**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 РОЗВИТКУ РОБОЧОЇ СИЛИ В ГАЛУЗІ КІБЕРБЕЗПЕКИ**”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Владислав СНІЖКО
*(підпис)* *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Владислав СНІЖКО
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна МУЖАНОВА
*к. держ. упр., доцент* Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

**Київ 2025**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут кібербезпеки та захисту інформації**

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

**ЗАТВЕРДЖУЮ**
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Сніжку Владиславу Миколайовичу
*(прізвище, ім’я, по батькові здобувача)*

1. Тема кваліфікаційної роботи “Сучасні методи розвитку робочої сили в галузі кібербезпеки”, керівник кваліфікаційної роботи МУЖАНОВА Тетяна, к. держ. упр., доцент,
*(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)*

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: розвиток робочої сили з кібербезпеки, дефіцит кадрів, навчання і підвищення кваліфікації, методи неформальної і практичної освіти.

4. Перелік питань, які мають бути розроблені:
   4.1. Дослідити сучасний стан і тенденції розвитку робочої сили в галузі кібербезпеки у світі.
   4.2. Встановити особливості розвитку робочої сили в галузі кібербезпеки в Україні.
   4.3. Проаналізувати сучасні методи розвитку та підвищення кваліфікації кадрів з кібербезпеки.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2025 р.

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Етапи кваліфікаційної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Визначення об’єкту, предмету, мети та завдань дослідження. | 18.03.2025 | |
| 2. | Збір та аналіз літератури. | 29.03.2025 | |
| 3. | Дослідження сучасного стану і тенденцій розвитку робочої сили в галузі кібербезпеки у світі. | 08.04.2025 | |
| 4. | Встановлення особливостей розвитку робочої сили в галузі кібербезпеки в Україні. | 22.04.2025 | |
| 5. | Аналіз сучасних методів розвитку та підвищення кваліфікації кадрів з кібербезпеки. | 08.05.2025 | |
| 6. | Формулювання висновків за результатами проведеного дослідження. | 20.05.2025 | |
| 7. | Оформлення роботи. | 22.05.2025 | |
| 8. | Оформлення презентації. | 03.06.2025 | |
| 9. | Отримання рецензії на роботу. | 03.06.2025 | |
| 10. | Захист в ЕК. | __.06.2025 | |

Здобувач вищої освіти _____ Владислав СНІЖКО
*(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 бакалавра**

Направляється здобувач Сніжко В.М. до захисту кваліфікаційної роботи
*(прізвище та ініціали)*
за спеціальністю 125 Кібербезпека
*(код, найменування спеціальності)*
освітньої програми Управління інформаційною та кібернетичною безпекою
*(назва)*
на тему: "Сучасні методи розвитку робочої сили в галузі кібербезпеки"

Кваліфікаційна робота і рецензія додаються.

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

**Висновок керівника кваліфікаційної роботи**

Здобувач СНІЖКО Владислав у кваліфікаційній роботі дослідив сучасний стан і тенденції розвитку робочої сили в галузі кібербезпеки у світі; встановив особливості розвитку робочої сили в галузі кібербезпеки в Україні; проаналізував сучасні методи розвитку та підвищення кваліфікації кадрів з кібербезпеки.

Під час підготовки кваліфікаційної роботи СНІЖКО Владислав показав хорошу теоретичну та практичну підготовку, довів володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення наукових проблем, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача СНІЖКА Владислава на позитивну оцінку та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою 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 Сніжко В.М. 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 бакалаврську роботу

здобувача вищої освіти СНІЖКА Владислава
на тему “Сучасні методи розвитку робочої сили в галузі кібербезпеки”

**Актуальність.** У сучасних умовах зростаючих загроз цифровому простору кібербезпека стала обов’язковою передовою успішного функціонування держав, бізнесу та всього суспільства. Однак, як свідчить практика, попит на висококваліфіковану робочу силу значно перевищує пропозицію. Глобальний ринок переживає значний дефіцит кадрів, який сягає мільйонів осіб, а професійна і експертна спільнота активно шукає шляхи вирішення цієї проблеми з використанням інноваційних методів і технологій.

Враховуючи ці аспекти, дослідження сучасних методів розвитку робочої сили в галузі кібербезпеки є актуальним науковим завданням.

**Позитивні сторони.**

1. У роботі досліджено сучасний стан і тенденції розвитку робочої сили в галузі кібербезпеки у світі; встановлено особливості розвитку робочої сили в галузі кібербезпеки в Україні; проаналізовано сучасні методи розвитку та підвищення кваліфікації кадрів з кібербезпеки.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу зроблено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Здобувач опрацював достатню джерельну базу, в тому числі результати багатьох соціологічних досліджень, здійснив аналіз ситуації на ринку праці й освітніх послуг з кібербезпеки в Україні.

4. Робота має практичну спрямованість, містить рекомендації щодо перспективних напрямків розвитку висококваліфікованих кадрів з кібербезпеки.

**Недоліки.**

Доцільно було б детальніше розглянути новітні форми навчання фахівців з кібербезпеки, зокрема симуляції, ділові ігри, віртуальні лабораторії.

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

**Висновок:** Кваліфікаційна робота виконана на достатньому науково-методичному рівні і заслуговує позитивної оцінки, а здобувач СНІЖКО Владислав заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____

*підпис* Ім’я, ПРІЗВИЩЕ

# РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню сучасних методів розвитку робочої сили в галузі кібербезпеки. Робота складається зі списку умовних позначень і скорочень, вступу, трьох розділів, що містять 27 рисунків і 4 таблиці, висновків і списку використаних джерел із 50 найменувань. Загальний обсяг роботи становить 83 аркуша, з яких 4 аркушів займає список використаних джерел.

***Метою роботи*** є дослідження сучасних методів розвитку робочої сили в галузі кібербезпеки.

***Об'єктом дослідження*** є кадрове забезпечення галузі кібербезпеки.

***Предмет дослідження –*** сучасні методи розвитку робочої сили в галузі кібербезпеки.

***Методи дослідження.*** Для вирішення поставленого наукового завдання використано методи аналізу та синтезу, порівняння, узагальнення, статистичного аналізу демографічних даних і прогнозування.

Як результат у роботі досліджено сучасний стан і тенденції розвитку робочої сили в галузі кібербезпеки у світі; встановлено особливості розвитку робочої сили в галузі кібербезпеки в Україні; проаналізовано сучасні методи розвитку та підвищення кваліфікації кадрів з кібербезпеки.

***Галузь застосування.*** Описані підходи можуть бути використані для вирішення проблем дефіциту кадрів у галузі кібербезпеки та їх розвитку на рівні підприємств, організацій, а також на загальнодержавному рівні. Застосування напрацювань дослідження сприятиме підвищенню рівня кваліфікації персоналу з кібербезпеки і зміцненню кіберстійкості України в умовах сучасних загроз.

**Ключові слова:** РОЗВИТОК РОБОЧОЇ СИЛИ З КІБЕРБЕЗПЕКИ, ДЕФІЦИТ КАДРІВ, НАВЧАННЯ І ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ, МЕТОДИ НЕФОРМАЛЬНОЇ І ПРАКТИЧНОЇ ОСВІТИ

# ABSTRACT

The qualification work is devoted to the study of modern methods of workforce development in the field of cybersecurity. The work consists of a list of symbols and abbreviations, an introduction, three chapters containing 27 figures and 4 tables, conclusions and a list of references which consists of 50 items. The total volume of the work is 83 pages, of which 4 pages are occupied by the list of references.

***The purpose of the study*** is to investigate modern methods of cybersecurity workforce development.

***The object of the study*** is cybersecurity workforce provision.

***The subject of the study*** is modern methods of cybersecurity workforce development.

***Research methods.*** To solve the scientific task, the methods of analysis and synthesis, comparison, generalization, statistical analysis and forecasting were used.

As a result, in the paper current state and trends in the cybersecurity workforce development in the world were investigated; the features of the cybersecurity workforce development in Ukraine were established; modern methods of development and advanced training of cybersecurity personnel were analyzed.

***Field of application.*** The described approaches can be used to solve the problems of shortage and development of cybersecurity personnel at the levels of enterprises, organizations, as well as at the national level. The application of the research results will contribute to increasing the level of qualification of cybersecurity personnel and strengthening the cyber resilience of Ukraine in the face of modern threats.

***Keywords:*** DEVELOPMENT OF CYBERSECURITY WORKFORCE, SHORTAGE OF CYBERSECURITY PERSONNEL, TRAINING AND IMPROVING QUALIFICATIONS, INFORMAL AND PRACTICAL EDUCATION.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

| | |
|---|---|
| CTF | Capture The Flag |
| DevSecOps | Development, Security, and Operations |
| GDPR | General Data Protection Regulation |
| GCF | The Global Cybersecurity Forum |
| ISC2 | International Information System Security Certification Consortium |
| ISO | International Organization for Standardization |
| SOC | Security Operations Center |
| NICE | National Initiative for Cybersecurity Education |
| OWASP | Open Worldwide Application Security Project |
| ECSF | European Cybersecurity Skills Framework |
| ISSP | Information Systems Security Partners |
| NIST | National Institute of Standards and Technology |
| SIEM | Security Information and Event Management |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| SANS | SysAdmin, Audit, Network and Security |
| APT | Advanced Persistent Threat |
| CWE | Common Weakness Enumeration |
| ML | Machine Learning |
| CCPA | California Consumer Privacy Act |
| ICS | Industrial Control Systems |
| МН | Машинне навчання |
| ШІ | Штучний інтелект |

# ВСТУП

***Актуальність теми.*** У XXI столітті кібербезпека еволюціонувала до стратегічної складової функціонування держав, бізнесу та всього суспільства. Це спровокувало безпрецедентне збільшення потреби у висококласних спеціалістах. Однак, світовий ринок відчуває відчутний дефіцит кадрів, який, за експертними оцінками, сягає мільйонів осіб. Ця проблема загострюється стрімким знеціненням знань і невідповідністю існуючих освітніх програм вимогам галузі.

Для України проблема забезпечення кадрами з кібербезпеки стає надзвичайно актуальною. Мобілізація фахівців, масштабна міграція населення і "відтік мізків" закордон суттєво обмежили пропозицію кваліфікованої робочої сили. Ці фактори формують пряму загрозу для рівня кіберзахисту держави.

З огляду на зазначене, дослідження сучасних методів розвитку робочої сили в галузі кібербезпеки є актуальним науковим завданням.

***Мета роботи*** полягає у дослідженні сучасних методів розвитку робочої сили в галузі кібербезпеки.

***Об'єкт дослідження*** – кадрове забезпечення галузі кібербезпеки.

***Предмет дослідження –*** сучасні методи розвитку робочої сили в галузі кібербезпеки.

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

1. Дослідити сучасний стан і тенденції розвитку робочої сили в галузі кібербезпеки у світі.

2. Встановити особливості розвитку робочої сили в галузі кібербезпеки в Україні.

3. Проаналізувати сучасні методи розвитку та підвищення кваліфікації кадрів з кібербезпеки.

***Методи дослідження.*** Для вирішення означеного вище наукового завдання в роботі використано методи аналізу та синтезу, порівняння, узагальнення, статистичного аналізу демографічних даних і прогнозування.

***Практичне значення одержаних результатів.*** Запропоновані підходи та рекомендації сприятимуть обґрунтованому вибору і впровадженню ефективних методів та інструментів підготовки та розвитку персоналу в галузі кібербезпеки. Їх застосування сприятиме подоланню кадрового дефіциту, підвищенню рівня кваліфікації спеціалістів і, як наслідок, загальному зміцненню кіберстійкості України в умовах сучасних загроз.

***Апробація результатів*** кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

# РОЗДІЛ 1. СУЧАСНИЙ СТАН І ТЕНДЕНЦІЇ РОЗВИТКУ РОБОЧОЇ СИЛИ В ГАЛУЗІ КІБЕРБЕЗПЕКИ У СВІТІ

## 1.1 Глобальна динаміка та попит на фахівців у сфері кібербезпеки

Кібербезпека розвивається, а разом з нею розвивається і робоча сила. Щоб краще зрозуміти цю динамічну сферу, насамперед слід з'ясувати її обсяг і масштаби, як вона зростає і чи встигає пропозиція нових працівників за попитом ринку праці.

У XXI столітті кібербезпека перестала бути виключно технічною сферою, а перетворилася на стратегічний компонент функціонування держави, бізнесу та суспільства загалом. Із цим стрімким розвитком пов’язане й зростання потреби у висококваліфікованих фахівцях. Щоб глибше зрозуміти сучасні виклики, пов’язані з кадровим забезпеченням сфери кібербезпеки, варто насамперед розглянути загальну динаміку формування робочої сили у світовому контексті, її розподіл за регіонами та галузями, а також масштаби дефіциту кадрів.

Міжнародна некомерційна організація з тестування і сертифікації фахівців в галузі інформаційної безпеки (Міжнародний консорціум з сертифікації безпеки інформаційних систем (International Information System Security Certification Consortium, ISC2) дійшла висновку, що глобальна кількість працівників у сфері кібербезпеки становила 5,5 мільйона осіб у 2023 році, що на 8,7% більше, ніж рік тому, з них майже 440 тисяч нових робочих місць. Зростання відбулося в усіх регіонах, але особливо високі показники спостерігаються у двох нових країнах Близького Сходу, Азійсько-Тихоокеанському регіоні та Північній Америці. Японія, зокрема, зростає швидкими темпами - 24% з року в рік. Латинська Америка, після багатьох років значного зростання, починає вирівнюватися: темпи зростання Бразилії знизилися з 18,3% у 2022 році до 8,9% у 2023 році, а Мексика дещо знизила темпи зростання в річному обчисленні [1].

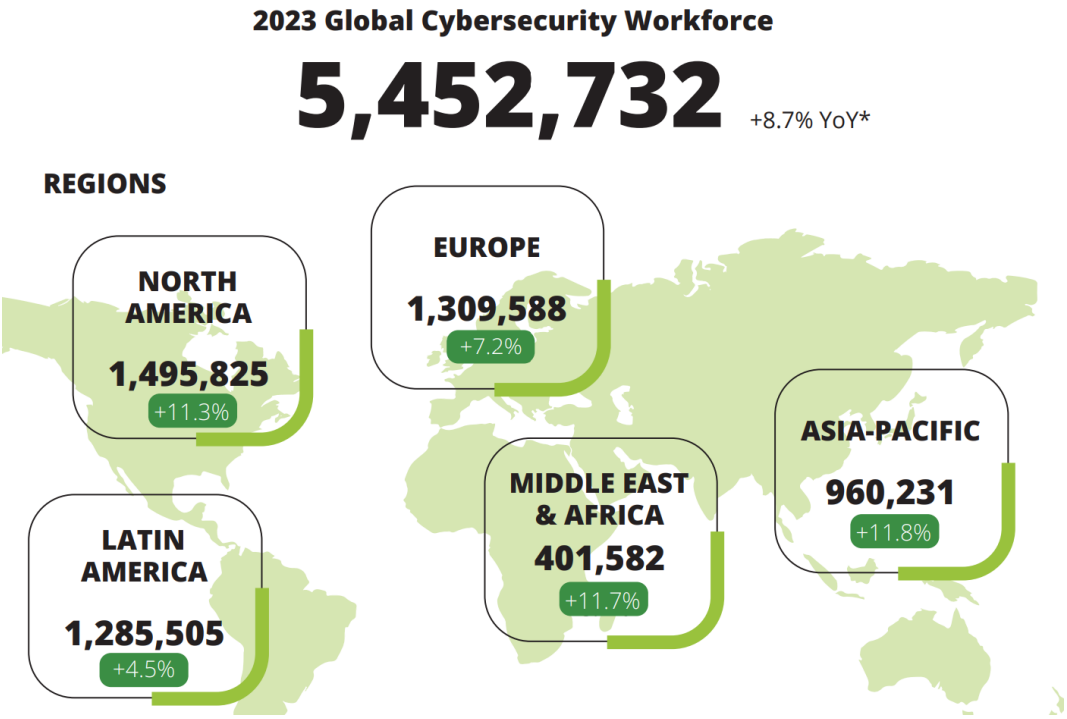


Рис. 1.1. Кількість фахівців з кібербезпеки у 2023 році згідно з дослідженням ISC2

Водночас, звіт всесвітньої неурядової організації Глобальний форум кібербезпеки The Global Cybersecurity Forum (GCF) показав, що станом на 2024 рік світова робоча сила в галузі кібербезпеки налічує 7,1 мільйона професіоналів, при цьому спостерігаються значні регіональні відмінності.

Азійсько-Тихоокеанський регіон на чолі з Індією та Китаєм має найбільшу робочу силу в абсолютному вираженні, за ним слідують Північна та Південна Америка, а потім Європа. США лідирують за рівнем зрілості кібербезпеки, в них зосереджено 70% світових постачальників послуг з кібербезпеки, тоді як Китай та Індія швидко стають центрами кібербезпеки. Натомість, показники Африки є значно меншими: там налічується менше 300 тисяч професіоналів у сфері кібербезпеки. Ці географічні відмінності відображають загальні показники глобального розвитку та підкреслюють різні рівні зрілості кібербезпеки [2].

Розподіл робочої сили з кібербезпеки в різних галузях відрізняється. Дві провідні галузі з найбільшою кількістю працівників у сфері кібербезпеки - це технологічні компанії та компанії, що надають фінансові послуги. Технологічна галузь лідирує з приблизно 19% світового персоналу з кібербезпеки, головним

чином завдяки своїй подвійній ролі як постачальника, так і споживача продуктів і послуг з кібербезпеки, за нею слідує сектор фінансових послуг з 18% (Рис. 1.2).

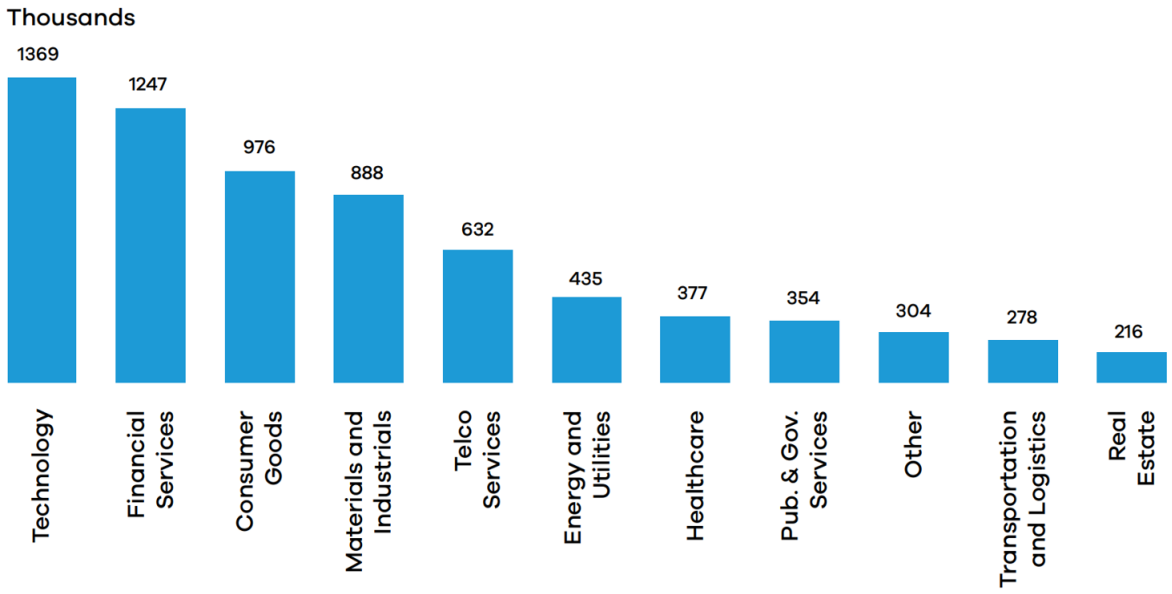


Рис. 1.2. Розподіл фахівців з кібербезпеки за галузями у 2024 році згідно зі звітом GCF

Незважаючи на постійне зростання робочої сили, дослідження ISC2 показало, що попит все ще випереджає пропозицію. Цього року дефіцит кіберфахівців зріс ще на 12,6%, причому найбільше в Азійсько-Тихоокеанському регіоні (особливо в Японії та Індії) та Північній Америці. У регіонах з особливо швидким зростанням пропозиції, таких як Близький Схід і Латинська Америка, попит нарешті починає наздоганяти пропозицію, так що у 2024 році дефіцит кадрів кібербезпеки фактично скоротився.

Важливо відзначити, що дефіцит робочої сили розраховується як різниця між кількістю фахівців з кібербезпеки, які необхідні організаціям для належного захисту, і кількістю фахівців з кібербезпеки, які можуть бути найняті. Дефіцит кадрів не має на меті оцінити фактичний стан ринку праці для фахівців з кібербезпеки. У часи економічної нестабільності багато організацій пішли на скорочення, включаючи заморожування найму та звільнення. Це, однак, не впливає на дефіцит робочої сили, оскільки потреба організацій у фахівцях з кібербезпеки залишається незмінною, незалежно від того, чи є у них кошти для найму достатньої кількості персоналу.

Відповідно до розрахунків ISC2 у 2023 році обсяги дефіциту фахівців з кібербезпеки по всьому світу досягли позначки в майже 4 млн. осіб. Розподіл показників браку фахівців з кібербезпеки за регіонами показано на рис. 1.3.

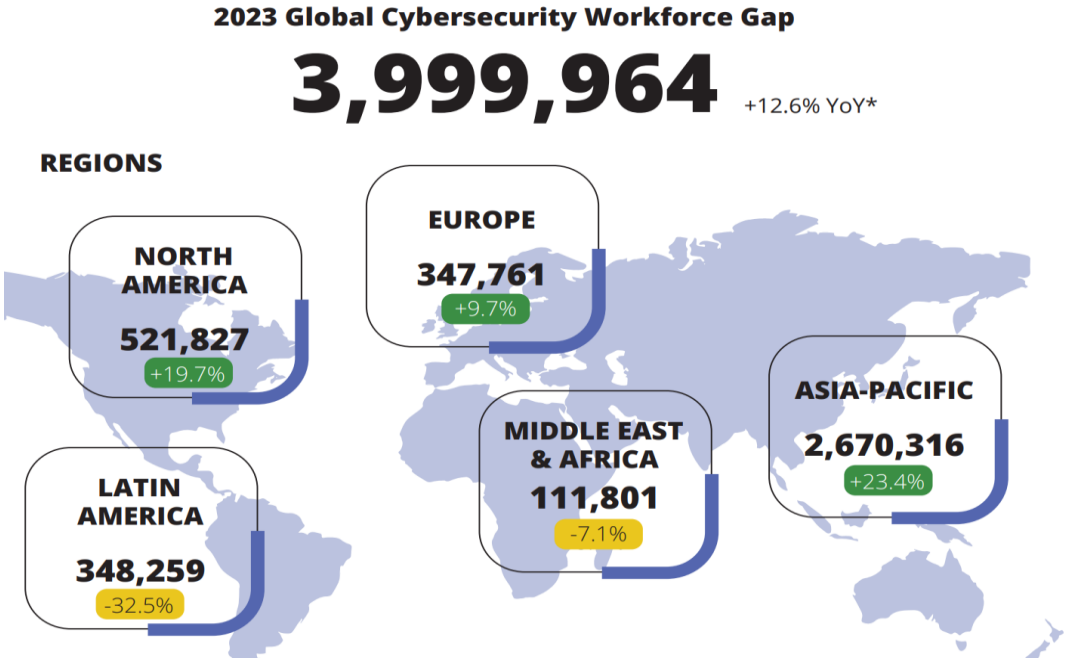


Рис. 1.3. Кількість фахівців з кібербезпеки у 2023 році згідно з дослідженням ISC2

Відповідно до звіту Міжнародного форуму з кібербезпеки у 2024 році глобальний дефіцит фахівців з кібербезпеки становить 2,8 мільйона осіб. Викликає тривогу той факт, що на кожні п'ять робочих місць у сфері кібербезпеки припадає менше чотирьох кваліфікованих фахівців. Азійсько-Тихоокеанський регіон стикається з найбільш гострим дефіцитом, на який припадає 60% глобального дефіциту. Цей дефіцит зумовлений роками недостатнього інвестування в поєднанні зі зростаючою важливістю кібербезпеки.

Дослідження показало, що 59% директорів з інформаційної безпеки стверджують, що дефіцит робочої сили є «головною перешкодою для досягнення їхньої позиції в галузі безпеки». Прогнози свідчать, що цей дефіцит стане ключовим фактором, який спричиняє понад 50% значних інцидентів кібербезпеки в усьому світі [2].

Скорочення та економічна невизначеність посилюють існуючу проблему дефіциту навичок. Нинішнє макроекономічне середовище нормалізувало

зростання витрат, зниження доходів і дефіцит робочої сили. Як наслідок, багато організацій вирішили скоротити витрати (наприклад, урізати бюджет, звільнити працівників, заморозити наймання та просування по службі), щоб підтримати свій баланс.

Однак ці організаційні скорочення, особливо в командах з кібербезпеки, мають наслідки, які виходять за рамки простого скорочення витрат. Фахівці з кібербезпеки є важливими захисниками від ризиків і вразливостей, але скорочення знижують їхню продуктивність, задоволеність та розвиток навичок. Кіберспеціалісти нарікають на те, що скорочення та пов'язані з ними проблеми, такі як нестача кадрів і прогалини в навичках, впливають на їхню повсякденну роботу, і наголошують на необхідності пошуку можливостей для вирішення цієї проблеми як на рівні організацій, так і держави.

Опитування 14 865 фахівців з кібербезпеки від ISC2 показало, що *скорочення є поширеною проблемою для фахівців з кібербезпеки*. Загалом 47% працівників сфери кібербезпеки стикалися зі скороченнями (звільнення, урізання бюджету, заморожування прийому на роботу або просування по службі), а 22% з цієї групи постраждали від скорочень (як прямих, так і непрямих) у сфері кібербезпеки. Ще 28% зазнали скорочень в інших підрозділах своїх організацій, що може суттєво вплинути на персонал з кібербезпеки (рис. 1.4).

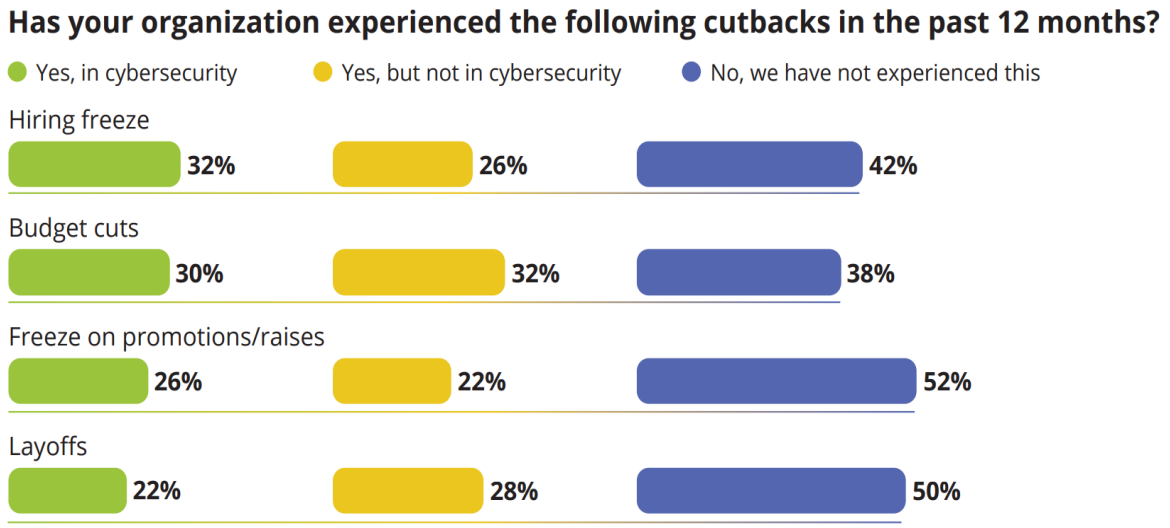


Рис. 1.4. Результати дослідження ISC2 щодо скорочення фахівців

41% респондентів вважають, що скорочення вплинули на їхню команду безпеки непропорційно більш масштабно у порівнянні з рештою персоналу організації. Крім цього, скорочення як команди кібербезпеки, так і решти організації можуть створити значні ризики для кібербезпеки.

Як свідчать результати дослідження, *скорочення впливають на деякі галузі та регіони значно сильніше, ніж на інші*. Скорочення відбулися в усіх основних галузях, але особливо постраждали від скорочень у сфері кібербезпеки індустрія розваг, будівництво, автомобільна промисловість і технологічний сектор. Географічно найбільше звільнень відбулося в Латинській Америці, потім - Близький Схід і Африка. [1].

Опитування IBM показало, що приблизно 64% дефіциту кадрів у сфері кібербезпеки непропорційно сконцентровано в чотирьох галузях: фінансові послуги, матеріали й обладнання, споживчі товари і технології (Рис. 1.5). Це не дивно, враховуючи, що вони є ціллю приблизно 70% всіх глобальних кібератак, а також з огляду на те, що вартість одного порушення у кожній з цих галузей, як правило, є найвищою [3].

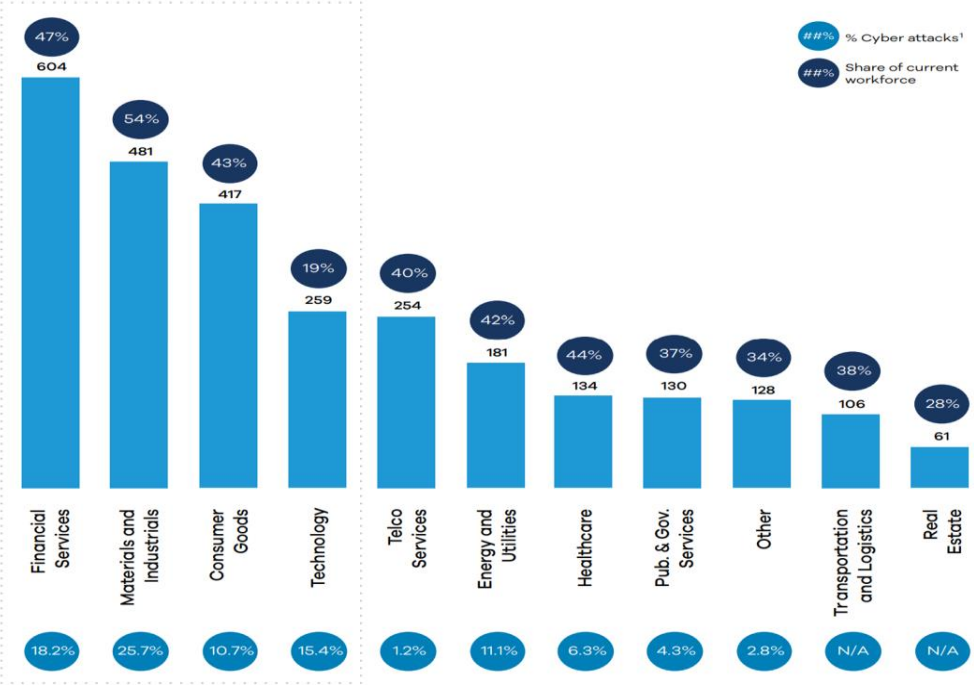


Рис. 1.5. Показники дефіциту кіберфахівців за галузями

Встановлено, що в результаті *скорочень організації консолідують ресурси та проводять реструктуризацію*, часто змінюючи підходи до роботи фахівців з

кібербезпеки. 53% опитаних стверджують, що скорочення призвели до затримок із закупівлею або впровадженням технологій, тоді як 40% організацій з тих, хто зазнав скорочень, реструктуризували свої команди безпеки або перемістили їх у межах організації. 35% навіть скасували навчальні програми з кібербезпеки, які є критично важливим чинником розвитку навичок і заповнення прогалин у знаннях.

Результати опитування підтвердили, що *скорочення також впливають на організації, що займаються кібербезпекою, на командному та індивідуальному* рівнях. 71% фахівців з кібербезпеки відчули негативний вплив скорочень на своє робоче навантаження. Майже дві третини фахівців стверджують, що скорочення також погіршують продуктивність, моральний дух команди і здатність підготуватися до майбутніх загроз. Інсайдерські ризики та реагування на загрози є ще двома ключовими елементами впливу скорочень на рівні команди. Більше половини фахівців (57%) відчули, що *скорочення в організації перешкоджають їхньому реагуванню на загрози*, а 52% побачили *збільшення кількості інцидентів, пов'язаних з внутрішніми ризиками* (Рис. 1.6).

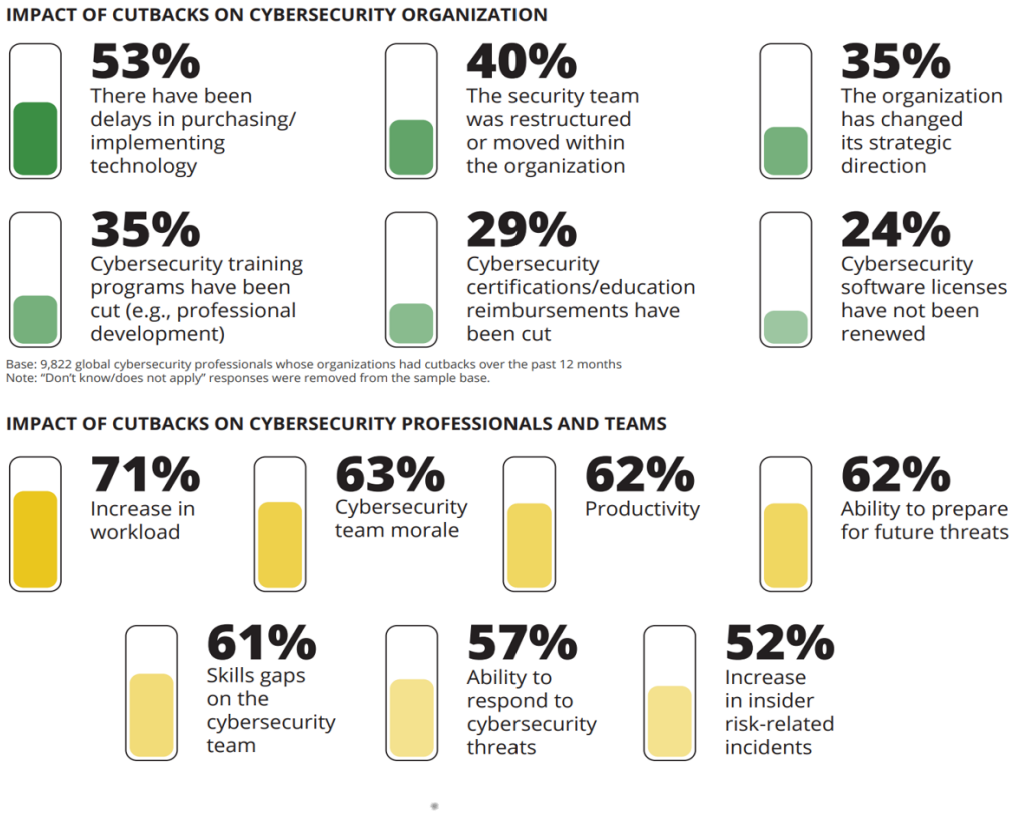


Рис. 1.6. Результати дослідження ISC2 щодо впливу скорочення фахівців з кібербезпеки на організацію

На думку 31% респондентів, у їхніх організаціях у подальшому відбудуться додаткові скорочення у сфері кібербезпеки, а 70% очікують, що ці скорочення включатимуть звільнення. 54% очікують додаткових скорочень у своїх компаніях загалом, незалежно від того, чи будуть вони стосуватися кібербезпеки, чи ні.

Майже дві третини опитаних працівників сфери кібербезпеки знають когось, кого звільнили цього року. Це стосується як працівників з кібербезпеки, так і представників інших сфер діяльності в їхніх власних організаціях, а також в інших організаціях. Те, що колег з кібербезпеки звільняють з інших організацій, може суттєво вплинути на сприйняття працівниками власних компаній. Навіть якщо респондент не знав когось, кого звільнили з його власної організації, але знав, що когось звільнили з іншої організації цього року, він майже втричі частіше очікував звільнень у власній організації протягом наступних 12 місяців [1].

### 1.2 Причини та наслідки дефіциту кадрів і прогалин у навичках

Попри значне зростання кількості спеціалістів, у багатьох країнах спостерігається критичний брак не лише працівників, а й компетентностей. Для розуміння глибини проблеми важливо проаналізувати причини, що спричиняють нестачу кваліфікованих кадрів, а також прогалини в навичках, які нерідко завдають ще більшої шкоди.

Організації відчувають нестачу кадрів та прогалини у навичках, але знаходять рішення - кадрове забезпечення. Очікується, що дефіцит кадрів посилиться, але він також сприймається по-різному залежно від стажу роботи. Хоча потреба в кадрах з кібербезпеки є як ніколи великою, звільнення та скорочення серед інших чинників спричинили значний дефіцит кадрів і прогалини у навичках з кібербезпеки. Дослідження виявило, що не вистачає персоналу для запобігання та усунення проблем з безпекою, а брак бюджету є поширеною причиною (Рис. 1.7).


Рис. 1.7. Причини дефіциту кіберфахівців згідно з дослідженням ISC2

Прогалини у навичках є поширеним явищем, але можуть становити більш серйозну проблему, ніж дефіцит персоналу. Нестача загальної кількості працівників з кібербезпеки в організації – це не єдина причина, через яку організації можуть відчувати брак кадрів з кібербезпеки. Дефіцит навичок відображає ситуацію, в якій командам кібербезпеки не вистачає працівників, які володіють певними навичками, необхідними для ефективного функціонування.

З'ясовано, що існує чітка і критична потреба заповнити прогалини в навичках у професії кібербезпеки. Визначивши, в яких сферах існують ці прогалини та які навички є найбільш бажаними, можна краще зрозуміти больові точки та наблизитися до вирішення проблеми.

Отже, відповідно до результатів опитування ISC2 майже всі організації мають прогалини в навичках з кібербезпеки. 92% фахівців з кібербезпеки стверджують, що їхні організації страждають від нестачі навичок в одній або декількох сферах, а 43% вказують на одну або більше значних або критичних прогалин у навичках в їхніх організаціях. Прогалини в навичках варіюються від

технічних навичок, таких як тестування на проникнення та впровадження Zero Trust, до нетехнічних навичок, таких як комунікація.

Встановлено, що значний вплив на дефіцит навичок мають звільнення. Більшість організацій, які зазнали скорочень у сфері кібербезпеки (51%), постраждали від втрати навичок порівняно з лише 39% організацій, які не зазнали скорочень. Насправді, звільнення, мають більший вплив на дефіцит навичок, ніж на загальну нестачу кадрів.

Прогалини у навичках часто мають гірші наслідки, ніж дефіцит фахівців. В організаціях може бути багато працівників з кібербезпеки, але якщо всім їм бракує певних критично важливих навичок, то надлишок персоналу може бути повністю зведений нанівець. 59% працівників сфери кібербезпеки зазначили, що прогалини у навичках можуть бути гіршими, ніж загальна нестача працівників. Ця цифра ще вища (67%) серед працівників, чиї організації насправді мають як прогалини в навичках, так і загальну нестачу персоналу [1].

Опитування також виявило можливості зменшення негативного впливу браку навичок. Так, 58% респондентів вважають, що негативний вплив дефіциту працівників можна пом'якшити, заповнивши прогалини у ключових навичках. Це робить критичним пріоритетом визначення і вжиття заходів для навчання працівників у життєво важливих сферах знань з кібербезпеки або надання компенсацій для зовнішнього професійного розвитку й отримання професійних сертифікатів і навчання.

Проблеми з підбором персоналу й відсутність стратегічного бюджетування також призводять до прогалин у навичках. Дві найпоширеніші причини розриву в навичках, на які вказали респонденти, - це неможливість знайти фахівців з необхідними навичками і боротьба за утримання власних працівників із затребуваними навичками через низьку заробітну плату, відсутність можливостей для просування по службі тощо.

Велику роль тут відіграє пропозиція достатньої винагороди за працю: 58% працівників з кібербезпеки в організаціях, які не пропонують конкурентну заробітну плату, відзначили, що в їхніх організаціях є прогалини в навичках,

незважаючи на те, що вони намагаються втримати людей із затребуваними навичками. Для порівняння, лише 38% працівників організацій, які платять високу заробітну плату, бачать прогалини в навичках. І загалом 48% організацій, які не пропонують конкурентну заробітну плату, мають значний дефіцит навичок, порівняно з 31% компаній, які пропонують прийнятну для персоналу оплату.

HR-менеджери, які займаються наймом фахівців з кібербезпеки, не можуть вирішити цю проблему через обмеження в політиці своїх організацій. Часи економічної нестабільності надають організаціям критично важливу можливість заохочувати нові шляхи розвитку кар'єри в сфері кібербезпеки, заповнюючи при цьому прогалини в навичках. Водночас, респонденти відзначили нестачу навчальних ресурсів для IT-персоналу, який хотів би займатися кібербезпекою (33%), ще однією головною причиною дефіциту навичок в їхніх компаніях.

Встановлено, що більш досвідчені в технічному плані IT-фахівці без попереднього досвіду роботи в сфері кібербезпеки зацікавлені в приєднанні до цієї професії. Ці вмотивовані спеціалісти подають заявки на посади і готові приєднатися до команд з кібербезпеки, однак деякі організації не надто охоче розширюють сферу найму.

Менеджери з підбору персоналу в сфері кібербезпеки погоджуються з тим, що їхні організації занадто неохоче приймають на роботу певні категорії працівників. Приблизно половина (45%) кажуть, що вони неохоче наймають працівників початкового рівня або що занадто сильно покладаються на освіту/диплом при пошуку кандидатів (45%) [1].

Слід відзначити, що дефіцит навичок найбільш поширений у критично важливих сферах. Найбільші прогалини у навичках виявлено у сферах, які набувають все більшого значення у світі кібербезпеки. Найпоширенішими прогалинами у навичках на сьогоднішній день є сфери безпеки хмарних обчислень, безпеки штучного інтелекту (ШІ) і машинного навчання (МН), а також реалізація концепції нульової довіри (Рис. 1.8).


Рис. 1.8. Види навичок з кібербезпеки, які становлять найбільший дефіцит згідно з дослідженням ISC2

Натомість звіт GCF, наряду з затребуваними навичками безпеки мережі й архітектури, а також хмарної безпеки, відносить до найбільш дефіцитних навичок у галузі кібербезпеки лідерство (керівництво), яку 50% організацій визначають як свій головний виклик зараз і через п'ять років. На їх думку, конвергенція кібербезпеки та ділової хватки є надзвичайно важливою, але її важко знайти серед наявних професіоналів.

Логічно, що скорочення, дефіцит кадрів і прогалини у навичках збільшують ризики для організацій, зокрема ризики кібератак і зниження рівня кіберзахисту. Так, 57% працівників стверджують, що дефіцит фахівців наражає їх організації на помірний або екстремальний ризик кібератак. Це пов'язано з нездатністю проводити критичну, ретельну оцінку ризиків і залишатися гнучкими в умовах складного ландшафту загроз через брак необхідних навичок.

В умовах економічної нестабільності знижується рівень упевненості у кібербезпеці. Дефіцит кадрів та прогалини в навичках підсилюють цю тенденцію. Про це свідчать результати опитування, відповідно до яких 52%

респондентів занепокоєні здатністю своїх команд з кібербезпеки забезпечити безпеку організації, особливо тих, у яких бракує фахівців, і, відповідно, навичок.

Аналіз GCF показує, що серед безлічі причин постійного дефіциту кадрів у сфері кібербезпеки, є складність наймати спеціалістів через невідповідність між попитом і пропозицією на професіоналів у цій галузі [2].

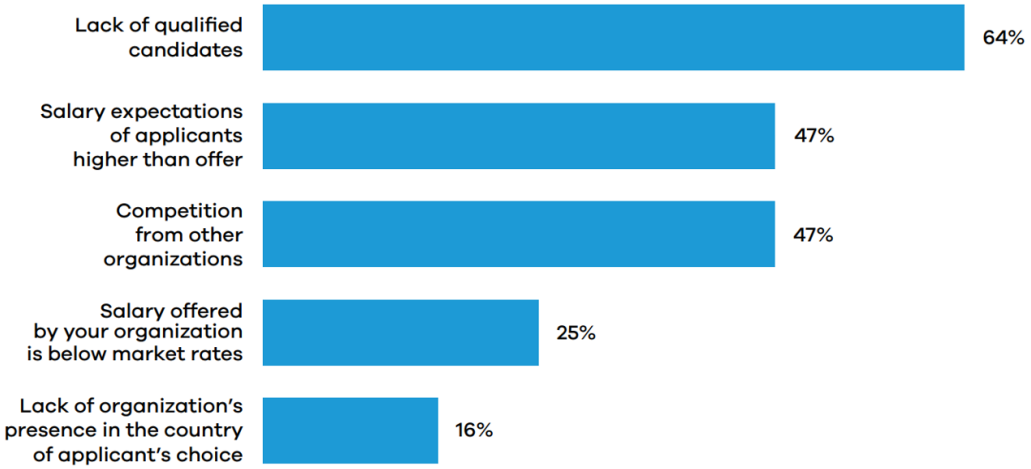


Рис. 1.9. Найбільші виклики у подоланні дефіциту фахівців з кібербезпеки відповідно до звіту GCF

Підсумовуючи, варто наголосити, що швидкий розвиток технологій має як величезні переваги, так і масштабні виклики для забезпечення кібербезпеки організацій. Опитування показало, що 60% організацій визначили швидку зміну технологій як найсерйозніший виклик для підтримання сучасних та ефективних команд кібербезпеки.

### 1.3 Шляхи подолання кадрової кризи в галузі кібербезпеки

В умовах загального браку спеціалістів і зростаючого ландшафту загроз організації змушені шукати ефективні механізми подолання кризи в кадровому забезпеченні. Сучасна практика доводить, що стратегічне управління талантами, інвестиції в навчання, переорієнтація підходів до найму і культура інклюзивності є тими інструментами, що дозволяють зменшити ризики.

Цілеспрямоване підвищення кваліфікації та покращення робочої культури зменшують ризики, пов'язані з нестачею кадрів і навичок. Незважаючи на ці виклики, існують способи, за допомогою яких організації можуть зменшити кіберризики, пов'язані з нестачею кадрів і прогалинами в навичках.

Для подолання цих перешкод доцільно реалізувати низку наступних кроків. Безсумнівною є необхідність упровадження ініціатив, спрямованих на запобігання або пом'якшення дефіциту кадрів. Ініціативи з навчання очолюють цей список разом зі створенням кращих умов праці та забезпеченням різноманітності, рівності й інклюзивності (Diversity, Equity, and Inclusion, DEI). Вони спрямовані на залучення й утримання найцінніших талановитих фахівців і підвищення кваліфікації персоналу всередині компанії.

Підвищення кваліфікації працівників є важливим, особливо в часи економічної нестабільності, коли багато компаній стикаються із заморожуванням найму. Освітні заходи можуть пом'якшити дефіцит кадрів, розподіляючи навички та запобігаючи значним прогалинам у експертизі. Дослідження показали, що організації, які сьогодні інвестують у навчання, майже вдвічі рідше мають критичні прогалини у навичках, ніж ті, які не інвестують і не планують цього робити. З іншого боку, виявлено, що аутсорсингові послуги практично не впливають на зменшення дефіциту кадрів.

Керівництво організації має постійно пам'ятати про негативний вплив на кадрову політику занепокоєння, невпевненості працівників у завтрашньому дні. Встановлено, що майже 65% працівників початкового і нижчого рівня побоювалися, що кількість працівників з кібербезпеки в їхніх організаціях зменшиться протягом наступних 12-ти місяців. Однак, чим вищий стаж респондента, тим менш імовірно, що він очікує скорочення працівників упродовж наступного року. Керівникам служб кібербезпеки важливо розуміти занепокоєння тих, хто стоїть нижче них в організаційній ієрархії, і обов'язково повідомляти про плани компанії щодо кадрового забезпечення в найближчому майбутньому.

Згідно з дослідженням ISC2 основними напрямами подолання дефіциту фахівців з кібербезпеки є перегляд і оновлення засад наймання персоналу; навчання й підвищення кваліфікації персоналу; перекваліфікація наявного персоналу; створення комфортних умов праці та висока оплата праці (Рис. 1.10):

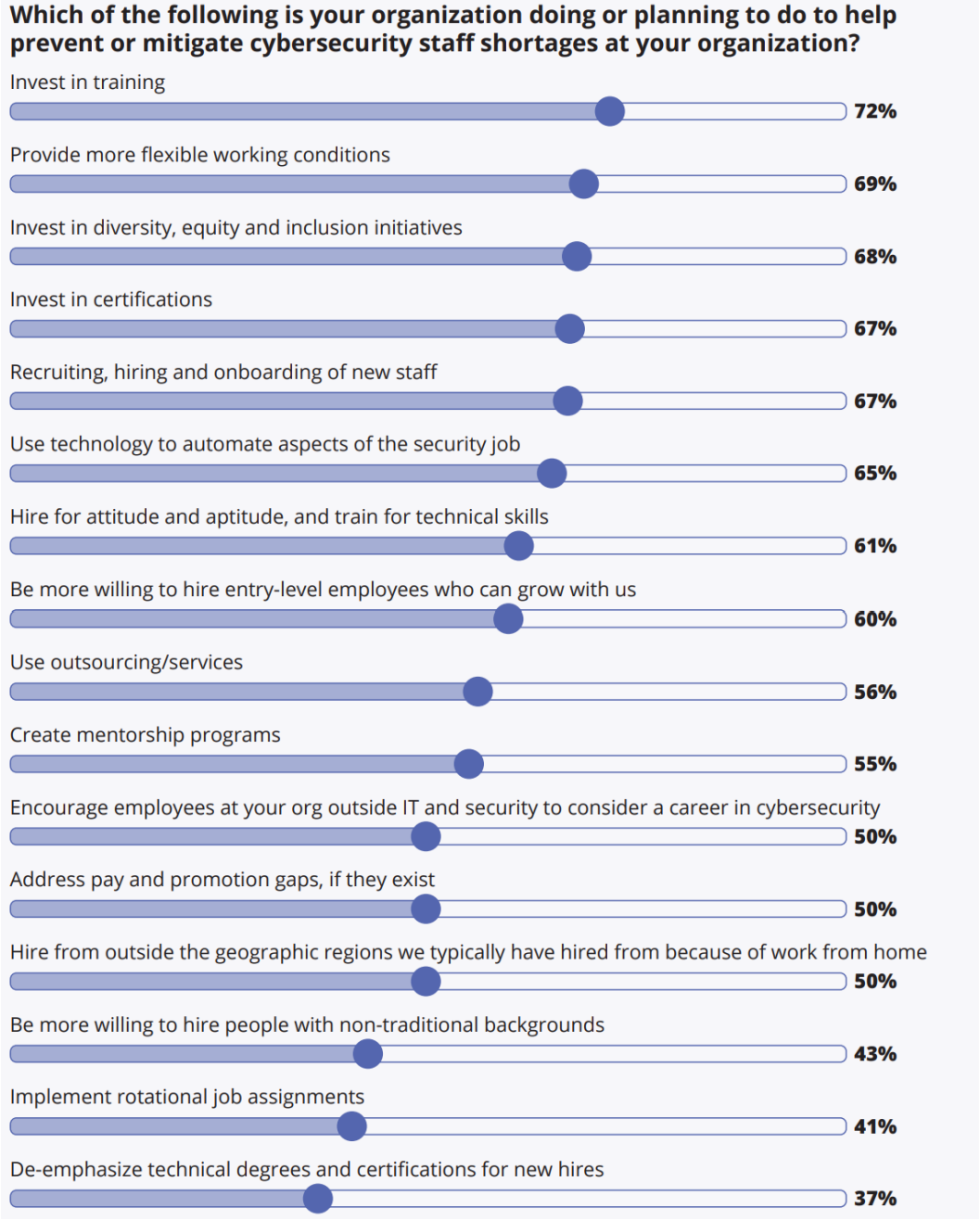


Рис. 1.10. Основні напрями подолання дефіциту фахівців з кібербезпеки згідно з дослідженням ISC2

1. Рекрутинг, найм та адаптація нового персоналу (67% респондентів); наймання персоналу за ставленням до праці та здібностями, в тому числі фахівців початкового рівня, з перспективою подальшого навчання технічним

навичкам - 61%; наймання працівників з інших географічних регіонів, в тому числі на умовах віддаленої роботи - 50% і кандидатів з нетрадиційним досвідом - 43%.

2. Інвестування в навчання (72% опитаних), сертифікацію (67%); ініціативи щодо різноманітності, рівності та інклюзивності (68%); використання аутсорсингових послуг з навчання й підвищення кваліфікації - 56%; реалізація програм наставництва - 55%.

3. Заохочення працівників своєї організації, які не належать до IT та безпеки, будувати кар'єру в сфері кібербезпеки - 50%; ротації кадрів - 41%.

4. Забезпечення більш гнучких умов праці - 69%; використання нових технологій для автоматизації різних аспектів роботи у сфері безпеки - 65%; усунення розриву в оплаті праці та просуванні по службі - 50% [1].

GCF бачить можливості вирішення проблеми нестачі кваліфікованих фахівців із кібербезпеки у дотриманні принципів Рамкової програми управління талантами кібербезпеки (The Cybersecurity Talent Framework), яка передбачає приваблення, залучення талановитих осіб у галузь кібербезпеки, забезпечення освіти і практичного навчання фахівців з кібербезпеки, працевлаштування талановитих кандидатів на посадах з кібербезпеки, утримання високо-кваліфікованих спеціалістів у кібергалузі [4] (Рис. 1.11).


Рис. 1.11. Основні етапи програми управління талантами кібербезпеки

Для формування професійних кадрів з кібербезпеки необхідні комплексні та спільні зусилля в рамках всієї екосистеми кібербезпеки. Стратегічні рекомендації GCF охоплюють всю Рамкову програму розвитку талантів у сфері кібербезпеки [4]. Пріоритетні заходи управління талантами показані на рис. 1.12.


Рис. 1.12. Пріоритетні заходи формування кваліфікованої робочої сили з кібербезпеки

Розглянемо представлені заходи детальніше.

*Цільове та стратегічне охоплення.* Одним із важливих напрямів зусиль щодо формування кваліфікованої робочої сили з кібербезпеки є впровадження цілеспрямованих ініціатив з набору персоналу, спрямованих на недостатньо залучені групи, зокрема жінок і представників меншин, шляхом тісної співпраці з освітніми установами, галузевими органами та громадськими організаціями. Ці партнерства мають виходити за рамки поверхневої взаємодії і включати стипендії, програми наставництва і спеціальні кар'єрні шляхи, які безпосередньо спрямовані на подолання бар'єрів, з якими ці групи стикаються при входженні в сферу кібербезпеки.

*Впровадження кібербезпеки в організаційну ДНК* забезпечується шляхом підвищення ролі кібербезпеки в рамках основної корпоративної стратегії, а також позиціонування її як важливої для місії та довгострокового успіху організації. Слід популяризувати ці ролі не просто як технічні посади, а як такі,

що мають вирішальне значення для захисту глобальної цифрової безпеки, залучаючи таким чином професіоналів, мотивованих не стільки технічними викликами, скільки важливістю місії та цілей кібербезпеки.

*Національні та академічні кампанії за кар'єру в сфері кібербезпеки.* Обов’язковим компонентом створення кваліфікованого пулу фахівців з кібербезпеки є співпраця з державними органами й освітніми закладами для запуску національних кампаній, які позиціонують кібербезпеку як найкращий вибір кар'єри, використовують сучасні підходи, реальні кейси, рольові моделі та інтерактивні навчальні платформи.

Заклади освіти мають тісно співпрацювати з галуззю для забезпечення профорієнтації в режимі реального часу, гарантуючи, що студенти розуміють різноманітні та динамічні можливості в секторі кібербезпеки. Ця діяльність охоплює розширення доступу до стажувань, навчання та раннього кар'єрного досвіду, що сприятиме плавному переходу студентів у категорію працівників-практиків. Крім цього, навчальні заклади повинні співпрацювати з компаніями галузі кібербезпеки у ході розробки навчальних програм з урахуванням попиту.

*Інтеграція питань кібербезпеки в систему освіти з початкового рівня* передбачає впровадження компонентів з кібербезпеки в навчальні програми початкової та середньої школи, щоб розвивати інтерес і фундаментальні галузеві знання на ранніх етапах навчання. Це має бути підкріплено практичними проєктами, клубами з кібербезпеки і партнерством із професіоналами галузі, які можуть забезпечити реальний контекст і наставництво.

*Оновлення навчальних програм відповідно до потреб галузі кібербезпеки* має на меті забезпечення відповідності і тісного взаємозв’язку програм і планів навчання майбутніх кіберфахівців динамічним вимогам і потребам галузі. Це передбачає включення навчання з кібербезпеки в різні дисципліни, такі як право, бізнес та інженерія, щоб гарантувати, що ці фахівці будуть всебічно розвиненими і здатними у рамках своїх професійних обов’язків вирішувати проблеми кібербезпеки.

*Сприяння розвитку культури безперервного навчання.* На думку експертів, організації самі мають робити значний внесок у розвиток потенціалу своїх фахівців з кібербезпеки, зокрема шляхом створення платформи безперервного навчання, які забезпечать працівникам із кібербезпеки постійний доступ до новітніх знань, інструментів і передових практик. Варто використовувати партнерські відносини з лідерами галузі й постачальниками освітніх послуг, щоб пропонувати сертифікати, мікрокредити та програми підвищення кваліфікації, які допоможуть працівникам випереджати нові загрози. Ці ресурси можна централізувати в легкодоступному, комплексному навчальному центрі для підтримки професіоналів на всіх етапах кар'єри [4-5].

*Впровадження практики наймання персоналу з кібербезпеки на основі навичок* відображає зміну підходів до працевлаштування. Для визначення конкретних навичок, компетенцій і знань, необхідних для пріоритетних робочих місць і ролей у сфері кібербезпеки організаціям рекомендують використовувати напрацьовані документи:

– Концепцію робочої сили з кібербезпеки (NICE) від Національного інституту стандартів і технологій NIST [6];

– Європейську концепцію навичок з кібербезпеки (ECSF) від Європейської агенції з кібербезпеки ENISA [7];

– Дорожню карту розвитку робочої сили у галузі кібербезпеки (SCyWF14) від Глобального форуму з кібербезпеки (GCF) [8].

*Розширення кадрового резерву за допомогою інклюзивних практик.* Актуальним викликом для сучасних організацій є розширення зусиль з підбору персоналу й охоплення ними нетрадиційних кандидатів, зосередившись на здібностях і потенціалі, а не лише на досвіді. Це передбачає залучення жінок та інших недостатньо представлених груп на стажування і працевлаштування на посади початкового рівня, а також зобов'язання підвищувати кваліфікацію та перекваліфікацію за потреби. Такі стратегії можуть ефективно подолати дефіцит кадрів і наповнити команди кібербезпеки свіжими кадрами.

*Створення інклюзивної, різноманітної та сприятливої культури.* Сьогодні організаціям необхідно впроваджувати комплексні стратегії та ініціативи, які виходять за рамки політики, щоб створити справді інклюзивну культуру на робочому місці. Серед основних виділяють ініціативи, спрямовані на підвищення психологічної безпеки персоналу, гендерної рівності, добробуту, а також створення мереж і програм наставництва, які підтримують утримання і просування жінок та інших слабо представлених у сфері кібербезпеки груп.

*Прозорий кар'єрний ріст та розвиток.* Важливим завданням організації у справі формування кваліфікованої робочої сили з кібербезпеки є розробка прозорих шляхів розвитку кар'єри, які надають кіберфахівцям чіткі можливості для зростання, навчання та просування по службі. Для цього доцільно налагодити механізми постійного зворотного зв'язку, розробити плани професійного розвитку й забезпечити доступ до тренінгів з лідерства, щоб підвищити задоволеність роботою і зменшити плинність кадрів. Таким чином організація гарантовано може утримати найкращі таланти у висококонкурентній галузі [5,9].

Для подолання глобального дефіциту робочої сили та розриву в навичках необхідна співпраця між керівниками органів державної влади, топ-менеджерами приватних організацій, а також в екосистемі кібербезпеки загалом. Лідери повинні працювати разом, щоб надихати і розвивати наступне покоління кіберфахівців, покращуючи освіту, підвищуючи обізнаність і надаючи можливості працевлаштування недостатньо представленим групам.

Зусилля щодо формування кваліфікованої робочої сили з кібербезпеки мають також охоплювати інтеграцію кібербезпеки в шкільні програми, розробку програм навчання і підвищення кваліфікації, сприяння розвитку різноманітних талантів і створення інклюзивного середовища. Надання пріоритету розвитку робочої сили та випередження мінливого ландшафту загроз може забезпечити безпечне цифрове майбутнє і продовжити сприяти глобальному економічному і технологічному прогресу. У протилежному випадку, організації можуть залишитися без засобів захисту критично важливих систем, зазнати фінансових

втрат, допустити до підриву довіри до цифрових систем, які лежать в основі глобальної економіки.

**Висновки до розділу 1**

Встановлено, що внаслідок зростання потреби у спеціалістах з кібербезпеки упродовж останніх кількох років питання підготовки та підвищення кваліфікації кіберфахівців є серйозним викликом. Сьогодні галузь кібербезпеки, яка через економічну нестабільність скоротила значну кількість персоналу, все одно переживає серйозний дефіцит кадрів, потребуючи від близько 3 до 4 млн. нових працівників. На думку експертів, ця тенденція буде тільки посилюватися.

Основними причинами нестачі фахівців з кібербезпеки є труднощі в пошуку кваліфікованих працівників, недостатній бюджет на працевлаштування кіберфахівців, відносно низький рівень заробітної плати, значна конкуренція і висока плинність кадрів з кібербезпеки, недооцінювання керівництвом важливості персоналу з кібербезпеки, недостатнє навчання і підвищення кваліфікації діючих працівників, низька пріоритетність забезпечення кібербезпеки на рівні організації.

Дослідження показало, що трьома найпоширенішими прогалинами у кібернавичках є питання безпеки мережі й архітектури, хмарних обчислень, ШІ та МН, а також реалізація концепції нульової довіри. Крім перелічених до найбільш дефіцитних навичок у галузі кібербезпеки експерти відносять лідерство, яке 50% організацій визначають це як свій головний виклик зараз і на найближчі п'ять років.

За результатами аналізу виділено такі основні способи подолання проблеми нестачі кадрів і прогалин у навичках на рівні організації: навчання й сертифікація фахівців за кошти організації; створення кращих (гнучких) умов праці, впровадження ініціатив з різноманітності, рівності та інклюзивності персоналу; підвищення кваліфікації наявних працівників; наймання персоналу за ставленням і здібностями, а не знаннями й навичками; наймання спеціалістів

початкового рівня з подальшим навчанням і працівників для віддаленої роботи; перекваліфікація ІТ-фахівців; висока оплата праці і просування по службі.

У рамках всієї екосистеми кібербезпеки експерти рекомендують впроваджувати цілеспрямовані ініціативи з набору персоналу, спрямовані на недостатньо представлені групи; усвідомити значення кібербезпеки як критично важливої діяльності на рівні організацій; проводити національні кампанії просування кібербезпеки як найкращого варіанту кар'єри у співпраці організацій і державних органів; сприяти інтеграції освіти з кібербезпеки в навчальні програми початкової та середньої школи з метою раннього розвитку інтересу і фундаментальних галузевих знань; оновлювати навчальні програми з кібербезпеки й інтегрувати їх елементи в інші програми підготовки; розвивати культуру безперервного навчання тощо.

# РОЗДІЛ 2. ОСОБЛИВОСТІ РОЗВИТКУ РОБОЧОЇ СИЛИ В ГАЛУЗІ КІБЕРБЕЗПЕКИ В УКРАЇНІ

## 2.1. Характеристика поточного стану ринку кібербезпеки України

Ринок праці у сфері кібербезпеки в Україні за останні роки зазнав істотних змін під впливом цифровізації та зростання кіберзагроз. За останні вісім років український ринок кібербезпеки зріс у чотири рази, досягнувши $138 млн у 2024 році. За прогнозами, протягом наступних п’яти років ринок зросте ще на 50% і досягне $209 млн (Рис. 2.1). Про це свідчать результати дослідження, проведеного компанією DataDriven Research & Consulting, ініційованого підкомітетом з кібербезпеки Європейської бізнес-асоціації (EBA) та комітетом з кібертехнологій Асоціації «IT України». Дослідження було проведено за підтримки Aspen Institute Kyiv, який реалізує програму «Діалог з кібербезпеки», та Програми USAID Cybersecurity Activity [10].

Наразі частка України на глобальному ринку у сфері кібербезпеки – менше 1%. Проте Україна є законодавцем трендів на ринку кібербезпеки, випереджаючи інші країни за кіберекспертизою, завдяки роботі у сегменті досліджень і розробок, особливо в розробці інноваційних рішень.

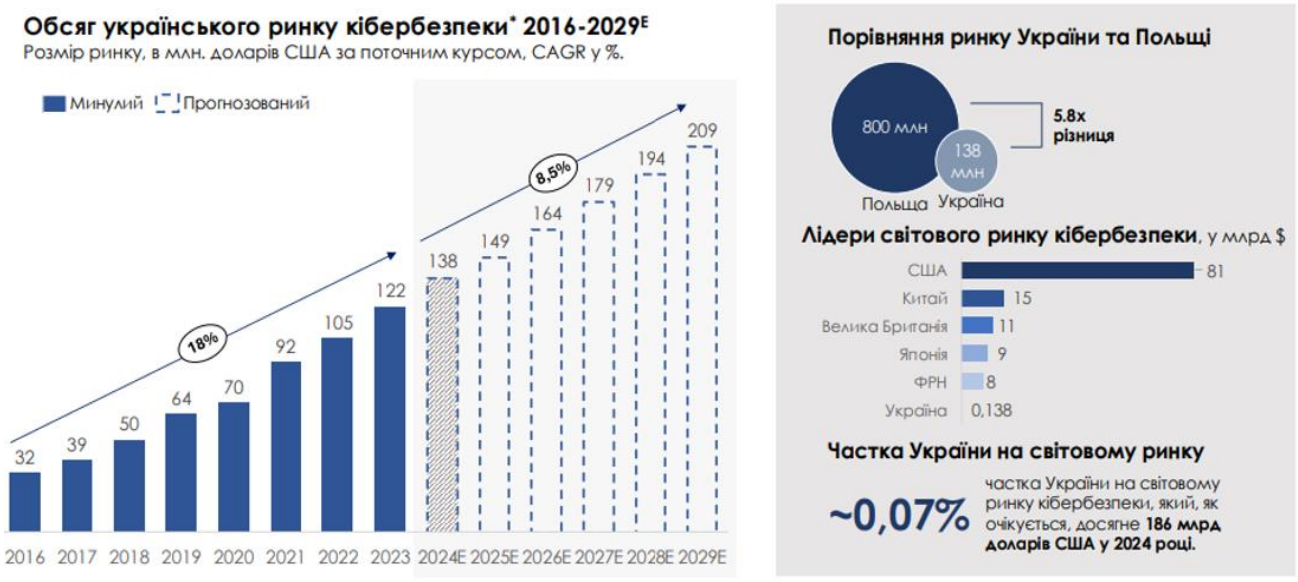


Рис. 2.1. Прогнозування ринку

Також з дослідження є розуміння, який ріст ринку кібербезпеки був у попередні роки, його неоднорідність, з періодами прискорення та сповільнення, в 2020, 2021 та 2022 роках:

- У 2020 році, під впливом COVID-19 бізнес зіткнувся з фінансовими проблемами і бюджетними обмеженнями, надаючи пріоритет основним оперативним процесам, а не інвестиціям у кібербезпеку. Ресурси були перерозподілені на підтримку віддаленої роботи, що призвело до скорочення витрат на передові рішення з кібербезпеки.
- Прискорення росту ринку у 2021 році було зумовлено зростанням кіберзлочинності, посиленням уваги до кібербезпеки та безперервною діловою активністю через реструктуризацію в умовах карантину. Найбільше зростання спостерігалося у сфері хмарної безпеки (+76%), оскільки компанії все більше покладалися на хмарні сервіси для віддаленої роботи.
- Помірний ріст ринку у 2022 році був зумовлений релокаціями компаній та закриттями офісів, що призвели до зменшення внутрішнього попиту на кібербезпеку та сповільнення росту інвестицій. Держава частково задовільнила зростаючі потреби у сфері кібербезпеки за рахунок робітників держсектору та мобілізації [10].


Рис. 2.2. Тенденції зростання ринку кібербезпеки України

Ключовим сегментом українського ринку кібербезпеки є мережева безпека. Найшвидше розвиваються сфери хмарної безпеки, захисту даних і безпеки кінцевих точок, що відображає зростаючий попит на нові технології й рішення в Україні.

На світовому ринку кібербезпеки у 2024 році домінує сегмент безпекових послуг із часткою 53%, тоді як в Україні переважають кіберрішення, частка яких становить 57%. Така структура зумовлена низкою ключових чинників:

• *Зростанням частоти та масштабу кібератак.* Повномасштабна війна призвела до значного збільшення кількості та складності атак на інформаційні системи України, що, своєю чергою, зумовило необхідність швидкого впровадження автоматизованих рішень, таких як шифрування даних, системи автоматичного виявлення загроз тощо.

• *Необхідністю оперативного реагування.* В умовах постійної загрози масштабних кібератак українські компанії змушені надавати перевагу готовим кіберрішенням, які можна впровадити негайно, замість тривалого розроблення персоналізованих засобів захисту.

• *Дефіцитом кваліфікованих фахівців.* Обмежена кількість спеціалістів у галузі кібербезпеки спричинила активне використання автоматизованих рішень, які потребують мінімального людського втручання.

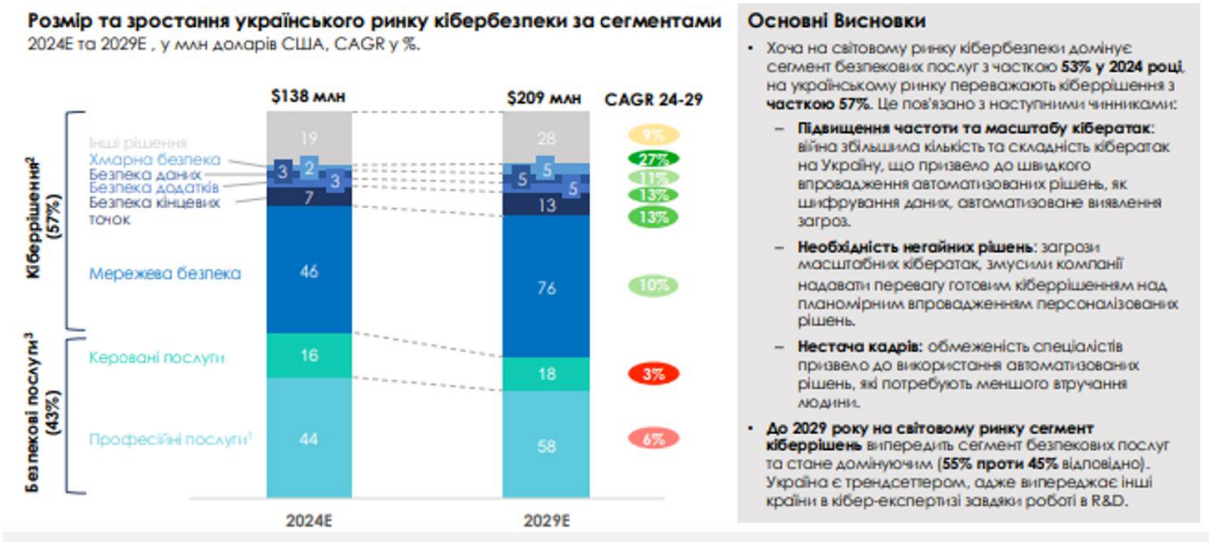


Рис. 2.3. Сегмент мережевої безпеки

Основними рушійними силами ринку в Україні є цифровізація та зростання ризику реальних втрат від кібератак (Рис. 2.4).


Рис. 2.4. Основні рушійні сили ринку

Інші фактори, що сприяють зростанню ринку, охоплюють:

*1. Всебічна цифровізація.* З впровадженням цифрових рішень у державному та бізнес-секторах зростає ризик кіберзагроз. Це вимагає зміцнення заходів безпеки для захисту конфіденційної інформації та забезпечення стабільної роботи систем.

*2. Ріст обсягу кібератак.* Перебування в умовах кібервійни є ключовим чинником зростання кількості атак. Усі сектори змушені реагувати на підвищені ризики, інвестуючи в передові рішення з кіберзахисту.

*3. Зростання ризику реальних втрат.* Кібератаки (віруси-вимагачі, витоки даних) порушують бізнес-процеси, спричиняють простої та значні витрати. Також можливі втрати прибутку, репутаційні збитки та зниження довіри клієнтів.

*4. Стимулювання ринку донорами.* Під час війни розвиток галузі значною мірою залежить від міжнародної технічної допомоги (наприклад, проєкти USAID) та підтримки з боку світових і національних компаній. Така підтримка є критично важливою в умовах обмеженого державного фінансування.

*5. Ріст популярності та спроможностей ШІ.* ШІ використовується як для посилення кіберзахисту, зокрема виявлення загроз, аналіз даних, автоматизація безпеки, так і як інструмент нових, складніших атак .

Інновації, такі як використання ШІ для автоматизації реагування та блокчейну для захисту передачі даних, формують нові підходи до безпеки. Дослідження визначає ключові тренди на ринку кібербезпеки: мережева безпека залишатиметься найбільшим сегментом (36% до 2029 року), а хмарна безпека демонструватиме найдинамічніше зростання. У той самий час, українські розробники ПЗ продовжать відставати від міжнародних гравців у складності рішень, а принципи «нульової довіри» визначатимуть нові моделі поведінки користувачів та бізнесу.

Також згідно з цим дослідженням розуміємо, що повномасштабна війна Росії спричинила сплеск кібератак в Україні, збільшивши попит на автоматизовані рішення та інноваційні технології. В Україні постійні кібератаки російських хакерських груп, таких як UAC-0010, спрямовані переважно на державні установи, оборонну промисловість, телекомунікації, фінансові установи та енергетичний сектор. У 2023 році було зафіксовано 2544 кіберінциденти, що на 16% більше, ніж у 2022 році (Рис. 2.5) [10].

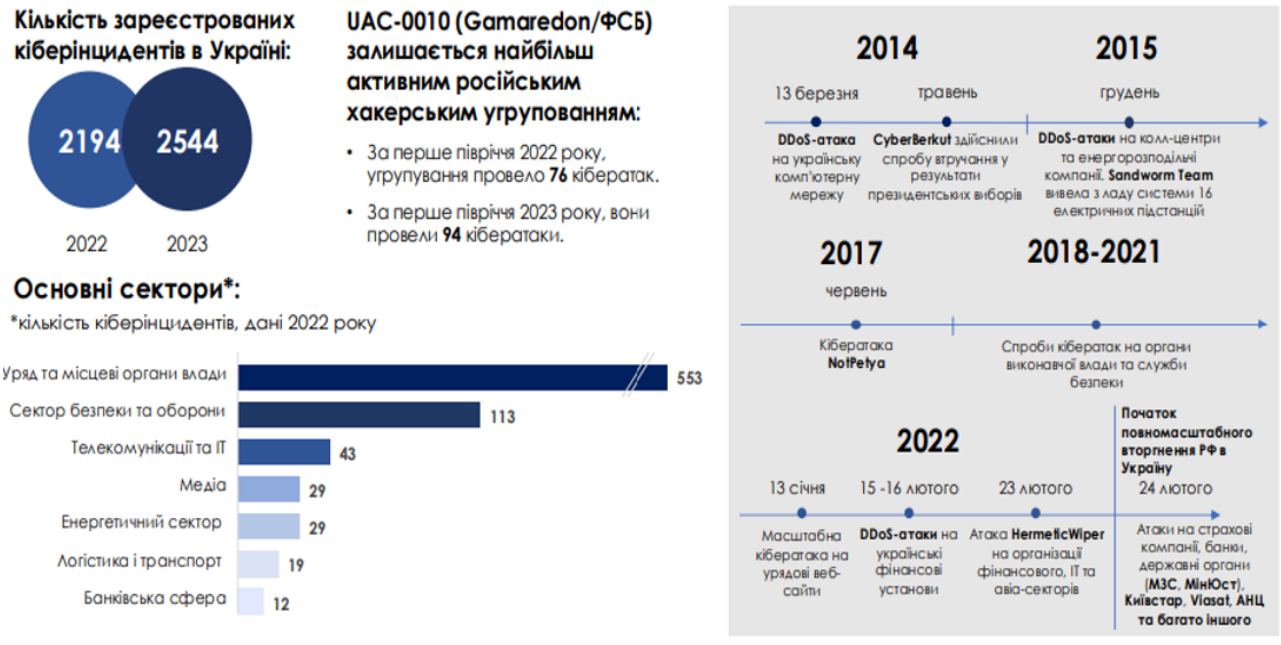


Рис. 2.5. Статистика кібератак в Україні в умовах збройного конфлікту

Таким чином, однією з характерних рис сучасного ринку кібербезпеки України є дефіцит кваліфікованих фахівців, яка серйозно впливає на розвиток галузі.

## 2.2. Методи підготовки та підвищення кваліфікації фахівців з кібербезпеки в Україні

Зважаючи на кількість загроз та високу швидкість розвитку галузі кібербезпеки, Українська держава та вітчизняні підприємства, установи й організації потребують висококваліфікованих фахівців з кібербезпеки у достатній кількості. Тільки за наявності потужної робочої сили можна забезпечити високий рівень захищеності національного інформаційного простору.

Однак, Україна, як і більшість держав світу, відчуває суттєву нестачу спеціалістів з кібербезпеки, зокрема за такими напрямами як тестування на проникнення, моніторингу захищеності, управління інцидентами, аналізу загроз і вразливостей. Натомість, найбільшим є попит на експертів з кіберзахисту, адміністраторів інформаційної безпеки та спеціалістів із захисту персональних даних. З огляду на постійні технологічні нововведення, фахівці мають демонструвати володіння найактуальнішими знаннями та навичками для ефективної протидії кіберзагрозам.

*Формальна освіта.* Для вирішення цієї проблеми зусилля української влади, компаній та закладів освіти спрямовуються насамперед на розвиток системи формальної освіти, яка забезпечує підготовку фахівців у сфері кібербезпеки у вищих навчальних закладах на першому (бакалаврському) та другому (магістерському) рівнях вищої освіти. Слід відзначити, що популярність спеціальності F5 (125) Кібербезпека та захист інформації постійно зростає.

Станом на 2025 рік фахівців з кібербезпеки готують понад 60 закладів вищої та передвищої фахової освіти [11]. Рейтинг найбільш затребуваних ЗВО України [12], які впровадили освітні програми за спеціальністю Кібербезпека та захист інформації, показано на рис. 2.6.

З огляду на зростання зацікавленості в отриманні вищої освіти з кібербезпеки вищі навчальні заклади відкривають профільні спеціальності, удосконалюють навчальні програми відповідно до міжнародних стандартів і

вимог потенційних роботодавців, прагнуть забезпечити високу якість і практичну спрямованість підготовки кіберспеціалістів.

**10 найпопулярніших університетів серед вступників на кібербезпеку у 2024 році**:

1. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».
2. Національний університет «Львівська політехніка».
3. Національний авіаційний університет.
4. Київський національний університет імені Тараса Шевченка.
5. Державний університет інформаційно-комунікаційних технологій.
6. Вінницький національний технічний університет.
7. Державний торговельно-економічний університет.
8. Львівський національний університет імені Івана Франка.
9. Київський національний економічний університет імені Вадима Гетьмана.
10. Харківський національний університет радіоелектроніки.

Рис. 2.6. Рейтинг кращих закладів освіти, які готують фахівців з кібербезпеки

Попри певні труднощі з ІТ-сферою в Україні у 2024 році до десятки найпопулярніших спеціальностей увійшли аж три ІТ-спеціальності, серед яких і «Кібербезпека та захист інформації» (Рис. 2.7) [13].

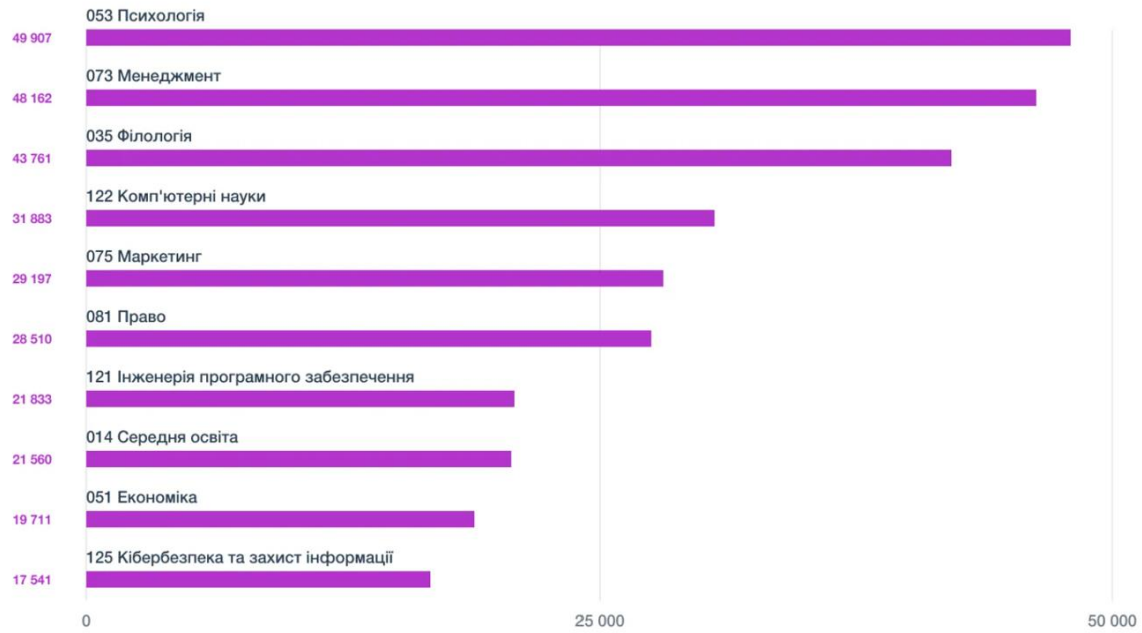


Рис. 2.7. Рейтинг найпопулярніших спеціальностей ЗВО у 2024 році

На сьогодні спеціальність F5 (125) Кібербезпека та захист інформації охоплює три спеціалізації, які загалом зосереджені на технологіях, технічних засобах та управлінні кібербезпекою та захистом інформації.

Про популярність спеціальності свідчать результати досліджень, відповідно до яких лише у 2024 році на дану спеціальність зареєстровано 17329 заяв. У 2024 році на підготовку бакалаврів за спеціальністю 125 «Кібербезпека та захист інформації» держава виділила 1 457 бюджетних місць [12].

Усі компетенції та навички випускників освітніх програм зібрані у стандарті вищої освіти за спеціальністю зі змінами від 29 жовтня 2024 року [14].

Аналіз стратегій розвитку провідних технічних вишів України [15-18] показав, що основними завданнями підготовки ІТ-спеціалістів загалом, і фахівців з кібербезпеки зокрема є: запровадження нових перспективних напрямів підготовки; забезпечення високої якості освітніх послуг; постійне оновлення освітніх програм і планів, змісту навчання з урахуванням інновацій і тенденцій розвитку галузі, вимог працедавців; забезпечення практичної спрямованості навчального процесу з використанням новітніх технологій і засобів захисту інформації; ефективна співпраця з компаніями-представниками для урахування вимог ринку праці і галузі кібербезпеки у процесі навчання; міжнародний обмін студентами і викладачами для запозичення передового досвіду кращих закордонних закладів вищої освіти.

Велика увага зосереджена закладів вищої освіти приділяється спрямуванню підготовки здобувачів на здобуття практичного досвіду за фахом. Студенти проходять навчання, імітуючи реальні робочі ситуації спеціалістів з кібербезпеки, у лабораторіях, функціонування яких підтримується провідними компаніями в галузі ІТ та кібербезпеки: Huawei, IBM, Cisco, ESET тощо [19-20].

Навчання ґрунтується на компетентнісному підході, який враховує потреби ринку праці і надає студентам можливість оволодіти практичними навичками роботи з SOC системами, інструментами OSINT, SIEM,

інструментами цифрової криміналістики і платформами для виявлення шкідливого програмного коду.

Частою практикою у закладах вищої освіти України є підтримання тісного партнерства з компаніями-партнерами щодо проведення навчальних курсів і організації стажувань, після завершення яких видаються сертифікати, які підтверджують набуття нових компетенцій.

*Неформальна освіта*. З метою покращення якості підготовки здобувачів вищої освіти та її адаптивності до вимог і тенденцій розвитку галузі провідні вітчизняні підприємства, державні органи та міжнародні структури розгортають власні програми професійного навчання та підвищення кваліфікації для фахівців. Ці програми зосереджені на практичному навчанні, пристосованому до специфічних проблем кібербезпеки в бізнесі та державному секторі, і відіграють значну роль у створенні надійної кіберсистеми в Україні.

Наприклад, компанія «IT Спеціаліст», яка надає професійні послуги у сфері IT та кібербезпеки, розробила інтегровану систему корпоративного навчання та підвищення кваліфікації експертів з кібербезпеки CyberIN [21]. Програма CyberIN, реалізується у співпраці з українськими вишами, розроблена для вдосконалення практичних навичок роботи з системами захисту інформації в реальному середовищі. Вона розрахована як на тих, хто лише починає свій шлях у сфері кібербезпеки, так і на досвідчених спеціалістів, які прагнуть покращити свої знання та навички відповідно до актуальних міжнародних стандартів: ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls тощо.

Основними компонентами програми CyberIN є основний блок, спеціальні та профільні дисципліни, кожен з яких має на меті формування комплексу професійних і «м’яких» навичок (Таблиця 2.1).

Таблиця 2.1.

Програма курсу CyberIN

| **Блок** | **модуль** | **зміст** |
|---|---|---|
| **База** | **Hard skills** | -Computer networking<br>-Windows<br>-Linux |
| | **Soft skills** | -Кібергігієна<br>-Клієнтоорієнтованість<br>-Ділова етика |
| **Спеціальні дисципліни** | **Hard skills** | -Архітектура корпоративних систем<br>-Системи захисту<br>-Pentest<br>-Security Operation Center<br>-Віртуалізація, контейнеризація та хмари<br>-СУІБ та перевірка відповідності стандартам PCI DSS, GDPR, SWIFT |
| | **Soft skills** | -Корпоративні комунікації<br>-Ефективна робота в команді<br>-Культура роботи з документами<br>-Культура листування |
| **Профільні дисципліни** | **Hard skills** | -Автоматизація робочих проєктів<br>-Pentest<br>-SOC<br>-Security Engineering – SIEM |
| | **Soft skills** | -Проєктне управління<br>-Публічні виступи |

**Навчання Re/start in Cyber.** Навчальна програма для світчерів, які мріють побудувати кар’єру у кібербезпеці від ISSP

Ще одну можливість навчання пропонує українська компанія ISSP (Information Systems Security Partners) разом з Міністерством цифрової трансформації України, канадський Toronto Metropolitan University та рекрутингова платформа BazaIT, які запустили безкоштовну 3-місячну

навчальну програму «Re/start in Cyber» для бажаючих розпочати кар’єру в галузі кібербезпеки або змінити свою нинішній фах на професію кіберфахівця [22].

Основною метою програми є надати талановитим українцям якісні знання та практичні навички, що допоможуть їм знайти свою першу роботу в кібербезпеці.

Програма охоплює такі основні теми у галузі кібербезпеки: компоненти та концепції комп'ютера; операційні системи, контейнери й віртуалізація; мережа Інтернет; ОС Linux; основи мережевої взаємодії; сервери баз даних і електронної пошти; практичне програмування та концепції; основи Windows; сучасне комп'ютерне обладнання; концепції безпеки; концепції наступальної безпеки проникнення в мережі та комп'ютери (Рис. 2.8).

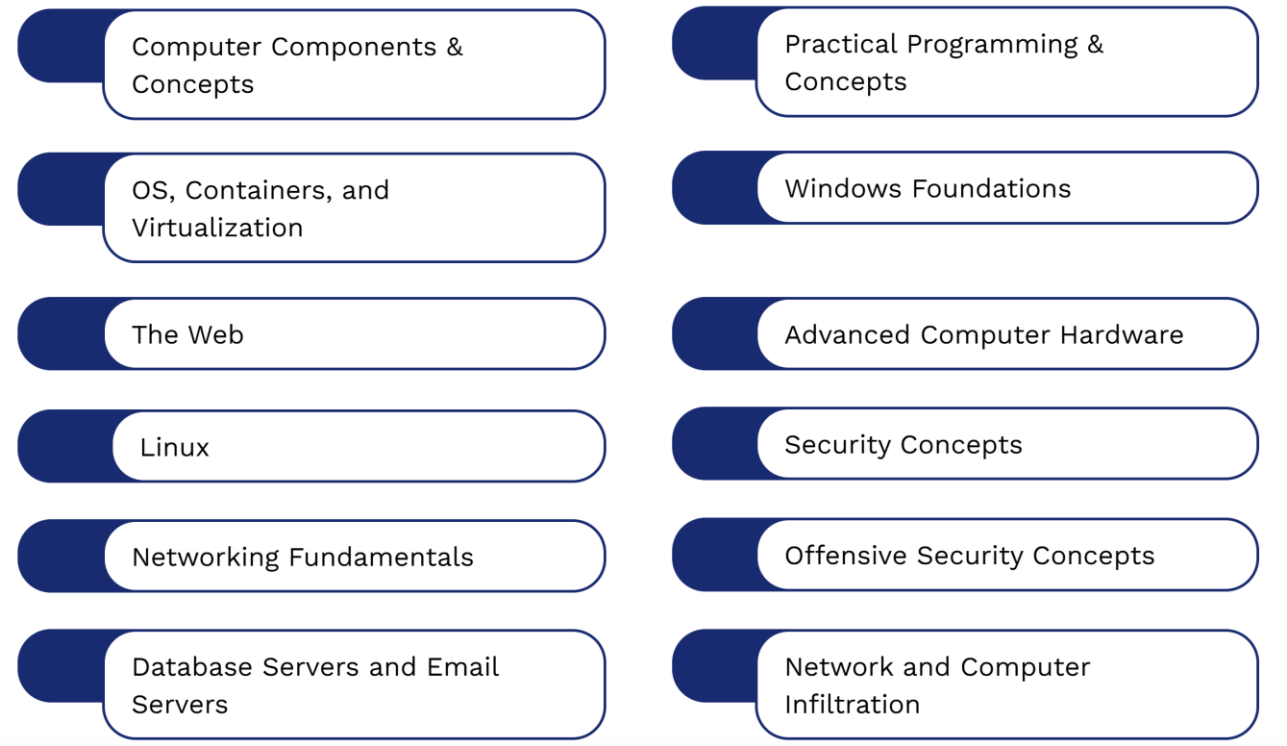


Рис. 2.8. Основні теми курсу «Re/start in Cyber»

Учасники програми, які успішно пройдуть навчання, зможуть отримати престижний сертифікат GIAC Foundational Cybersecurity Technologies (GFACT), який визнається у всьому світі [23].

*Сертифікаційні програми для фахівців з кібербезпеки.* Дослідження українського ринку міжнародних сертифікаційних програм з кібербезпеки показало, що найбільш відомими та затребуваними є кваліфікаційні програми

CISSP від (ISC)2; CISA та CISM від ISACA та різноманітні сертифікати від CompTIA. Крім цього, вітчизняні кіберфахівці можуть пройти навчання й отримати міжнародні сертифікати від інших експертних організацій, таких як SANS, ITIL, а також розробників програмного та апаратного забезпечення (Cisco, Microsoft, Oracle, IBM).

Навчання за міжнародними програмами сертифікації від (ISC)2, ISACA, CompTIA та EC-Council в Україні проводять компанії - авторизовані провайдери послуг:

– Навчальний центр ISSP (CISSP, CISA, 9 сертифікатів CompTIA, включаючи Security+ та CySA+, 8 сертифікатів EC-Council, включаючи SEN, CPENT, CND, ESIN). Навчальний центр ISSP також розробляє індивідуальні курси з інформаційної безпеки, попередньо узгодивши з клієнтом завдання та очікувані результати навчання;

– Kyiv Chapter of ISACA (CISM, CISA, CGEIT and CRISC);

– Fast Lane Group (CISSP, 6 EC-Council certifications, including CEH, CND, CTIA, CHFI, ECIH, CPENT, CompTIA Security+);

– Price Waterhouse Coopers (PwC) Ukraine (CISM, CISA) [24].

Загальний перелік міжнародних сертифікатів для фахівців з кібербезпеки, які можна отримати в Україні, показано на рис. 2.9.

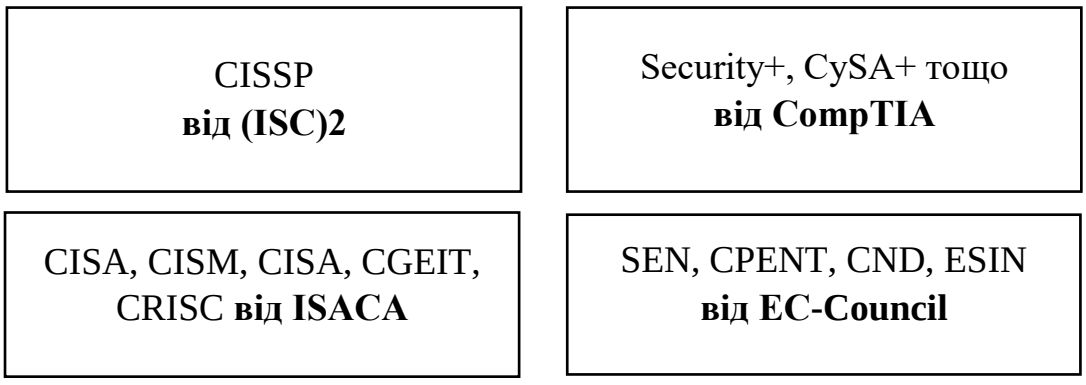


Рис. 2.9. Основні професійні сертифікації з кібербезпеки в Україні

Слід зазначити, що офіси всіх цих організацій розташовані в Києві. PwC в Україні має філії у Львові та Дніпрі. Загалом діяльність організацій та навчальних центрів з сертифікації фахівців у сфері кібербезпеки спрямована на

формування «нового класу» спеціалістів, які володітимуть унікальними навичками і забезпечать конкурентоспроможність своїх компаній не лише на внутрішньому, а й на міжнародному ринках.

### 2.3 Виклики й обмеження в розвитку робочої сили з кібербезпеки в Україні

Попри те, що заклади вищої освіти і компанії-представники галузі пристосовуються до викликів і загроз цифрового середовища, серед основних проблем відзначено нестачу кваліфікованих спеціалістів.

Боротьба за таланти триває у всіх галузях, однак у галузі кібербезпеки ситуація ускладняється ще й тим, що рівень кіберзагроз, як в Україні, так і у світі загалом, щороку лише зростає. Згідно із дослідженнями Global Cybersecurity Outlook 2023, 43% бізнес-лідерів вважають, що у найближчі два роки їхня організація стане жертвою кібератаки [25]. Як наслідок, вони готові виділяти більше ресурсів та залучати більше спеціалістів для протидії кібервикликам.

Огляд статистичних даних і наукових публікацій показав, що точних оцінок щодо дефіциту кіберфахівців в Україні немає, однак, за оцінками ISSP, пропозиція кваліфікованих кадрів на внутрішньому ринку за останній рік суттєво знизилася [26].

На зміни ринку праці у галузі кібербезпеки в Україні впливають як висвітлені вище загальносвітові тренди, так і фактори, пов’язані з війною, зокрема участь кіберфахівців у військовому протистоянні, служба в ЗСУ та підрозділах територіальної оборони. Отже, число наявних професіоналів на ринку суттєво зменшилося. Посилює дефіцит кадрів і міграція (як внутрішня, так і транскордонна). Крім кількісного існує ще й якісний (компетентнісний) вимір робочої сили з кібербезпеки: з огляду на пандемію COVID-19 і тривалі військові дії, внаслідок яких нормальний навчальний процес був порушений, якість підготовки кадрів вищими навчальними закладами викликає низку нарікань.

Водночас, потужним чинником формування дефіциту кваліфікованих кадрів з кібербезпеки є відтік кваліфікованих кадрів за кордон ("Brain Drain"), який не тільки не втратив свою критичність, набуває нових рис через вплив геополітичних факторів і загальних трендів на світовому ринку праці. Основні причини трудової міграції фахівців з кібербезпеки представлені на рисунку 2.10


Рис. 2.10. Причини міграції фахівців з кібербезпеки

Однією з основних причин є значна різниця у розмірах заробітної плати між Україною та економічно розвиненими країнами Європи, Північної Америки та Азії. Пропозиції від міжнародних компаній нерідко містять не лише вищу базову ставку, а й розширений соціальний пакет, бонуси та опції, що робить їх фінансово привабливішими. Робота в міжнародних компаніях відкриває широкі кар'єрні можливості та забезпечує визнання професійних досягнень на глобальному рівні. Участь у великих міжнародних проєктах підвищує вартість фахівця на ринку праці в майбутньому.

Зарубіжні компанії часто пропонують більш сучасне обладнання, доступ до передових технологій, гнучкий графік роботи і розвинену корпоративну культуру. Робота в таких умовах дає змогу фахівцям бути в курсі останніх тенденцій, розвивати нові навички і брати участь у розробці інноваційних рішень. Крім цього, вони забезпечують ширші можливості для професійного зростання, включаючи участь у міжнародних проєктах, конференціях, програмах навчальних і сертифікаційних програмах.

Впливовим чинником виїзду кіберфахівців за межі України є нестабільна економічна та політична обстановка в Україні, особливо в умовах триваючої

війни, спонукає багатьох фахівців шукати більш стабільне та безпечне середовище для себе та своїх родин [26].

Таким чином, відтік кваліфікованих кадрів має безпосередній негативний вплив на рівень кібербезпеки країни. Втрата досвідчених фахівців загострює вже наявний дефіцит досвідчених кадрів на внутрішньому ринку праці, що ускладнює формування команд кібербезпеки в державних установах, приватних компаніях та організаціях критичної інфраструктури. Нестача кваліфікованих спеціалістів може призвести до зменшення рівня експертизи та якості розробки, впровадження та підтримки систем кібербезпеки, роблячи країну вразливішою до кібератак, а також уповільнити процес виявлення, аналізу та ліквідації наслідків кіберінцидентів, збільшуючи потенційні збитки (Рис. 2.11).

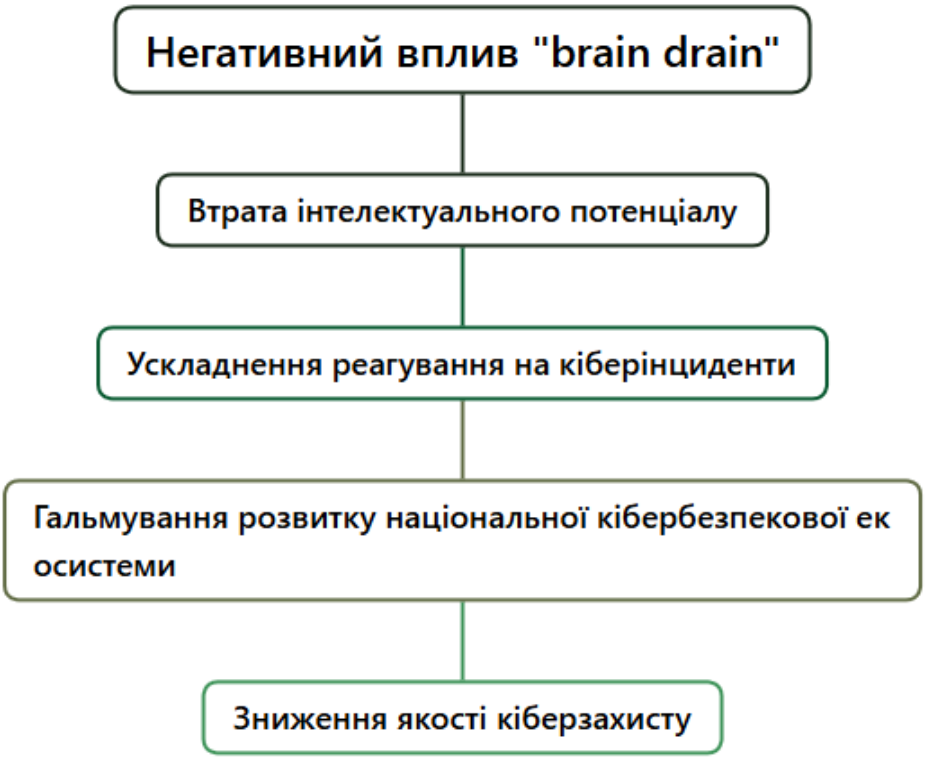


Рис. 2.11. Негативний вплив витоку кадрів

Відтік талановитих фахівців має наслідком призупинення розвитку вітчизняних кібербезпекових стартапів, наукових досліджень та інновацій у цій сфері, а держава втрачає цінний інтелектуальний потенціал та досвід, які могли б бути використані для посилення національної кібербезпеки та розвитку технологічного сектору.

Сьогодні проблема виток кадрів у сфері кібербезпеки може навіть посилитися через бажання фахівців знайти безпечніші умови та більш стабільні перспективи за кордоном. Це потребує від держави та приватного сектору активних дій з метою створення привабливих умов праці, підтримки професійного розвитку та підвищення престижу професії кіберфахівця в Україні.

### 2.4 Невідповідність кваліфікації кіберфахівців вимогам галузі

Стрімкий розвиток кіберзагроз, поява нових технологій атак і еволюція методів захисту створюють постійну потребу в актуалізації знань і навичок фахівців з кібербезпеки.

Слід відзначити, що на сьогодні поняття «фахівець з кібербезпеки» як назва посади ще не визначене. Цей термін застосовується до набору навичок, які використовують різні фахівці з кібербезпеки для запобігання кібератакам і пом'якшення наслідків витоку даних. Деякі з цих ролей включають, але не обмежуються адміністратором безпеки, системним адміністратором і аналітиком безпеки.

Фахівці з кібербезпеки - це IT-фахівці, які відповідають за захист даних і всієї IT-інфраструктури організацій. Вони є експертами у виявленні кіберзагроз та впровадженні заходів безпеки для збереження даних. Ці фахівці також створюють і впроваджують політики безпеки, проводять аналіз загроз і ризиків та здійснюють оцінку вразливостей.

Спеціаліст з кібербезпеки мають уміти виявляти підозрілі шаблони в комп'ютерних системах, стежити за всіма аспектами комп'ютерної інфраструктури на предмет загрозливої діяльності, створювати, встановлювати і використовувати різноманітні інструменти кібербезпеки, розробляти і впроваджувати стандарти безпеки.

Крім того, фахівці з кібербезпеки забезпечують мережеву безпеку, вживаючи заходів для блокування несанкціонованого доступу до комп'ютерної

мережі, проводять діагностику будь-яких змін, що відбуваються в IT-інфраструктурі.

У минулому більшість фахівців з кібербезпеки потребували вищої освіти, враховуючи принцип: чим вища посада фахівця з кібербезпеки, тим суворішими є вимоги до кваліфікації. Хоча це правило не є жорстким, воно досить поширене. Згідно з даними Cybersecurity Guide, 58% фахівців з кібербезпеки мають ступінь бакалавра, 23% - ступінь молодшого спеціаліста і 19% - ступінь магістра [27].

Однак роботодавці дедалі більше усвідомлюють переваги ширшого та інклюзивного кадрового резерву, який включає альтернативні шляхи працевлаштування в технологічній сфері. Так, сьогодні традиційна чотирирічна вища освіта не є обов’язковою. Замість диплому (або на додаток до нього) кваліфікувати IT-фахівця для роботи на посаді спеціаліста з кібербезпеки допомагають сертифікати з кібербезпеки або членство в професійних спільнотах фахівців з кібербезпеки, які нерідко дають конкурентну перевагу перед колегами.

**Вимоги до навичок і практичного досвіду у кібербезпеці.** Навички, необхідні фахівцю з кібербезпеки, можуть відрізнятися залежно від ролі, на яку претендує кандидат. Більшість фахівців з кібербезпеки потребують набору компетентностей, пов'язаних з управлінням ризиками та їх пом'якшенням, знанням мов програмування, операційних систем, комп'ютерних мереж, хмарною безпекою, реагуванням на інциденти, тестуванням на проникнення, пошуком, аналізом та реагуванням на загрози, етичним хакінгом, захистом інформації, оцінюванням вразливостей, виявленням і усуненням шкідливого програмного забезпечення, криптографією, застосуванням методів ШІ та МН, управлінням проєктами [28] (Рис. 2.12).

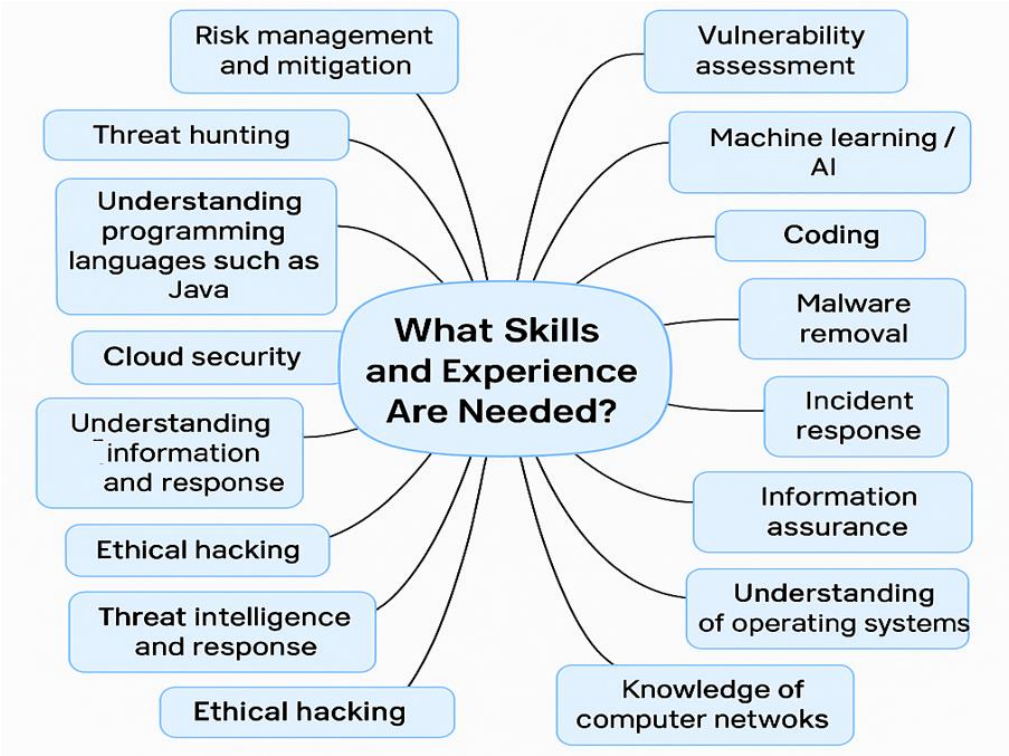


Рис. 2.12. Компетентності фахівця з кібербезпеки

На думку експертів [29], спеціалісти з кібербезпеки мають володіти знаннями й навичками за такими напрямами:

- комп'ютерна криміналістика: знання методів виявленні й розслідування комп'ютерних злочинів, збирання доказів і представлення їх у суді;
- нормативно-правова база: знання законів, стандартів, нормативних актів для дотримання встановлених норм, наприклад щодо захисту персональних даних, інформування керівництва, взаємодії з регуляторними органами;
- кіберконтррозвідка: виявлення й запобігання кібершпигунству з метою захисту конфіденційної інформацію;
- кіберінфраструктура: знання принципів і кращих практик розгортання й захисту кіберінфраструктури, безпечного з'єднання з Інтернетом тощо.
- державна політика у сфері кібербезпеки**:** знання особливостей і тенденцій національної політики в галузі кібербезпеки, участь у формування культури кібербезпеки.

Важливими також є м'які навички, такі як лідерство, робота в команді, комунікабельність і адаптивність, уважність до деталей і творчий підхід до

вирішення проблем. Ці професійні навички допомагають фахівцям з кібербезпеки запобігати порушенням безпеки та пом'якшувати їх наслідки, ефективно керуючи командами кібербезпеки та захищаючи IT-інфраструктуру. Крім того, для фахівців з кібербезпеки дуже важливими є хороші комунікативні навички.

Більшість посадових інструкцій спеціалістів з кібербезпеки вимагають від кандидата кількарічного досвіду роботи на посаді, пов'язаній із захистом даних. Ці IT-фахівці часто набувають і відточують навички кібербезпеки, отримуючи практичний досвід на робочому місці протягом певного періоду часу.

**Перспективи працевлаштування і зарплати фахівців з кібербезпеки.** Побудова кар'єри фахівця з кібербезпеки є перспективною, оскільки потреба в спеціалістах з кібербезпеки буде продовжувати зростати, досягнувши близько позначки у 234 тис. до 2033 року. За даними Бюро статистики праці США (BLS), CompTIA State of the Tech Workforce 2023 та Lightcast, прогнозоване зростання кількості фахівців з кібербезпеки на 10 років на 242% перевищує загальнонаціональний показник.

За даними Cyberseek, середня оголошена заробітна плата фахівця з кібербезпеки становить $124 910 доларів на рік [30].

Таблиця 2.2.

Вимоги і перспективи працевлаштування спеціаліста з кібербезпеки

| | |
|---|---|
| Середня зарплата у 2024 році | 124900 доларів США на рік |
| Типова освіта початкового рівня | Ступінь бакалавра |
| Досвід роботи за суміжною професією | Менше 5 років |
| Кількість робочих місць | 180700 |
| Перспективи працевлаштування | 33% (значно швидше, ніж у середньому) |
| Зміна зайнятості | 59100 |

Відносно швидко стати фахівцем з кібербезпеки можуть IT-фахівці, які мають ступінь бакалавра в галузі, пов'язаній з комп'ютерними технологіями; принаймні кілька років досвіду роботи, пов'язаної з кібербезпекою; базові сертифікати з кібербезпеки (Рис. 2.13)

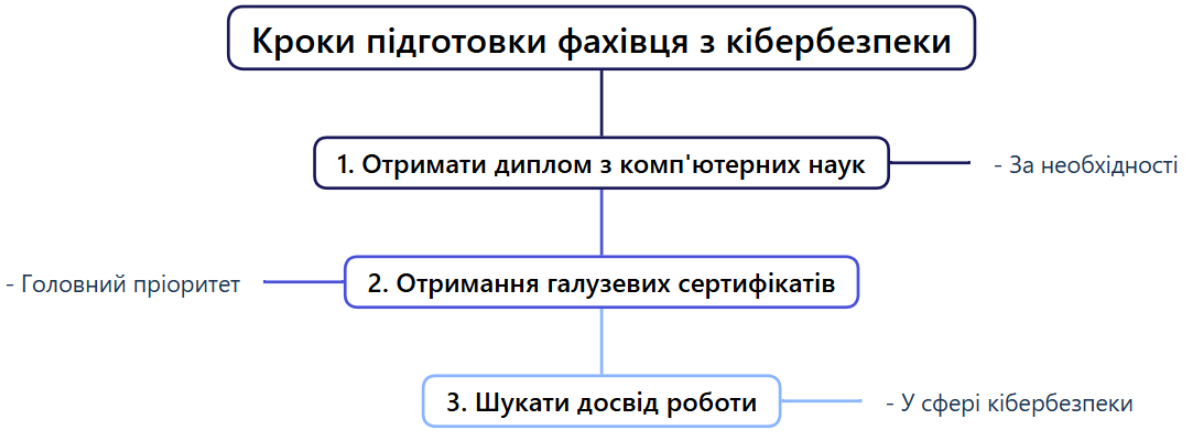


Рис. 2.13. Кроки підготовки фахівця з кібербезпеки

Отже, як бачимо, у світовій практиці вже чітко встановлені вимоги до професіонала з кібербезпеки. Вимоги щодо компетенцій випускників вітчизняних освітніх програм з кібербезпеки зібрані у стандарті вищої освіти за спеціальністю 125 «Кібербезпека».

Однак, в Україні спостерігається значна невідповідність кваліфікації існуючих фахівців актуальним вимогам ринку праці, що є серйозним викликом для забезпечення ефективного кіберзахисту на всіх рівнях.

**Відставання процесів підвищення кваліфікації та перекваліфікації кадрів**. У сфері кібербезпеки знання та навички швидко застарівають. Зловмисники постійно розробляють нові вектори атак, використовують складніші методи проникнення та експлуатації вразливостей. З огляду на це, системне підвищення кваліфікації та перекваліфікація кадрів є абсолютною необхідністю для підтримки їхньої компетентності на належному рівні. Фахівці повинні безперервно навчатися, освоювати нові інструменти і технології, розуміти останні тенденції у світі кіберзагроз та методи протидії їм. Це включає вивчення нових видів шкідливого ПЗ, методів соціальної інженерії, аналізу безпеки, хмарних технологій, захисту критичної інфраструктури тощо.

**Дефіцит практично-орієнтованих курсів.** Більшість навчальних програм у вишах і комерційних курсів зосереджені на теоретичних аспектах забезпечення кібербезпеки, у той час, як роботодавці очікують від своїх потенційних працівників володіння практичними навичками, наприклад, роботи з SIEM-системами або реагування на інциденти.

**Недостатня кількість україномовних навчальних матеріалів.** Значна частина передових навчальних матеріалів і курсів доступна переважно англійською мовою, що може створювати бар'єри для деяких фахівців.

**Складність поєднання навчання з роботою.** Фахівцям часто важко знайти час і ресурси для проходження тривалих навчальних курсів, особливо при високій завантаженості на робочому місці. На противагу працюючим спеціалістам, студентам важко отримати перше робоче місце через брак практичного досвіду.

**Висока вартість сертифікаційних програм**. Міжнародні сертифікати (наприклад, OSCP або CISSP) коштують від 500$, що робить їх недоступними для багатьох спеціалістів. За даними опитування Lviv IT Cluster (2024) [31], лише 12% фахівців з кібербезпеки в Україні мають хоча б один міжнародний сертифікат.

## Висновки до розділу 2

За результатами комплексного аналізу поточного стану вітчизняного ринку праці в галузі кібербезпеки встановлено, що ринок значно зріс упродовж останніх років, що зумовлено активною цифровізацією та збільшенням кількості кіберзагроз. Прогнози свідчать про подальше зростання обсягів ринку. Значний вплив на його розвиток справили пандемія COVID-19, військові дії і гострий дефіцит кваліфікованих фахівців.

Як показало дослідження, структура попиту має свої особливості, зокрема акцент робиться на впровадженні автоматизованих кіберрішень у зв’язку з браком кадрів. Ключовими рушійними факторами розвитку є цифровізація, зростання кіберзлочинності, інновації, підтримка донорських організацій і застосування ШІ. Висока динаміка ринку і здатність адаптуватися до викликів воєнного часу стимулюють розвиток інноваційних технологій і автоматизованих систем захисту.

Аналіз стану підготовки та підвищення кваліфікації фахівців з кібербезпеки в Україні засвідчив активну участь понад 60 закладів вищої освіти, які пропонують освітні програми, адаптовані до міжнародних стандартів, з тісною співпрацею з IT-компаніями та державними структурами. Серед актуальних тенденцій відзначено посилення попиту на практично орієнтовану освіту, вирішення проблем нестачі кадрів через інтеграцію практичних заходів, таких як корпоративні програми навчання й підвищення кваліфікації, кіберзмагання, стажування тощо.

Виявлено, що одним із головних викликів розвитку робочої сили у сфері кібербезпеки є суттєвий дефіцит кваліфікованих спеціалістів, який поглиблюється глобальними тенденціями, впливом війни, міграцією кадрів і порушенням освітнього процесу. Основними причинами відтоку фахівців є низький рівень заробітної плати, незадовільні умови праці, нестабільність і обмежені можливості професійного зростання в Україні. Втрата кваліфікованої робочої сили негативно впливає на рівень кібербезпеки, ускладнює реагування на інциденти та стримує розвиток національної кіберекосистеми. Водночас наголошено на необхідності впровадження активних заходів для покращення умов праці, підтримки фахівців і підвищення престижу професії за участі держави і приватного сектору.

Дослідження показало, що кваліфікація українських фахівців з кібербезпеки часто не відповідає міжнародним вимогам до знань, навичок і сертифікацій, необхідних для ефективної професійної діяльності. Встановлено, що причинами такої ситуації є, зокрема, недостатня кількість і висока вартість практично-орієнтованих курсів і міжнародних професійних сертифікацій, складнощі поєднання навчання з роботою, брак україномовних навчальних матеріалів.

# РОЗДІЛ 3. СУЧАСНІ МЕТОДИ РОЗВИТКУ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ КАДРІВ З КІБЕРБЕЗПЕКИ

У контексті стрімкого розвитку цифрових технологій, динамічного ускладнення кіберзагроз та глобальної цифрової трансформації, забезпечення висококваліфікованих кадрів у сфері кібербезпеки стає одним із ключових завдань державної та корпоративної політики. Традиційні підходи до професійного навчання більше не задовольняють потреби галузі, оскільки не встигають за темпами змін, що відбуваються в інформаційному середовищі. Саме тому сучасна система підготовки кадрів повинна орієнтуватися на гнучкість, практичну спрямованість, міждисциплінарність та безперервний розвиток.

## 3.1 Інструменти неформальної та практичної освіти для кіберфахівців

Як показало дослідження, основними засобами реалізації неформальної та практичної освіти для спеціалістів галузі кібербезпеки є масові відкриті онлайн-курси (MOOC) та освітні платформи, практичні тренажери, віртуальні лабораторії, навчальні полігони та CTF-змагання з кібербезпеки (Рис. 3.1):


Рис. 3.1. Інструменти неформальної та практичної освіти з кібербезпеки

**Масові відкриті онлайн-курси та освітні платформи.** Масові відкриті онлайн-курси (MOOC, Massive Open Online Courses) – це безкоштовні навчальні курси, викладені для загального доступу в Інтернет. Такі курси є чудовим інструментом для поширення якісних знань від найкращих викладачів.

Вони є однією з найновіших форм дистанційного навчання, яка активно розвивається у світовій освіті. Курси зазвичай розраховані на студентів різних попередніх рівнів підготовки: як новачків, так і досвідчених фахівців.

Серед найбільш визнаних і поширених платформ можна виділити Coursera, edX, Udemy, Cybrary та FutureLearn.

*Coursera* є однією з провідних світових платформ масових відкритих онлайн-курсів (MOOC), яка співпрацює з понад 200 провідними університетами та компаніями, такими як Stanford University, Google та IBM. Вона пропонує широкий спектр курсів, спеціалізацій, професійних сертифікатів і навіть онлайн-ступенів, що робить її цінним ресурсом для кіберспеціалістів на будь-якому етапі кар'єри. Станом на червень 2025 року Coursera пропонує понад 10 курсів за напрямом «Кібербезпека», серед яких курси з основ кібербезпеки, аналітики кібербезпеки від IBM і Microsoft, хмарної безпеки, архітектури безпеки й автоматизації в кібербезпеці [32].

Ключовими перевагами платформи Coursera для кіберспеціалістів є: висока якість контенту, оскільки курси розроблені провідними університетами та лідерами галузі, що забезпечує актуальність та глибину матеріалів; структуровані програми, які складаються з кількох курсів, що забезпечують комплексний підхід до вивчення обраної спеціалізації; практична спрямованість: багато програм включають практичні завдання, проєкти та віртуальні лабораторії; гнучкість навчання, адже платформа надає кожному студенту можливість навчатися у власному темпі, з будь-якого місця та в будь-який час; верифіковані сертифікати, які високо цінуються роботодавцями.

*edX* - це некомерційна онлайн-платформа, заснована Гарвардським університетом та Массачусетським технологічним інститутом, що є однією з найавторитетніших освітніх платформ у світі. Вона вирізняється своїм фокусом на академічну якість, пропонуючи курси, професійні сертифікати, програми MicroMasters і навіть повноцінні онлайн-ступені від провідних світових університетів та освітніх установ. Це робить edX надзвичайно цінним ресурсом

для кіберспеціалістів, які прагнуть здобути глибокі теоретичні знання, доповнені практичними навичками.

Характеризуючи переваги edX для кібербезпеки, слід відзначити високий академічний рівень програм, які розробляються провідними університетами, що гарантує ґрунтовні знання та відповідність міжнародним стандартам; різноманіття форматів, які варіюються від окремих курсів до комплексних програм MicroMasters, які можуть зараховуватися як частина магістерських програм; гнучкість навчання, що проявляється в можливостях навчання за індивідуальним графіком і темпом. Крім цього, професійні сертифікати та MicroMasters програми від edX визнаються роботодавцями та можуть прискорити кар'єрне зростання або стати кроком до вищої освіти.

Як і Coursera, edX надає можливість отримання професійних сертифікатів, серед яких велика кількість курсів від відомих компаній, таких як IBM, Google, AWS, а також вендоронезалежних сертифікацій, зокрема Cybersecurity Essentials від EC-Council [33].

*FutureLearn* – це британська онлайн-платформа, яка відрізняється своїм акцентом на "соціальне навчання" та співпрацею з провідними університетами Великої Британії та світу, а також культурними установами. Вона пропонує курси, програми Micro-credentials (коротші, сфокусовані програми), ExpertTracks (навчальні шляхи з кількох курсів) та онлайн-ступені. Для фахівців з кібербезпеки FutureLearn є джерелом якісного академічного контенту, часто з унікальним британським поглядом на проблематику.

FutureLearn має низку переваг для фахівців з кібербезпеки, зокрема платформа забезпечує академічну строгість навчання завдяки тому, що курси розроблені авторитетними університетами, які гарантують глибокий і перевірений контент, надає так зване соціальне навчання, тобто сприяє взаємодії між студентами через обговорення та коментарі, створюючи спільноту навчання. Окрім переліченого FutureLearn пропонує різноманіття освітніх рівнів: від початкових курсів для широкої аудиторії до спеціалізованих програм і навіть магістерських ступенів, робить акцент на відповідність стандартам, зокрема

деякі курси мають акредитацію від визнаних органів, наприклад, NCSC (National Cyber Security Centre) Великої Британії.

Цікавим прикладом курсів, представлених на платформі, є так званий ExpertTrack - поглиблений онлайн-курс, створений, щоб допомогти студентам оволодіти новими навичками, які можна застосувати у своїй професійній кар'єрі. У галузі кібербезпеки студенти можуть пройти, зокрема, ExpertTrack "Цифрова безпека: Кіберзагрози та управління ризиками" (Digital Security Training: Cyber Threats and Risk Management). Цей курс складається з кількох курсів, що занурюють у більш глибокі аспекти цифрової безпеки та управління ризиками, і розглядає тактики соціальної інженерії (фішинг, смішинг, вішинг), різні типи кібератак (шкідливе ПЗ, ransomware) та рішення для захисту пристроїв. Також перевагами даного курсу є комплексний підхід до управління ризиками та розробки стратегій захисту. Підходить для тих, хто прагне розвивати не лише технічні, а й управлінські навички у кібербезпеці [34].

Аналіз провідних онлайн-освітніх платформ, таких як Coursera, edX і FutureLearn, демонструє їхню ключову роль у сучасному розвитку та підвищенні кваліфікації кадрів у галузі кібербезпеки. Ці платформи кардинально змінили ландшафт професійної освіти, зробивши високоякісні знання доступними для широкого кола фахівців, що є критично важливим в умовах динамічних кіберзагроз.

Слід відзначити, що в Україні також є подібні освітні платформи, зокрема, найбільша вітчизняна онлайн-платформа професійного розвитку в Україні Prometheus, яка була заснована у 2014 році [35]. На Prometheus представлені різноманітні курси і професійні програми, в тому числа в галузі IT, кібербезпеки, новітніх технологій.

**Практичні тренажери й навчальні полігони та CTF-змагання з кібербезпеки.** Успіх фахівця з кібербезпеки визначається не лише обсягом теоретичних знань, але й, що найважливіше, здатністю застосовувати їх на практиці. Традиційні методи навчання часто не можуть повною мірою відтворити реальні умови кібератак та захисту. Саме тому практичні тренажери,

навчальні полігони (Cyber Ranges) та змагання Capture The Flag (CTF) стали невід'ємними компонентами сучасної неформальної освіти та підвищення кваліфікації з кібербезпеки. Вони надають безпечне, контрольоване середовище для відпрацювання навичок, моделювання реальних сценаріїв та розвитку критичного мислення в умовах, максимально наближених до реальних.

*Практичні тренажери та віртуальні лабораторії (Virtual Labs)* – це програмні або хмарні середовища, які емулюють або симулюють реальні мережеві інфраструктури, операційні системи, додатки та пристрої. Їхня основна мета – надати кіберфахівцям (від початківців до досвідчених) можливість безпечно експериментувати, відпрацьовувати навички, тестувати інструменти і досліджувати вразливості без ризику пошкодити діючі виробничі системи.

На початковому етапі віртуальні лабораторії є ідеальним майданчиком для освоєння фундаментальних навичок. Тут можна практикувати налаштування мережевих пристроїв, таких як маршрутизатори, комутатори, фаєрволи, навчатися адмініструванню операційних систем (Linux, Windows Server) з точки зору безпеки, а також вдосконалювати роботу з командним рядком і глибоко зрозуміти основи мережевих протоколів.

Основна цінність Virtual Labs проявляється в кількох аспектах, зокрема через можливість імітувати атаки й іншу шкідливу активність і експериментувати з експлойтами в ізольованому середовищі, без ризику для реальних систем. Крім цього віртуальні середовища дозволяють отримати доступ до складної інфраструктури, розгортання якої в реальних умовах було б надто дорогим або трудомістким, а також моделювати типові та нестандартні ситуації, з якими стикаються фахівці з кібербезпеки щодня.

Важливою перевагою віртуальних лабораторій є те, що вони забезпечують інтеграцію багатьох інструментів, надаючи готові середовища з попередньо встановленими і налаштованими інструментами кібербезпеки, забезпечують масштабованість, завдяки чому можна легко створювати і видаляти навчальні середовища за потребою, адаптуючи їх до конкретних навчальних цілей.

На ринку існує безліч платформ, які надають віртуальні лабораторії та тренажери для навчання кібербезпеці. Вони відрізняються рівнем складності, спеціалізацією та форматом доступу.

Однією із провідних хмарних платформ, яка надає реалістичні та вимірювані, симуляційні тренування з кібербезпеки для окремих фахівців та цілих команд, є *RangeForce* [36]. Вона вирізняється своїм фокусом на розвиток практичних навичок захисту (так звана підготовка за напрямом "Blue Team") у середовищах, що максимально імітують реальні корпоративні мережі та інфраструктури, з використанням справжніх інструментів та протидією реальним кібератакам.

RangeForce пропонує комплексний підхід до кібернавчання, поєднуючи реалістичні симуляції з цілеспрямованим розвитком навичок. Платформа прагне надати фахівцям і командам можливість тренуватися в умовах, максимально наближених до реальних кіберзагроз.

RangeForce пропонує два основні взаємодоповнюючі компоненти:

1) Реалістичне симуляційне середовище для індивідуального та командного розвитку: RangeForce емулює справжні IT-інфраструктури, включаючи операційні системи, мережеві пристрої, додатки та реальні інструменти безпеки (наприклад, Splunk, CrowdStrike, Palo Alto Networks, Microsoft Defender). Цей підхід критично важливий для формування "м'язової пам'яті" та впевненості у використанні цих засобів у реальних умовах. Симуляції відтворюють актуальні кіберзагрози й атаки (програми-вимагачі, фішинг, DDoS, просування в мережі та інші тактики, техніки і процедури зловмисників), дозволяючи фахівцям відточувати навички реагування.

2) Розширені можливості навчання для різних потреб: Платформа розділена на дві ключові складові, що відповідають різним сценаріям навчання:

-*RangeForce Battle Skills* є програмою самостійного навчання, яка включає сотні інтерактивних модулів. Вона дозволяє індивідуальним користувачам безперервно розвивати свої навички, виявляти прогалини у знаннях та рухатися за персоналізованими навчальними планами..

*-RangeForce Battle Fortress (або Cloud Range / Drills)* – це хмарний кіберполігон, призначений для командних тренувань. Він дозволяє швидко запускати повномасштабні симуляції кібератак у реальному часі. Команди мають змогу відпрацьовувати злагодженість дій, комунікацію, пріоритезацію і лідерство під час симуляції реальних інцидентів, протидіючи динамічним супротивникам.

Цей двокомпонентний підхід дозволяє RangeForce ефективно покривати потреби як індивідуального, так і командного навчання, забезпечуючи глибоке занурення в практичні аспекти кібербезпеки.

*CTF-змагання (Capture The Flag)* - це ігровий формат змагань, де учасники (індивідуально або в командах) вирішують серію завдань, щоб знайти приховані "прапори". Прапори – це зазвичай рядки тексту або коду, які підтверджують успішне виконання завдання. CTF-змагання є одним з найефективніших способів відточити практичні навички, розвинути креативне і критичне мислення, а також навчитися працювати під тиском в умовах, максимально наближених до реальних кіберінцидентів.

Такі змагання можуть здатися грою, але насправді вони є важливим полігоном для відточування майстерності у сфері кібербезпеки. Вміння, отримані на CTF в контрольованому середовищі, зокрема аналіз мережі, обернене проектування, прикладна криптографія, безпека веб-застосунків, цифрова криміналістика тощо, необхідні для захисту від реальних кібератак [37].

Мета змагань CTF із захоплення прапора - знайти та вилучити необхідну інформацію або дані в емульованому середовищі. Водночас, для учасників змагання CTF є потужним способом привернути увагу потенційних роботодавців. На відміну від традиційного процесу працевлаштування, коли резюме відбирають у відділі кадрів, перш ніж передати їх відповідному відділу, на змаганнях CTF учасники часто спілкуються безпосередньо з потенційним працедавцем, який також може брати участь у цьому змаганні. Отже, змагання CTF відіграють важливу роль не тільки в підготовці, але й пошуку кваліфікованих кіберфахівців.

Щоб взяти участь у CTF або знайти матеріали для навчання, існують численні ресурси, наприклад *PicoCTF* - одне з найбільших безкоштовних онлайн-змагань, започатковане Університетом Карнегі-Меллон. Воно ідеально підходить для початківців, оскільки завдання поступово ускладнюються і часто супроводжуються навчальними матеріалами [38].

## 3.2 Професійні спільноти, науково-практичні заходи і менторські програми

Окрім формального навчання і практичних тренажерів, надзвичайно важливу роль у розвитку та підвищенні кваліфікації кадрів у сфері кібербезпеки відіграють професійні спільноти, галузеві заходи й менторські програми. Вони створюють екосистему для безперервного обміну знаннями, нетворкінгу, наставництва та підтримки, що є критично важливим в умовах постійно мінливого ландшафту кіберзагроз та технологій.

**Професійні спільноти**. Це групи фахівців, об'єднаних спільними інтересами, цілями або професією. У кібербезпеці вони є життєво важливим джерелом актуальної інформації, підтримки і можливостей для співпраці. Їхнє основне призначення полягає в безперервному обміні знаннями та досвідом, де фахівці обговорюють нові загрози, вразливості, інструменти та методології. Це створює динамічне середовище для колективного навчання й адаптації до швидких змін в індустрії. Паралельно, спільноти є чудовим майданчиком для нетворкінгу, дозволяючи налагоджувати цінні зв'язки з колегами, потенційними роботодавцями та партнерами.

Крім того, вони пропонують практичну допомогу у вирішенні проблем, адже учасники можуть отримати поради від досвідчених фахівців щодо конкретних завдань або інцидентів. Спільноти також активно сприяють кар'єрному розвитку, публікуючи оголошення про вакансії та надаючи рекомендації щодо навчання та сертифікацій, що є особливо цінним для тих, хто шукає нові можливості або прагне підвищити свою кваліфікацію.

У таблиці 3.1 представлені короткі відомості про найбільш відомі міжнародні організації в галузі кібербезпеки.

*Відкритий проект безпеки веб-застосунків (OWASP)* - це некомерційний фонд, який надає рекомендації щодо розробки, придбання та обслуговування надійних і безпечних програмних застосунків [39].

OWASP відомий своїм популярним списком 10 найбільших вразливостей безпеки веб-додатків, який базується на консенсусі спільноти розробників щодо головних ризиків безпеки і оновлюється кожні кілька років з огляду на зміни ландшафту кіберзагроз. У списку пояснюються найнебезпечніші недоліки безпеки веб-застосунків і надаються рекомендації щодо їх усунення.

Таблиця 3.1.

Міжнародні організації в галузі кібербезпеки

| Назва | Опис | Активності |
|---|---|---|
| OWASP | Спільнота з веб-безпеки | - Локальні chapter-групи<br>- Дослідження вразливостей (Top 10)<br>- Воркшопи, CTF |
| ISACA | Асоціація з кібербезпеки та аудиту | - професійні сертифікації (CISA, CISM)<br>- конференції |
| SANS Institute | Лідер у кібербезпековій освіті | - цифрова криміналістика, пентест-тренінги<br>- ініціативи з кібербзахисту |
| Black Hat / Def Con | Всесвітні хакерські конференції | - виступи експертів<br>- воркшопи із застосування експлойтів |

OWASP прагне навчати розробників, дизайнерів, архітекторів та власників бізнесу ризикам, пов'язаним з найпоширенішими вразливостями безпеки веб-додатків. Фонд підтримує як продукти з відкритим кодом, так і комерційні продукти безпеки. Він відомий як форум, на якому експерти з безпеки та фахівці з інформаційних технологій можуть спілкуватися та набувати досвіду.

*ISACA (Information Systems Audit and Control Association)* – це глобальна асоціація для фахівців з аудиту, контролю, управління ризиками та безпеки інформаційних систем. Своєю місією організація бачить розширення можливостей своїх членів протягом їхньої кар'єри шляхом надання всебічних знань, навичок, повноважень і доступу до глобальної спільноти, забезпечення якісної підготовки до вирішення сучасних викликів і впровадження майбутніх інновацій [40].

Досягнення місії ISACA забезпечує через надання провідних у галузі сертифікацій, безперервного оновлення навичок і освіти на основі ефективності, розробку і просування дослідницьких ідей, концепцій, стандартів, інструментів, політик, підтримку місцевих відділень і глобальної мережі. Асоціація пропонує для фахівців із кібербезпеки такі всесвітньо визнані професійні сертифікації як CISA (сертифікований аудитор інформаційної безпеки) і CISM (сертифікований менеджер інформаційної безпеки), а також близько десяти інших програм підвищення кваліфікації.

*SANS Institute* – це приватна комерційна компанія США, заснована в 1989 році, яка має на меті надати професіоналам із кібербезпеки практичні навички та знання, необхідні для того, щоб зробити світ безпечнішим [41]. Для цього Інститут проводить високоякісне навчання, видає престижні професійні сертифікати, організовує стажування й академічні програми з отриманням дипломів, створює й надає доступ до фахових інформаційних ресурсів для задоволення потреб кожного кіберпрофесіонала.

Black Hat, заснована в 1997 році, є всесвітньо визнаною серією заходів з кібербезпеки, яка пропонує найбільш технічні та релевантні дослідження з проблем кібербезпеки, найновіших тенденцій, досліджень і розробок в галузі.

Брифінги і тренінги Black Hat ґрунтуються на потребах глобальної спільноти безпеки, яка прагне об'єднати найкращих професіоналів галузі, сприяє кар'єрному просуванню кіберпрофесіоналів на всіх рівнях, заохочує розвиток і співпрацю між академічними колами, дослідниками світового рівня та лідерами

державного і приватного секторів. Сьогодні брифінги та тренінги Black Hat проводяться щорічно в Сполучених Штатах, Європі й Азії [42].

Україна також має приклади впливових спільнот професіоналів з IT і кібербезпеки (Таблиця 3.2).

*IT Асоціація України* (IT Ukraine Association) - найбільше національне об'єднання IT-компаній, яка представляє інтереси понад 100 тисяч IT-спеціалістів; захищає інтереси IT-компаній у сфері оподаткування та юридичних аспектів ведення діяльності; реалізує освітні й соціальні проєкти; забезпечує юридичну та PR-підтримку, обмін досвідом між учасниками і партнерами Асоціації. Асоціація представляє інтереси компаній-учасників у міжнародних індустріальних об'єднаннях та організаціях DIGITALEUROPE, WITSA, EMOTA [43].

Таблиця 3.2.

Українські спільноти фахівців з кібербезпеки

| Назва | Опис | Активності |
|---|---|---|
| IT Асоціація України | об'єднання IT-компаній | - освітні й соціальні проєкти<br>- обмін досвідом |
| Наукова асоціація кібербезпеки України (ISCA) | Спільнота науковців і практиків з кібербезпеки | - дослідження, проєкти<br>- тренінги, конференції, семінари<br>- сертифікація фахівців |
| Kharkiv & Lviv IT Clusters | Регіональні IT-асоціації | - хакатони, тренінги з кібербезпеки |

*Наукова асоціація кібербезпеки України (ISCA)* визначає свою мету як підвищення загального рівня кібербезпеки українського суспільства шляхом створення свідомої спільноти активних науковців та фахівців-практиків; дослідницької, проєктної та аналітичної роботи у галузі кібербезпеки; інноваційної освітньої діяльності в галузі кібербезпеки; організації спеціалізованих тренінгів, наукових конференцій і семінарів з кібербезпеки; сертифікації фахівців за різними напрямками в галузі кібербезпеки [44].

Діяльність *Харківського і Львівського IT кластерів,* які об'єднують передові українські IT-компанії, освітні заклади та представників влад, спрямована на створення сприятливих умов для ведення бізнесу через покращення якості освіти, розвиток талантів, різносторонню підтримку IT-компаній і адвокацію інтересів галузі. Обидві організації прагнуть трансформувати технічну освіту відповідно до запитів галузі й найкращих світових практик, підтримувати реалізацію студентських проєктів і стартапів, організовувати події для професійного зростання тощо.

**Науково-практичні заходи з кібербезпеки.** Аналіз діяльності професійних, освітніх і дослідницьких організацій з кібербезпеки в Україна показав, що основними методами навчання, підвищення кваліфікації й обміну досвідом серед професіоналів з кібербезпеки є науково-практичні заходи і конференції, мітапи та воркшопи з кібербезпеки, практичні тренажери, навчальні кіберполігони та CTF-змагання, а також професійні спільноти, галузеві заходи й менторські програми

*Конференції з кібербезпеки в Україні* - це масштабні зібрання, що об'єднують тисячі фахівців, дослідників, представників компаній, державних органів і академічної спільноти. Вони є головним майданчиком для презентації новітніх досліджень, аналізу глобальних тенденцій та обговорення стратегічних питань кібербезпеки. Однією з таких є щорічний Київський Міжнародний Форум з Кібербезпеки [45].

*Мітапи* (meetups) і *воркшопи* (workshops) є ключовими форматами локальної взаємодії для фахівців з кібербезпеки в Україні. Вони створюють динамічне середовище для обміну знаннями, практичного навчання та нетворкінгу без необхідності участі у великих і дороговартісних конференціях. Ці заходи можуть бути організовані як професійними асоціаціями, так і незалежними спільнотами, університетами або компаніями.

*Мітапи* – це, зазвичай, кількагодинні зустрічі кіберфахівців-однодумців онлайн або безпосередньо у вечірній час або вихідні, що включають короткі доповіді або розгорнуті презентації від місцевих експертів, обговорення.

Тематика охоплює широкий спектр питань: від аналізу нових кіберзагроз і демонстрації інструментів до обговорення регуляторних змін або реальних кейсів. Після офіційної частини часто відбувається неформальне спілкування.

*Воркшопи*, натомість, є більш інтенсивними практичними заняттями, що тривають від кількох годин до повного дня і мають на меті під керівництвом інструктора вдосконалити конкретні практичні навички учасників, наприклад роботу з інструментами (Wireshark, Burp Suite), практику безпечної розробки, проведення розслідування цифрових злочинів чи тестування на проникнення.

Прикладом Воркшопу є “Silverfort & Check Point: контроль доступу та безпека хмар - нова ера кібербезпеки!” від компанії «IT Specialist» [46].

### 3.3 Перспективні напрями розвитку професіоналів з кібербезпеки

Кібербезпека – це галузь, яка ніколи не стоїть на місці. Вона розвивається паралельно з технологічним прогресом та постійною еволюцією кіберзагроз, що робить її однією з найбільш динамічних і складних сфер сьогодення. У цьому контексті, ефективний розвиток кадрів є не просто бажаним, а життєво необхідним для забезпечення національної безпеки, економічної стабільності й захисту критичних інфраструктур.

Розуміння того, які знання, навички та спеціалізації будуть затребувані завтра, дозволяє системно підходити до підготовки фахівців, інвестувати в перспективні освітні програми і сприяти формуванню нової генерації кіберспеціалістів.

Дослідження показало, що найбільш перспективними напрямами розвитку робочої сили з кібербезпеки є спеціалізація кадрів відповідно до нових технологій і загроз; розвиток навичок міжособистісного спілкування й управлінських компетенцій; забезпечення міждисциплінарного характеру освіти в галузі кібербезпеки.

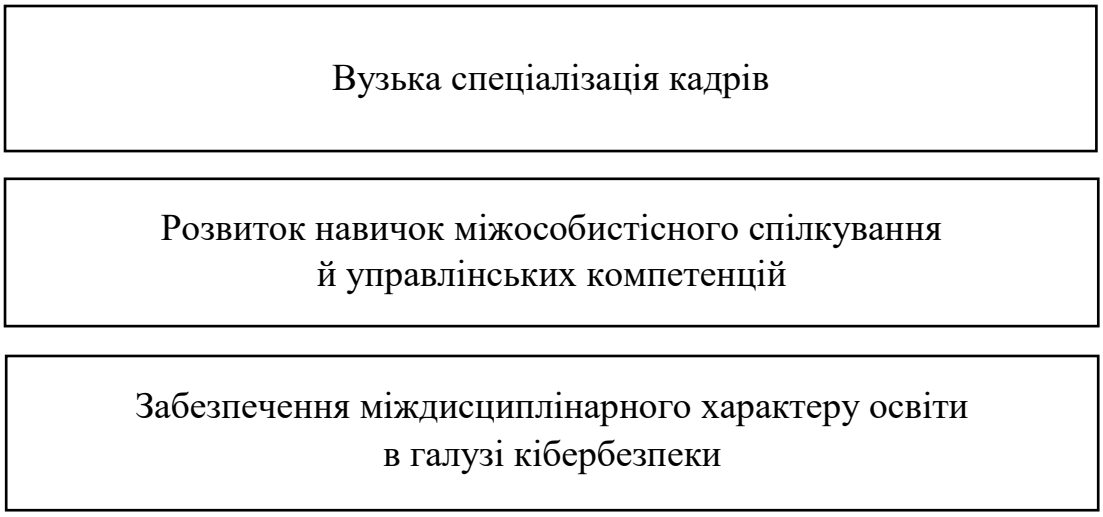


Рис. 3.2. Перспективні напрями розвитку робочої сили з кібербезпеки

**Спеціалізація кадрів відповідно до нових технологій і загроз.** Сучасний ландшафт кібербезпеки характеризується швидким розвитком нових технологій і, відповідно, появою унікальних векторів загроз. Це призводить до зростання потреби не просто у фахівцях загального профілю, а й у вузькопрофільних експертах, чиї компетенції безпосередньо відповідають викликам, що постають перед новими архітектурами і системами. Зі збільшенням складності й масштабу цифрових екосистем, спеціалізація стає не розкішшю, а необхідністю для ефективного захисту.

Зростає попит на фахівців, що володіють глибокими знаннями і практичними навичками за такими ключовими напрямами:

*Штучний інтелект (ШІ) та машинне навчання (МН).* ШІ і МН у сфері кібербезпеки використовує інтелектуальні алгоритми й машинне навчання для покращення виявлення загроз, запобігання та реагування. Він аналізує дані, визначає закономірності та приймає обґрунтовані рішення щодо захисту систем і даних від кіберзагроз. Можливості ШІ є особливо корисними для автоматизації багатьох завдань, таких як аналіз журналів, сканування вразливостей і виявлення загроз, що дозволяє кіберфахівцям зосередитися на складніших питаннях.

ШІ та МН змінюють кібербезпеку у кращий бік, а важливість фахівців зі ШІ та МН неможливо переоцінити. Їхня роль є вирішальною для досягнення таких ключових цілей при застосуванні ШІ та МН, як забезпечення довіри та цілісності даних; запобігання непередбачуваній та небезпечній поведінці

штучних моделей; захист конфіденційності та персональних даних; збереження інтелектуальної власності та конкурентних переваг компаній; інтеграція безпеки на всіх етапах життєвого циклу кібербезпеки; зменшення ризиків кібербезпеки у критичних інфраструктурах.

Таким чином, фахівці з безпеки на основі ШІ та МН є архітекторами довіри в цифрову епоху. Вони гарантують, що ШІ-системи, масштаби застосування яких зростають з величезною швидкістю, є надійними, безпечними і продуктивними, мінімізуючи ризики і максимізуючи користь від інновацій. Їхня роль є незамінною для сталого і безпечного розвитку технологій майбутнього [47].

*Експерти з безпеки хмарних обчислень* – це спеціалісти, які фокусуються на всебічному захисті даних, додатків та інфраструктури, що розміщуються в хмарних середовищах, розв'язуючи проблеми безпеки, які є унікальними для хмарних екосистем.

Експерти хмарних обчислень охоплюють весь життєвий цикл хмарних ресурсів, від проєктування до моніторингу. Першим кроком є проєктування і впровадження надійних хмарних архітектур, визначення оптимальних заходів безпеки для різних сервісів. Фахівці з хмарної безпеки контролюють доступ і конфігурації, налаштовуючи жорсткі політики управління ідентифікацією та доступом (IAM), застосовуючи принцип мінімальних привілеїв. Таким чином, вони протидіють несанкціонованому доступу та помилкам у налаштуваннях, які є одними з найчастіших причин інцидентів.

Важливим завданням спеціалістів з хмарної безпеки є впровадження стратегії шифрування даних, як у стані спокою, так і під час передачі, й управління ключами шифрування з метою запобігання витокам конфіденційної інформації та порушенням регуляторних вимог. Вони інтегрують автоматизовані перевірки безпеки у процеси розробки (DevSecOps), щоб виявляти і виправляти вразливості на ранніх етапах, уникаючи серйозних проблем у майбутньому.

Моніторинг загроз і реагування на інциденти охоплюють такі повноваження фахівців з безпеки хмарних обчислень як налаштування систем збору й аналізу логів безпеки, розробка правил для виявлення аномальної

активності й потенційних атак. Вони керують оперативним реагуванням на інциденти, мінімізуючи збитки від прихованих проникнень і швидкого поширення кібератак у динамічному хмарному середовищі [48].

*DevSecOps-інженери* – це фахівці, які інтегрують безпеку в процеси розробки, розгортання й експлуатації програмного забезпечення. Development, Security, Operations – модель, у якій забезпечення безпеки відбувається на кожному з етапів.

Основними обов'язками DevSecOps-інженерів є інтеграція безпеки в DevOps; тестування та сканування на вразливості; захист розробки і процесів безперервної інтеграції та безперервної доставки (CI/CD) програм; забезпечення безпеки контейнерів і платформи Kubernetes. DevSecOps-інженери також займаються безпекою в хмарних середовищах (AWS, Azure, GCP), захищають API та мікросервіси від загроз, моніторять загрози та реагують на інциденти за допомогою систем моніторингу, таких як SIEM, XDR та SOC.

DevSecOps-інженери допомагають захистити ПЗ та інфраструктуру від кібер-атак та інших загроз, тісно співпрацюють з командами розробників, фахівців з операційної діяльності та безпеки і, нарешті, вони забезпечують відповідність ПЗ та процесів розробки вимогам безпеки і стандартам галузі.

Слід відзначити, що експерти в галузі кібербезпеки також відзначають серед найбільш затребуваних фахівців з кібербезпеки такі: інженер з кібербезпеки; аналітик кібербезпеки; архітектор мережевої безпеки; розробник програмного забезпечення безпеки; тестувальник на проникнення/етичний хакер; аналітик шкідливого ПЗ; аналітик з цифрової криміналістики [49].

**Soft skills та управлінські компетенції в кібербезпеці.** Як показало дослідження, найбільшим є попит на переважно технічні спеціальності з кібербезпеки, водночас, постійно зростають вимоги щодо наявності у фахівців з кібербезпеки так званих «м’яких» навичок, а також управлінських компетенцій.

Як відомо, «м’які» навички (soft skills) - це риси характеру і навички міжособистісного спілкування, які дозволяють людині ефективно взаємодіяти з

іншими. На робочому місці soft skills вважаються доповненням до «жорстких» навичок (hard skills), які стосуються знань і професійних навичок людини.

На конкурентному ринку праці особи, які демонструють хороше поєднання жорстких і м’яких навичок, часто користуються вищим попитом, а роботодавці шукають збалансоване поєднання жорстких і м’яких навичок, коли приймають рішення про наймання особи. Роботодавці нерідко цінують працівників із сильними навичками спілкування та самопрезентації, високим рівнем організованості й управління часом, вміннями вести переговори і навчати колег, розподіляти завдання між членами команди й ефективно ними керувати [50].

Кіберфахівці повинні володіти ефективною комунікацією, щоб чітко пояснювати складні технічні ризики керівництву та колегам, а також навчати користувачів безпечним практикам. Вони постійно застосовують критичне мислення для аналізу інцидентів, ідентифікації першопричин проблем і розробки інноваційних рішень у відповідь на нові загрози. У динамічному середовищі кібербезпеки необхідна адаптивність та готовність до безперервного навчання, адже технології і тактики зловмисників еволюціонують щодня.

Крім того, співпраця та командна робота є запорукою успішного реагування на інциденти та впровадження комплексних заходів безпеки, що вимагає злагодженої взаємодії з різними відділами. Нарешті, етична обізнаність і професіоналізм є основою довіри, забезпечуючи відповідальне ставлення до конфіденційних даних і дотримання правових норм. Разом ці "м'які" навички перетворюють технічного спеціаліста на всебічно розвиненого, затребуваного та надійного захисника у складному цифровому світі.

Для кіберфахівців, які займають керівні посади, управлінські компетенції є визначальними для їх успіху. Вони дозволяють не лише вирішувати технічні проблеми, а й ефективно управляти людьми, процесами та ресурсами, перетворюючи кібербезпеку на стратегічну перевагу організації. Менеджери з кібербезпеки повинні володіти стратегічним мисленням, щоб оцінювати ризики в бізнес-контексті й розробляти довгострокові стратегії захисту. Вони є

лідерами, які будують і мотивують команди, забезпечуючи професійний розвиток і злагоджену роботу персоналу.

У кризових ситуаціях управлінці демонструють здатність до швидкого прийняття рішень, ефективно координуючи реагування на інциденти і мінімізуючи збитки. Крім того, вони відповідають за управління проєктами та ресурсами, планування бюджетів, забезпечення відповідності регуляторним вимогам і правову обізнаність. Ці компетенції дозволяють їм не просто захищати технології, а й управляти усіма аспектами кібербезпеки, забезпечуючи стійкість і надійність організації в умовах постійних загроз.

**Міждисциплінарний характер освіти з кібербезпеки.** Кіберзагрози є глобальними, і їхня протидія вимагає міжнародної співпраці та комплексного підходу, що виходить за межі суто технічних знань. Це стимулює формування глобального кібербезпекового ринку праці й потребує переходу до міждисциплінарної освіти, яка поєднує знання з різних галузей.

Формування єдиного глобального кібербезпекового ринку праці означає, що фахівці мають бути готові працювати в міжнародних командах, розуміти різні правові системи та культурні особливості. Це стимулює поглиблене вивчення таких напрямів міжгалузевого характеру:

*Міжнародне законодавство і стандарти*. Фахівцю з кібербезпеки необхідне розуміння законів, нормативних актів і галузевих стандартів, які регулюють обробку даних, кібербезпеку та відповідальність у різних країнах або економічних блоках. Основними нормативними документами, які регулюють питання кібербезпеки є Загальний регламент про захист даних Європейського Союзу (GDPR), Каліфорнійський закон про конфіденційність споживачів у США (CCPA), а також міжнародні стандарти, зокрема стандарти серії ISO 27k, які визначають засади функціонування систем управління інформаційною безпекою, та NIST Cybersecurity Framework.

Глобальні компанії оперують даними користувачів по всьому світу. Фахівець з кібербезпеки повинен знати, як забезпечити нормативну відповідність цим різноманітним правилам, щоб уникнути величезних штрафів,

зберегти репутацію компанії та забезпечити легальність міжнародних операцій з даними. Розуміння цих норм є особливо критичним для українських фахівців, які часто працюють на аутсорсингу або у міжнародних компаніях.

*Кібердипломатія та міжнародні відносини.* Професіонал з кібербезпеки, особливо на керівній посаді, має знати засади взаємодії держави і міжнародних організацій для вирішення питань кібербезпеки, протидії кіберзлочинності, кібершпигунству та кібервійнам. Важливим є розуміння положень міжнародних конвенцій, насамперед Будапештської конвенції про кіберзлочинність, двосторонніх і багатосторонніх угод, а також ролі міжнародних організацій (ООН, НАТО, ЄС) у формуванні кіберполітики.

Сучасні кібератаки часто мають транскордонний характер, а їх джерелом можуть бути державні актори. Фахівці з кібербезпеки, особливо ті, хто працює в органах державної влади, командах CERT/CSIRT або у великих корпораціях, які нерідко є цілями хакерів на замовлення конкуруючих держав або компаній, повинні розуміти політичний контекст, щоб ефективно співпрацювати з правоохоронними органами різних країн, брати участь у міжнародних обмінах інформацією про загрози і сприяти розвитку міжнародного кіберправа.

Для України в умовах повномасштабної війни розуміння кібердипломатії є життєво необхідним для формування міжнародної підтримки та протидії агресії в кіберпросторі.

*Економіка підприємства і бізнес-діяльності.* Володіння економічними знаннями дає фахівцям здатність оцінювати кібербезпеку не лише з технічної, але й з фінансової та бізнес-перспективи. Це включає розуміння економічної ефективності інвестицій у безпеку, моделі кіберстрахування та стратегії управління ризиками, а також вартості інцидентів. Такі експерти допомагають керівництву обґрунтовувати витрати на кібербезпеку, аналізувати потенційні збитки й ухвалювати економічно виправдані рішення щодо захисту інформації.

*Психологія людини та маніпулятивні технології.* Критично важливим для протидії атакам, що експлуатують найслабшу ланку в багатьох системах кіберзахисту - "людський чинник", є знання людської психології. Розуміючи

принципи мислення, поведінки та психологічні вразливості людини, фахівці з кібербезпеки зможуть розробити ефективні тренінги з кібергігієни, які змінюють поведінку співробітників.

Для створення ефективних механізмів протидії атакам соціальної інженерії (фішинг, вішинг, претекстинг) спеціаліст з кібербезпеки має добре розбиратися в сутності маніпулятивних технологій, а для покращення загальної культури кібербезпеки в організації – володіти методами інформаційно-психологічного впливу, зокрема переконання, ведення дискусії і вирішення конфліктів.

*Інженерні знання й операційні технології (ОТ)* є дуже важливим для кіберспеціаліста з огляду на те, що кібербезпека є незамінним елементом захисту критичної інфраструктури і промислових систем. Фахівці з такою комбінацією компетенцій розуміють специфіку промислових систем управління (ICS), вбудованих систем та Інтернету речей (IoT). Вони здатні кваліфіковано захищати інформаційно-комунікаційні системи об’єктів енергетики, водопостачання, транспорту, а також мільярди IoT-пристроїв від складних кібератак, забезпечуючи безперервність і захищене функціонування цих життєво важливих систем.

*Цифрова криміналістика (Digital Forensics).* Наукова дисципліна, що займається збором, аналізом і збереженням цифрових доказів з комп'ютерних систем і мереж у спосіб, який дозволяє їх використовувати в юридичних цілях, сьогодні стала особливо популярною, а кваліфіковані аналітики з цифрової криміналістики є затребуваними на ринку праці.

Для успішного розслідування кіберзлочинів комп’ютерний криміналіст має володіти методами відновлення даних, аналізу шкідливого ПЗ, виявлення джерел і встановлення етапів атаки, а також бути здатним відновити хронологію подій, ідентифікувати зловмисників (атрибуція), визначити збитки та зібрати докази, які можуть бути передані до правоохоронних органів як на національному, так і на міжнародному рівні. Це є критичним чинником для притягнення кіберзлочинців до відповідальності й покращення майбутніх механізмів захисту.

*Мови програмування та англійська мова.* Знання таких мов, як Python (для автоматизації, аналізу даних, розробки інструментів), C/C++ (для реверс-інжинірингу, аналізу низькорівневих систем), Go, PowerShell, Bash (для автоматизації та адміністрування), JavaScript (для веб-безпеки) зазвичай є обов'язковими для фахівця з кібербезпеки. Вільне володіння англійською мовою має охоплювати як знання технічної термінології, так і здатність до ефективного усного і письмового спілкування.

Це дозволяє кіберфахівцям не лише використовувати готові інструменти, а й розробляти власні скрипти для автоматизації рутинних завдань, аналізувати шкідливі програми, проводити тестування на проникнення і впроваджувати безпечний код, що дає глибоке розуміння принципів роботи систем захисту.

Отже, як показало дослідження, інтеграція компетенцій з різних наукових і практичних дисциплін є не тільки обов'язковою вимогою для сучасного кіберфахівця, але й передумовою забезпечення ефективного кіберзахисту організацій і підприємств. Це створює попит на гібридні ролі та фахівців, які здатні мислити системно, розуміючи не лише технічні аспекти, а й правові, психологічні, економічні та інженерні контексти кібербезпеки.

## Висновки до розділу 3

Встановлено, що традиційні підходи до професійного навчання з кібербезпеки більше не відповідають потребам галузі, а сучасна система підготовки кадрів все більше орієнтується на гнучкість, практичну спрямованість, міждисциплінарність і безперервний розвиток.

Інструменти неформальної та практичної освіти для кіберфахівців, зокрема безкоштовні онлайн-курси й освітні платформи, такі як Coursera, edX, Udemy, Cybrary та FutureLearn, стають популярними інструментами отримання якісних знань від перевірених розробників. Практичні тренажери, навчальні полігони і CTF-змагання стали невід'ємними елементами підвищення кваліфікації з кібербезпеки. Вони надають безпечне, контрольоване середовище для

відпрацювання навичок кіберфахівців і моделювання реальних сценаріїв в умовах, максимально наближених до реальних. Професійні спільноти, науково-практичні заходи і менторські програми відіграють важливу роль у розвитку та підвищенні кваліфікації кадрів у сфері кібербезпеки, створюючи екосистему для безперервного обміну знаннями, нетворкінгу, наставництва і фахової підтримки.

Дослідження показало, що внаслідок швидкого розвитку нових технологій і динамічних змін сучасного ландшафту кібербезпеки зростає попит на фахівців, що володіють глибокими знаннями і практичними навичками за такими напрямами як ШІ і МН, хмарна безпека, інженерія DevSecOps, а також аналітика й архітектура кібербезпеки, розробка програмного забезпечення безпеки, пентестинг, цифрова криміналістика тощо.

Незважаючи на те, що найбільшим є попит на переважно технічні спеціальності з кібербезпеки, роботодавці все частіше очікують від спеціалістів з кібербезпеки володіння так званими «м'якими» навичками, зокрема ефективної комунікації й роботи в команді, організованості й вирішення конфліктів, а також управлінськими компетенціями.

Формування глобального ринку праці в галузі кібербезпеки потребує переходу до міждисциплінарної освіти, яка поєднує знання з різних галузей, зокрема міжнародного законодавства і стандартів, засад кібердипломатії та міжнародних відносин, економіки і психології людини, інженерії та операційних технологій, цифрової криміналістики, технічної англійської мови.

Отже, як показало дослідження, сьогодні зростає попит на гібридні ролі та фахівців, які здатні мислити системно, розуміючи не лише технічні аспекти, а й правові, психологічні, економічні та інженерні контексти кібербезпеки.

# ВИСНОВКИ

Встановлено, що галузь кібербезпеки через економічну нестабільність і скорочення персоналу переживає серйозний дефіцит кадрів, потребуючи від близько 3 до 4 млн. нових працівників. Основними причинами нестачі фахівців з кібербезпеки є труднощі в пошуку кваліфікованих працівників, недостатній бюджет на кібербезпеку, недостатній рівень заробітної плати, висока конкуренція і плинність кадрів, недостатнє навчання і підвищення кваліфікації діючих працівників, низька пріоритетність кібербезпеки на рівні організації.

Дослідження показало, що трьома найпоширенішими прогалинами у кібернавичках є питання безпеки мережі й архітектури, хмарних обчислень, AI та ML, а також реалізація концепції нульової довіри. Крім перелічених, до найбільш дефіцитних навичок у галузі кібербезпеки відносять лідерство.

Виділено такі основні способи подолання проблеми нестачі кадрів і прогалин у навичках на рівні організації: навчання й сертифікація фахівців за кошти організації; створення кращих (гнучких) умов праці, впровадження ініціатив з різноманітності, рівності та інклюзивності персоналу; підвищення кваліфікації наявних працівників; наймання персоналу за ставленням і здібностями, а не знаннями й навичками; наймання спеціалістів початкового рівня з подальшим навчанням і працівників для віддаленої роботи; перекваліфікація IT-фахівців; висока оплата праці і просування по службі.

Аналіз ринку освітніх послуг в Україні засвідчив, що понад 60 закладів вищої освіти пропонують освітні програми, адаптовані до міжнародних стандартів і розроблені у тісній співпрацю з IT-компаніями. Серед актуальних тенденцій відзначено посилення попиту на практично орієнтовану освіту, вирішення проблем нестачі кадрів через інтеграцію практичних заходів, таких як корпоративні програми навчання й підвищення кваліфікації, кіберзмагання, стажування тощо.

Виявлено, що одним із головних викликів розвитку робочої сили у сфері кібербезпеки є суттєвий дефіцит кваліфікованих спеціалістів, який поглиблюється глобальними тенденціями, впливом війни, міграцією кадрів і порушенням

освітнього процесу. Основними причинами відтоку фахівців є низький рівень заробітної плати, незадовільні умови праці, нестабільність і обмежені можливості професійного зростання в Україні. Водночас наголошено на потребі впровадження активних заходів для покращення умов праці, підтримки фахівців і підвищення престижу професії за участі держави і приватного сектору.

Дослідження показало, що кваліфікація українських фахівців з кібербезпеки часто не відповідає міжнародним вимогам. Встановлено, що причинами такої ситуації є, зокрема, недостатня кількість і висока вартість практично-орієнтованих курсів і міжнародних професійних сертифікацій, проблеми з поєднанням навчання з роботою, брак україномовних навчальних матеріалів.

Встановлено, що основними інструментами неформальної та практичної освіти для кіберфахівців є безкоштовні онлайн-курси й освітні платформи, практичні тренажери, навчальні полігони і CTF-змагання. Професійні спільноти, науково-практичні заходи і менторські програми також відіграють важливу роль у розвитку та підвищенні кваліфікації кадрів у сфері кібербезпеки.

Окреслено перспективні напрями розвитку робочої сили з кібербезпеки. Встановлено, що внаслідок швидкого розвитку нових технологій і динамічних змін сучасного ландшафту кібербезпеки зростає попит на фахівців, що володіють спеціалізованими навичками (ШІ, МН, хмарна безпека, інженерія DevSecOps тощо). Сьогодні від спеціалістів з кібербезпеки все частіше очікують володіння навичками ефективної комунікації, роботи в команді й управлінськими компетенціями. Очевидною є потреба в міждисциплінарному підході до підготовки кіберфахівців, які в нинішніх умовах мають володіти знаннями з різних галузей, зокрема міжнародного законодавства і стандартів, кібердипломатії та міжнародних відносин, економіки і психології, інженерії й операційних технологій, цифрової криміналістики тощо.

Отже, як показало дослідження, сьогодні зростає попит на фахівців, які здатні мислити системно, розуміючи не лише технічні аспекти, а й правові, психологічні, економічні та інженерні контексти кібербезпеки, виконувати вузькоспеціалізовані й гібридні ролі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023. *ISC2.* URL: https://surl.li/rmzpef

2. 2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap. 2024. *Global Cybersecurity Forum.* URL: https://surl.lu/tbyofh

3. What the cybersecurity workforce can expect in 2024. 03 January 2024. *IBM*. URL: https://www.ibm.com/think/insights/cybersecurity-workforce-trends-2024.

4. Strategic Cybersecurity Talent Framework. White paper. 2024. *World Economic Forum.* URL: https://www.weforum.org/publications/strategic-cybersecurity-talent-framework/

5. Source, Develop and Retain Cybersecurity Talent. *Gartner*. URL: https://www.gartner.com/en/cybersecurity/insights/cybersecurity-talent

6. NICE Workforce Framework for Cybersecurity (NICE Framework). *National Institute for Standards and Technology (NIST*). URL: https://niccs.cisa.gov/tools/nice-framework

7. European Cybersecurity Skills Framework (ECSF): User Manual. September 2022. *ENISA*. URL: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

8. 2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap. GCF. URL: https://web-assets.bcg.com/61/d3/705fbd684d70b0e5f98cdcf7cf47/2024-cybersecurity-workforce-report.pdf

9. Gartner Warns Of Rising Cybersecurity Workforce Burnout, Urges Resilience Planning. 2025. *Business World.* URL: https://surl.li/fqqxfv

10. Огляд ринку кібербезпеки в Україні. Січень 2025. *IT Ukraine.* URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf

11. ЗВО України. Інформаційні технології. Кібербезпека та захист інформації. *Освіта.UA*. URL: https://osvita.ua/vnz/guide/search-17-0-0-42-25.html

12. Кібербезпека та захист інформації: все про спеціальність 125. *Education.ua*. URL: https://www.education.ua/news/2024/03/29/kiberbezpeka-ta-zakhyst-informatsii-vse-pro-spetsialnist-125/

13. Найпопулярніші спеціальності для вступу у 2024 році. *Скільки-скільки?* URL: https://skilky-skilky.info/u-2024-rotsi-vpershe-naypopuliarnishoiu-spetsialnistiu-stala-psykholohiia-47672-zaiavy-abituriientiv

14. Про внесення змін до стандарту вищої освіти за спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти: Наказ Міністерства освіти і науки України від 29.20.2024 № 1547. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-bakalavr-1547-vid-29-10-2024.pdf

15. Стратегія розвитку КПІ ім. Ігоря Сікорського на 2025–2030 роки. URL: https://kpi.ua/files/2025-2030-strategy.pdf

16. Стратегія розвитку «Львівська політехніка-2025». URL: https://lpnu.ua/sites/default/files/2020/pages/2316/strategiya2025.pdf

17. Стратегія розвитку НАУ. URL: https://surl.li/momqll

18. Стратегія розвитку університету ДУІКТ. URL: https://duikt.edu.ua/uploads/p_949_80703640.pdf

19. Хуавей Україна» подарувала мережеве обладнання для нової лабораторії ДУІКТ. *Huawei*. URL: https://www.huawei.com/ua/news/ua/2024/huawei%20equipment%20for%20suict%20cybersecurity%20lab

20. Навчання корпоративних користувачів. *ESET*. URL: https://www.eset.com/ua/about/newsroom/special-offer/55/?srsltid=AfmBOopWxocvgjFjAcl-u0xRjURcx3HEBflXpPw8R4IgHan8fxcJzJg6&utm

21. CyberIN. *IT Спеціаліст.* URL: https://my-itspecialist.com/cyberin

22. Re/start your career: switch to cybersecurity. Cybersecurity training for career switchers. *ISSP*. URL: https://www.issp.com/cybersecurity-fundamentals-for-career-switchers-in-ukraine

23. GIAC Foundational Cybersecurity Technologies Certification. URL: www.giac.org/certifications/foundational-cybersecurity-technologies-gfact/

24. Tetiana M. Muzhanova, Yuriy M. Yakymenko, Mykhailo M. Zaporozhchenko, Vitalij S. Tyshchenko. International Vendor-Neutral Certification for Information Security Professionals. *Кібербезпека: освіта, наука, техніка*. 2022. № 4 (16). С. 129-141. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/369/306

25. Global Cybersecurity Outlook 2023. *World Economic Forum*. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

26. Чому існує дефіцит фахівців з кібербезпеки. *SPEKA.media*. URL: https://speka.media/deficit-kiberspecialistiv-comu-ukrayinski-faxivci-cinuyutsya-na-vagu-zolota-vzjr69

27. Cybersecurity specialist careers: Your essential roadmap. *Cybersecurity Guide*. URL: https://cybersecurityguide.org/careers/security-specialist/

28. Your Next Move: Cybersecurity Specialist. *CompTIA*. URL: https://www.comptia.org/blog/how-to-become-a-cybersecurity-specialist

29. What Degree Do I Need for a Career in Cybersecurity? URL: https://www.cyberdegrees.org/resources/degree-required-for-cybersecurity-career/

30. What is a Cybersecurity Specialist? *CompTIA*. URL: https://www.comptia.org/en/blog/what-is-a-cybersecurity-specialist/

31. IT Future. Lviv IT Cluster. URL: https://itcluster.lviv.ua/it-future/

32. Best Cybersecurity Courses & Certificates Online. *Coursera*. URL: https://www.coursera.org/courses?query=cybersecurity

33. Cybersecurity Essentials Professional Certificate. *edX*. URL: https://www.edx.org/certificates/professional-certificate/ec-council-cybersecurity-essentials

34. Digital Security Training: Cyber Threats and Risk Management. *FutureLearn*. URL: https://www.futurelearn.com/experttracks/digital-security-training

35. Prometheus. URL: https://prometheus.org.ua/

36. RangeForce Cloud-Based Cyber Range. Cybersecurity Training. *RangeForce*. URL: https://www.rangeforce.com/

37. Змагання CTF - ключ до успішної кар'єри у сфері кібербезпеки. *DOU*. URL: https://dou.ua/forums/topic/43810/

38. picoCTF - CMU Cybersecurity Competition. *picoCTF*. URL: https://picoctf.org/

39. OWASP Foundation. The Open Source Foundation for Application Security. URL: https://owasp.org/

40. ISACA: Empowering Careers. Advancing Trust in Technology. *ISACA*. URL: https://www.isaca.org/

41. Cyber Security Training. SANS Courses, Certifications & Research. *SANS*. URL: https://www.sans.org/emea/

42. About Us. *Black Hat*. URL: https://www.blackhat.com/about.html

43. IT Ukraine Association. URL: https://itukraine.org.ua/pro-asotsiatsiyu/

44. Scientific Cyber Security Association. URL: https://scsa.org.ua/association/

45. Київський Міжнародний Форум з Кібербезпеки 2025. URL: https://cyberforumkyiv.org/

46. Воркшоп “Silverfort & Check Point - IT Specialist". *IT Спеціаліст*. URL: https://my-itspecialist.com/silverfort-check-point-cloud-security-access-control-workshop

47. Cloud Security Engineer Career Guide: Skills, Roles, and How to Get Started. *ExamCollection*. URL: https://www.examcollection.com/blog/cloud-security-engineer-career-guide-skills-roles-and-how-to-get-started/

48. Все про DevSecOps: роль, принципи роботи та ключові інструменти. URL: https://university.sigma.software/what-is-devsecops/

49. Top 8 in-demand cybersecurity jobs for 2025 and beyond. *TechTarget*. URL: https://www.techtarget.com/whatis/feature/5-top-cybersecurity-careers

50. What Are Soft Skills? Definition, Importance, and Examples. *Investopedia*. URL: https://www.investopedia.com/terms/s/soft-skills.asp