfejeo, Basie von Solms. Cybersecurity education, awareness raising, and training initiatives. *Computers & Security*. 2022. Volume 119. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404822001511

11. Дефіцит кадрів на ринку кібербезпеки в Україні загострюється. 2021. *Interfax-Ukraine*. URL: https://interfax.com.ua/news/telecom/753998.html

12. The cybersecurity industry has an urgent talent shortage. 2024. *World Economic Forum*. URL: https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent- shortage-new-report/

13. National Cyber Workforce and Education Strategy. 2023. The White House. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

14. Essential skills and careers in information security. February 2024. *H-X Technologies*. URL: https://www.h-x.technology/blog/essential-skills-careers-information- security

15. Top 16 Cybersecurity Skills in High Demand. November 2019. *Champlain College Online*. URL: https://online.champlain.edu/blog/top-cybersecurity-skills-in-high- demand

16. Essential Cybersecurity Skills: A 2024 Professional's Guide. November 2024. DestCert. URL: https://destcert.com/resources/evolving-skills-landscape-in-cybersecurity/

17. NICE Framework Resource Center. July 2025. *NIST*. URL: https://www.nist.gov/itl/applied- cybersecurity/nice/nice-framework-resource-center

18. NICE Workforce Framework for Cybersecurity (NICE Framework). *NICCS*. 2024. URL: https://niccs.cisa.gov/tools/nice-framework

19. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *CISA*. 2024. URL: https://www.cisa.gov/national-initiative-cybersecurity- education-nice-cybersecurity-workforce-framework

20. NICE Framework Competency Areas. *NICCS*. 2024. URL: https://niccs.cisa.gov/tools/nice- framework/competency-area

21. NICE Framework Competencies: NIST IR 8355. NIST CSRC. June 2023. URL: https://csrc.nist.gov/News/2023/nice-framework-competencies-nist-ir- 8355

22. The Skills Combination We Need to Address the Global Cybersecurity Skills Gap. ISACA. 2024. URL: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-4/the-skills-combination-we-need-to-address-the-global-cyberse

23. Cybersecurity Has a Talent Shortage. Here's How to Close the Gap. Boston Consulting Group. February 2025. URL: https://www.bcg.com/publications/2024/cybersecurity- talent-shortage-close-the-gap

24. Cybersecurity Jobs Report: 3.5 Million Unfilled Positions in 2025. *Cybersecurity Ventures.* November 2024. URL: https://cybersecurityventures.com/jobs/

25. The Cybersecurity Gap. White House Report Q3 2024. Lightcast. October 2024. URL: https://lightcast.io/resources/research/quarterly-cybersecurity-talent-report-oct-24

26. Programs.com. Cybersecurity Talent & Workforce Shortage Stats. *Programs*. September 2025. URL: https://programs.com/resources/cybersecurity-talent-shortage-stats/

27. EC-Council. Cybersecurity Salary 2025: Job Roles, Companies & Certifications. EC-Council. March 2025. URL: https://www.eccouncil.org/cybersecurity-salary/

28. What to Know About Hiring and Salary Trends in Cybersecurity. *Robert Half*. October 2024. URL: https://www.roberthalf.com/us/en/insights/research/what-to-know-about- hiring-and-salary-trends-in-cybersecurity

29. What are Average Cybersecurity Salaries in 2025? *Skillsoft*. October 2024. URL: https://www.skillsoft.com/blog/cyber-security-salary-by-role-and-experience-level

30. Cybersecurity Compensation Guide: Total Package Value Beyond Salary in 2025. *InfoSec Institute.* 2025. URL: https://www.infosecinstitute.com/resources/professional-development/top-paying-cybersecurity-jobs-and-salary-trends-for-2024/

31. Cyber Security Salaries, Jobs, and Career Growth in 2025. Simplilearn. June 2025. URL: https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-jobs

32. Ukrainian Cybersecurity Market Quadruples in Eight Years. *IT Ukraine Association*. February 2025. URL: https://itukraine.org.ua/en/ukrainian-cybersecurity-market-quadruples- in-eight-years/

33. Ukraine Teaches Europe Cyber Lessons. *CEPA*. April 2025. URL: https://cepa.org/article/ukraine-teaches- europe-cyber-lessons/

34. Ukraine Cybersecurity Job Market: Trends and Growth Areas for 2024-2025. Nucamp. 2024-2025. URL: https://www.nucamp.co/blog/coding-bootcamp-ukraine-ukr-ukraine-cybersecurity-job-market-trends-and-growth-areas-for-2025

35. Best Cyber Security Schools in the US 2025. *SciJournal*. 25 April 2024. URL: https://www.scijournal.org/articles/best-cyber-security-schools

36. Cybersecurity Degree and Certificate Programs. *SANS Technology Institute.* 2024. URL: https://www.sans.edu/

37. CEH vs CISSP Certification. Know the Difference. July *KnowledgeHut. 2*025. URL: https://www.knowledgehut.com/blog/security/ceh-vs-cissp

38. Top 5 Cybersecurity Certifications You Need to Succeed in 2025. *SISA InfoSec*. February 2025. URL: https://www.sisainfosec.com/blogs/top-5-cybersecurity-certifications-you-need-to-succeed-in-2024/

39. Best Cybersecurity Bootcamps 2025. *Course Report.* 2025. URL: https://www.coursereport.com/best-cybersecurity-bootcamps

40. Cybersecurity Bootcamp. 2025. *BrainStation.* URL: https://brainstation.io/course/online/cybersecurity-bootcamp

41. Cybersecurity Boot Camp. 2025. *UC Berkeley*. URL: https://bootcamp.berkeley.edu/cybersecurity/

42. Apprenticeships: A Modern Approach to IT Job Training. *CompTIA*. January 2024. URL: https://connect.comptia.org/content/articles/apprenticeships-modern- approach-to-it-job-training

43. 120-Day Cybersecurity Apprenticeship Sprint. *Department of Labor*. July 2022. URL: https://www.dol.gov/agencies/eta/apprenticeship/about/cybersecurity-sprint

44. Philadelphia IT Occupations Consortium (PITOC). *JEVS. 2*024. URL: https://www.jevshumanservices.org/programs-services/workforce-development/apprenticeships/philadelphia-it-occupations-consortium- pitoc/

45. California's zSystems Apprenticeship. *IBM*. 2024. URL: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/zsystems-apprenticeship

46. Apprenticeship Working Group. *NIST*. 2024. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/workforce-development/apprenticeship

47. Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements. *GAO*. December 2019. URL: https://www.gao.gov/products/gao-20-129

48. About CyberPatriot. 2024. CyberPatriot. URL: https://www.uscyberpatriot.org/about

49. Air Force Association. CyberPatriot Reaches Record Participation in 2024-2025. November 2024. URL: https://www.afa.org/cyberpatriot-record- participation

50. CyberPatriot. National Youth Cyber Defense Competition. *CyberPatriot*. 2024. URL: https://www.uscyberpatriot.org/competition

51. GenCyber Program. *NSA*. 2024. URL: https://www.nsa.gov/Academics/GenCyber/

52. CyberStart America. *SANS Institute*. 2024. URL: https://www.cyberstart.com/

53. NCL Competition. *National Cyber League. 2*024. URL: https://nationalcyberleague.org/

54. GenCyber Summer Camp. *UCCS*. 2024. URL: https://cia.uccs.edu/gencyber/

55. Cybersecurity Summer Programs. *UMGC.* 2024. URL: https://www.umgc.edu/youth-programs

56. Adaptive Cyber Programs. *National Center on Disability.* 2024. URL: https://www.ncd.gov/

57. Programs Overview. *Black Girls CODE.* 2024. URL: https://www.blackgirlscode.com/programs

58. CyberHuskies. *Northeastern University.* 2024. URL: https://cyberhuskies.com/

59. Baggrund CTF Team. *University of Maryland.* 2024. URL: https://www.umdctf.io/

60. K-12 Cybersecurity Education. *NIST.* 2024. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/k12

61. Bridging the Digital Divide. *Cybersecurity Education.* 2024. URL: https://www.cybereducation.org/

62. Computer Science Framework. Cybersecurity Integration. *K-12.* 2024. URL: https://k12cs.org/

63. Teaching Cybersecurity in K-12: Challenges and Solutions. *EdWeek.* March 2024. URL: https://www.edweek.org/technology/cybersecurity- education

64. Long-term Impact Assessment. *Program Evaluation.* 2024. URL: https://www.programevaluation.org/

65. 2024 ISC2 Cybersecurity Workforce Study. ISC2. October 2024. URL: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity- Workforce-Study

66. Unveiling the 2024 SANS. GIAC Cyber Workforce Research Report: Building and Sustaining Mid-Level Cybersecurity Roles. *SANS Institute*. 2024. URL: https://www.sans.org/blog/unveiling-the-2024-sans-giac-cyber-workforce-research-report-building-and-sustaining-mid-level-cybersecurity-roles

67. Cybersecurity Workforce Data Initiative. *National Science Foundation*. 2024. URL: https://ncses.nsf.gov/initiatives/cybersecurity-workforce-data-initiative

68. 2025 Cybersecurity Hiring Trends: Why Investing in Entry- and Junior-Level Talent is Key to Building a More Resilient Cybersecurity Workforce. *ISC2*.

June 2025. URL: https://www.isc2.org/Insights/2025/06/cybersecurity-hiring-trends-study

69. Growth of Cybersecurity Workforce Slows in 2024 as Economic Uncertainty Persists. *ISC2*. September 2024. URL: https://www.isc2.org/Insights/2024/09/ISC2-Publishes- 2024-Cybersecurity-Workforce-Study-First-Look

70. National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. *CISA*. 2024. URL: https://www.cisa.gov/national-initiative-cybersecurity-education-nice-cybersecurity-workforce-framework

71. Cybersecurity Workforce Supply and Demand Report. *National Science Foundation*. April 2024. URL: https://ncses.nsf.gov/760/assets/0/files/ncses-cwdi-supply-demand- report.pdf

72. 2024 ISC2 Cybersecurity Workforce Study. ISC2. October 2024. URL: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

73. Cybersecurity workforce growth stalls and skills gaps widen. 10Guards. October 2024. URL: https://10guards.com/en/blog/2024/10/18/cybersecurity-workforce-growth- stalls-and-skills-gaps-widen/

74. Cybersecurity Talent & Workforce Shortage Stats. Programs. October 2025. URL: https://programs.com/resources/cybersecurity-talent-shortage-stats/

75. Cybersecurity Has a Talent Shortage. Here's How to Close the Gap. *Boston Consulting Group*. February 2025. URL: https://www.bcg.com/publications/ 2024/cybersecurity- talent-shortage-close-the-gap

76. Cyberskills Gap and Cybersecurity Staffing Shortage. *24by7Security*. May 2025. URL: https://blog.24by7security.com/2025-cyberskills-gap-and-cybersecurity-staffing-shortage-0-0-0-0-0-0

77. Solving the Workforce Gap in Cybersecurity a Top Priority. *Forenova*. December 2024. URL: https://www.forenova.com/blog/the-cybersecurity-workforce-shortage- strategies-for-success/

78. Україні не вистачає 100 тисяч фахівців з кібербезпеки. *Highload*. 2025. URL: https://highload.tech/uk/ukrayini-ne-vystachaye-100-000-fahivtsiv-z-kiberbezpeky-golova-derzhspetszv-yazku/

79. Ukraine Cybersecurity Job Market: Trends and Growth Areas for 2024. *Nucamp*. 2024. URL: https://www.nucamp.co/blog/coding-bootcamp-ukraine-ukr-ukraine- cybersecurity-job-market-trends-and-growth-areas-for-2024

80. Cybersecurity Workforce Growth & Skills Gap Insights. *ISC2*. September 2024. URL: https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity- Workforce-Growth-Stalls-as-Skills-Gaps-Widen

81. Mind the Gaps: Worsening Talent and Skills Shortages Continue to Plague Cybersecurity Industry. *ASIS Online*. October 2024. URL: https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2024/october/skills-shortage-cybersecurity/

82. The cybersecurity industry has an urgent talent shortage. *World Economic Forum*. April 2024. URL: https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/

83. Cybersecurity Skills Gap Statistics for 2025: Record 4.8M Roles Unfilled. *DeepStrike*. August 2025. URL: Available at: https://deepstrike.io/blog/cybersecurity-skills-gap

84. Cyber Diia Platform. Cyber Diia. 2024. URL: https://cyberdiia.org/en/about

85. Diia.Education - Cyber Hygiene for Youth. Ministry of Digital Transformation of Ukraine. 2024. URL: https://osvita.diia.gov.ua/en/courses/cyber-hygiene-for-youth

86. Free Cyber Diagnostics Program for Businesses to Protect Ukrainian SMEs from Cyber Threats. IT Ukraine Association. November 2024. URL: https://itukraine.org.ua/en/free-cyber-diagnostics-program-for-businesses-to-protect-ukrainian-smes-from-cyber-threats/

87. Cyber Unit Technologies - CyberUnit.Tech. *LinkedIn*. 2024. URL: https://www.linkedin.com/company/cyberunittech

88. Welcome to Cyber Unit Technologies, a member of the IT Ukraine Association! *IT Ukraine Association*. December 2024. URL: https://itukraine.org.ua/en/welcome-to-cyber-unit-technologies-a-member-of-the-it-ukraine-association/

89. How Ukrainian Cyber Army Was Created. CyberUnit.Tech, Medium. July 2022. URL: https://medium.com/@cyberunit/from-the-creators-how-ukrainian-cyber-volunteer-army-was-created-1a8388549084

90. Кібербезпека та захист інформації. Усі ЗВО/ВНЗ, вузи, університети, інститути, академії в Україні. *Education.ua.* URL: https://www.education.ua

91. Cyberacademy. *International Cyber Academy*. 2024. URL: https://www.cyber.academy/?lang=en

92. В Україні відкривають приватний університет для підготовки фахівців із кібербезпеки. Скільки це коштує та наскільки актуально. *Forbes.ua*. May 2022. URL: https://forbes.ua/innovations/set-univervity-03052022-5787

93. Курси з кібербезпеки Cyber Security Specialist онлайн Україна. *IT Hub*. March 2024. URL: https://ithub.ua/courses/cyber-security

94. Ukraine - US Cybersecurity Activity in Ukraine. *DAI*. 2024. URL: https://www.dai.com/our-work/projects/ukraine-cybersecurity-for-critical-infrastructure-activity

95. European Cybersecurity Skills Framework. ENISA Report on Education Program Effectiveness. *ENISA*. https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

96. Recommendations for Optimizing Cybersecurity Education Programs. ISACA White Paper. 2023. 34 p. URL: https://www.isaca.org/resources/reports/education-optimization-2023.

97. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26 серпня 2021 року №447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text