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: “УПРАВЛІННЯ ТАЛАНТАМИ ЯК ІНСТРУМЕНТ ПОДОЛАННЯ ДЕФІЦИТУ КАДРІВ У 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

_____ Софія ЦАРЕНОК
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-42

Софія ЦАРЕНОК
Ім’я, ПРІЗВИЩЕ

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

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

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
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Царенок Софії Олександрівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Управління талантами як інструмент подолання дефіциту кадрів у галузі кібербезпеки”,
керівник кваліфікаційної роботи Мужанова Тетяна Михайлівна, к.держ.упр., доцент,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51.

2. Строк подання кваліфікаційної роботи “12” травня 2026 р.

3. Вихідні дані до кваліфікаційної роботи: *управління персоналом у галузі кібербезпеки, управління талантами в галузі кібербезпеки, дефіцит кадрів з кібербезпеки, управління талантами у залученні й утриманні кваліфікованих кіберфахівців.*

4. Перелік питань, які мають бути розроблені:

4.1. Дослідити теоретичні основи управління талантами.

4.2. Проаналізувати передумови нестачі кваліфікованих кадрів у галузі кібербезпеки.

4.3. Встановити роль управління талантами у подоланні дефіциту кваліфікованих кіберфахівців і розробити відповідні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Дослідження теоретичних основ управління талантами.	08.04.2026	
4.	Аналіз передумов нестачі кваліфікованих кадрів у галузі кібербезпеки.	15.04.2026	
5.	Встановлення ролі управління талантами у подоланні дефіциту кваліфікованих кіберфахівців, розробка рекомендацій.	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Софія ЦАРЕНОК
(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 Царенок С.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Управління талантами як інструмент подолання дефіциту кадрів у галузі кібербезпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка ЦАРЕНОК Софія у кваліфікаційній роботі дослідила теоретичні основи управління талантами; проаналізувала передумови нестачі кваліфікованих кадрів у галузі кібербезпеки; встановила роль управління талантами у подоланні дефіциту кваліфікованих кіберфахівців і розробила відповідні рекомендації.

ЦАРЕНОК Софія показала розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, успішно використала різні методи наукового дослідження, проявила себе як самостійний і організований виконавець. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 25 лютого 2026 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки ЦАРЕНОК Софії на позитивну оцінку та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

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

"____" _____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка ЦАРЕНОК С.О. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти ЦАРЕНОК Софії
на тему “Управління талантами як інструмент подолання дефіциту кадрів у галузі кібербезпеки”

Актуальність. У сучасних умовах цифрової трансформації суспільства та стрімкого розвитку ІТ галузь кібербезпеки стикається зі значним дефіцитом кваліфікованих фахівців. Зростання кількості кіберзагроз, ускладнення технологій захисту інформації та високий попит на спеціалістів з кібербезпеки посилюють конкуренцію за людський капітал. У таких умовах особливого значення набуває управління талантами як стратегічний інструмент залучення, розвитку та утримання висококваліфікованих працівників.

З огляду на зазначене дослідження засад управління талантами як інструмент подолання дефіциту кадрів у галузі кібербезпеки є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено теоретичні основи управління талантами, проаналізовано сучасні підходи до залучення, розвитку, мотивації та утримання персоналу, а також особливості їх застосування у сфері високих технологій та кібербезпеки.

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

3. Авторка опрацювала значну джерельну базу, що включає вітчизняні та зарубіжні наукові публікації, аналітичні звіти міжнародних організацій і професійних об’єднань у сфері кібербезпеки та управління персоналом.

4. За результатами дослідження розроблено практичні рекомендації щодо вдосконалення системи управління талантами в галузі кібербезпеки, спрямовані на підвищення ефективності залучення та утримання кваліфікованих фахівців.

Недоліки.

Доцільно було б приділити більше уваги аналізу практичного досвіду впровадження систем управління талантами в українських організаціях та більш детально розглянути питання оцінювання ефективності запропонованих заходів.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувачка ЦАРЕНОК Софія заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню засад управління талантами як інструменту подолання дефіциту кадрів у галузі кібербезпеки. Робота складається зі вступу, трьох розділів, що містять 10 рисунків і 13 таблиць, висновків і списку використаних джерел із 46 найменувань. Загальний обсяг роботи становить 62 аркуші, з яких 4 аркуші займає список використаних джерел.

Метою роботи є дослідження засад управління талантами як інструменту подолання дефіциту кадрів у галузі кібербезпеки.

Об'єктом дослідження є управління персоналом у галузі кібербезпеки.

Предмет дослідження – засади управління талантами як інструменту подолання дефіциту кадрів у галузі кібербезпеки.

Методи дослідження.

Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, моделювання та прогнозування, узагальнення кращих практик управління персоналом в галузі кібербезпеки.

Як результат у роботі досліджено теоретичні основи управління талантами; проаналізовано передумови нестачі кваліфікованих кадрів у галузі кібербезпеки; встановлено роль управління талантами у подоланні дефіциту кваліфікованих кіберфахівців і розробити відповідні рекомендації.

Галузь застосування. Запропоновані підходи та рекомендації можуть бути використані державними і приватними організаціями під час розробки стратегій залучення, розвитку та утримання фахівців з кібербезпеки, а також під час удосконалення систем управління людськими ресурсами у сфері кібербезпеки.

Ключові слова: ДЕФІЦИТ КАДРІВ З КІБЕРБЕЗПЕКИ, УПРАВЛІННЯ ТАЛАНТАМИ В ГАЛУЗІ КІБЕРБЕЗПЕКИ, УПРАВЛІННЯ ТАЛАНТАМИ У ЗАЛУЧЕННІ Й УТРИМАННІ КВАЛІФІКОВАНИХ КІБЕРФАХІВЦІВ..

ABSTRACT

The qualification work is devoted to the study of talent management as a tool for overcoming the shortage of personnel in the field of cybersecurity. The work consists of an introduction, three chapters containing 10 figures and 13 tables, conclusions and a list of references containing 46 items. The total volume of the work is 62 pages.

The purpose of the study is to investigate the principles of talent management as a tool for overcoming the shortage of qualified personnel in the field of cybersecurity.

The object of the study is personnel management in the field of cybersecurity.

The subject of the study is talent management as a tool for attracting, developing, and retaining qualified cybersecurity specialists.

Research methods. In order to achieve the objectives of the study, the methods of analysis and synthesis, comparison, classification, forecasting, modeling, and generalization of best practices in talent management and cybersecurity workforce development were used. As a result, the work examines the theoretical foundations of talent management, analyzes the causes and consequences of the shortage of cybersecurity professionals, determines the role of talent management in overcoming the workforce gap in cybersecurity, and develops practical recommendations for improving talent management systems in organizations.

Field of application. The proposed approaches and recommendations can be used by public and private organizations in developing strategies for attracting, developing, and retaining cybersecurity professionals, as well as in improving human resource management systems in the field of cybersecurity.

Keywords: TALENT MANAGEMENT, CYBERSECURITY, CYBERSECURITY WORKFORCE SHORTAGE, HUMAN RESOURCE MANAGEMENT, RECRUITMENT AND RETENTION OF CYBERSECURITY PROFESSIONALS.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах цифрової трансформації та стрімкого розвитку інформаційних технологій галузь кібербезпеки стикається зі значним дефіцитом кваліфікованих фахівців. Зростання кількості кіберзагроз, поширення хмарних технологій, штучного інтелекту та цифрових сервісів призводять до постійного збільшення потреби у висококваліфікованих спеціалістах із кібербезпеки. Водночас темпи підготовки нових кадрів не відповідають потребам ринку праці, що створює суттєві ризики для організацій та держави загалом. У таких умовах особливого значення набуває управління талантами як стратегічний підхід до залучення, розвитку, мотивації та утримання працівників. Ефективне використання інструментів управління талантами дозволяє організаціям формувати кадровий потенціал, підвищувати конкурентоспроможність та забезпечувати належний рівень кіберстійкості.

З огляду на зазначене дослідження засад управління талантами як інструменту подолання дефіциту кадрів у галузі кібербезпеки є актуальним науковим завданням.

Мета роботи полягає у дослідженні засад управління талантами як інструменту подолання дефіциту кадрів у галузі кібербезпеки.

Об'єкт дослідження – управління персоналом у галузі кібербезпеки.

Предмет дослідження – засади управління талантами як інструмент подолання дефіциту кадрів у галузі кібербезпеки.

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

1. Дослідити теоретичні основи управління талантами.

2. Проаналізувати передумови нестачі кваліфікованих кадрів у галузі кібербезпеки.

3. Встановити роль управління талантами у подоланні дефіциту кваліфікованих кіберфахівців і розробити відповідні рекомендації.

Методи дослідження. Для вирішення поставлених завдань у роботі використано методи аналізу та синтезу, порівняння, класифікації, моделювання

та прогнозування, а також узагальнення вітчизняного та зарубіжного досвіду управління талантами й подолання кадрового дефіциту у сфері кібербезпеки.

Практичне значення одержаних результатів. Практичне значення роботи полягає у розробці рекомендацій щодо вдосконалення системи управління талантами в галузі кібербезпеки. Запропоновані підходи можуть бути використані організаціями для підвищення ефективності залучення, розвитку та утримання кваліфікованих фахівців, а також для формування кадрового резерву та зниження негативного впливу дефіциту кадрів на діяльність організації.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ТАЛАНТАМИ

1.1 Поняття та розвиток концепції управління талантами

У сучасних умовах глобалізації, цифрової трансформації економіки та стрімкого розвитку інформаційних технологій значення людського капіталу в забезпеченні конкурентоспроможності організацій істотно посилюється. Саме працівники, їх професійні знання, навички, креативність та здатність до інновацій дедалі більше визначають ефективність діяльності підприємств і перспективи їх стратегічного розвитку. У зв'язку з цим традиційні підходи до управління персоналом трансформуються, а особливого значення набуває концепція управління талантами (talent management) [1, 5].

Поняття «управління талантами» є відносно новим у теорії менеджменту, однак воно швидко стало одним із ключових напрямів сучасного управління людськими ресурсами. Вперше термін «управління талантами» був використаний Девідом Уоткінсом у праці «Talent Management Systems» у 2004 році. Водночас активний розвиток цієї концепції розпочався ще наприкінці 1990-х років після оприлюднення компанією McKinsey & Company дослідження «War for Talent», у якому наголошувалося на зростаючій конкуренції між організаціями за висококваліфікованих працівників [1].

Протягом останніх двох десятиліть концепція управління талантами зазнала суттєвих змін. Якщо на початковому етапі основна увага приділялася виявленню та розвитку обмеженої групи працівників із високим потенціалом, то сучасні підходи орієнтовані на розвиток талантів серед усіх категорій персоналу. Організації дедалі частіше застосовують інклюзивний підхід до управління талантами, відповідно до якого кожен працівник розглядається як потенційне джерело інновацій та розвитку. Такий підхід сприяє формуванню сприятливого робочого середовища та підвищенню рівня залученості персоналу [5].

У науковій літературі не існує єдиного підходу до трактування поняття «управління талантами», що свідчить про його складність і багатогранність [1, 5].

Е. Майклз, Х. Хендфілд-Джонс та Е. Екселрод розглядають управління талантами як процес залучення та утримання високоефективних працівників. М. Еффрон та М. Орт визначають його як діяльність HR-підрозділів щодо прогнозування потреби організації у талановитих працівниках, створення умов для їх своєчасного залучення та розвитку [1].

На думку Н. Б. Кузнецової, управління талантами є системним аспектом функціонування бізнесу, що передбачає інтеграцію процесів пошуку, розвитку та утримання талановитих працівників у загальну систему управління підприємством. О. І. Продіус, А. І. Журавель та М. О. Сітор розглядають управління талантами як напрям управління, який забезпечує формування довгострокових конкурентних переваг організації, підвищення прибутковості та прискорення інноваційних процесів [5].

Таким чином, більшість сучасних підходів свідчать про стратегічний характер управління талантами. Якщо традиційне управління персоналом переважно орієнтується на забезпечення кадрових потреб організації, то управління талантами спрямоване на формування та розвиток людського потенціалу, який здатний забезпечити стратегічний розвиток підприємства.

Важливим етапом еволюції концепції стало поступове витіснення терміну «управління людськими ресурсами» поняттям «управління талантами» на стратегічному рівні менеджменту персоналу. У сучасних організаціях саме талановиті працівники розглядаються як ключовий фактор інноваційності, продуктивності та стійкого розвитку.

Талант у сучасному менеджменті розглядається як сукупність професійних здібностей, знань, навичок, досвіду, інтелектуальних та творчих можливостей працівника. Талановиті працівники характеризуються високою продуктивністю, здатністю до швидкого навчання, креативністю та орієнтацією на досягнення результату. Саме вони забезпечують створення інноваційних продуктів,

впровадження нових технологій та формування конкурентних переваг організації [4, 5].

На думку О. І. Драган та М. Л. Пилипенка, талановитий працівник – це працівник, який має професійні компетенції, досвід, працює з високою самовіддачею, креативністю та продуктивністю, постійно прагнучи покращити результати своєї діяльності. При цьому критерії визначення талановитого працівника можуть відрізнятися залежно від специфіки діяльності підприємства та категорії персоналу [4].

Водночас у науковій літературі існують і критичні підходи до концепції управління талантами. Зокрема, окремі дослідники зазначають, що надмірна концентрація уваги на певній категорії працівників може призводити до нерівності в колективі та негативно впливати на мотивацію інших працівників. Крім того, складність визначення самого поняття «талант» ускладнює формування об’єктивної системи оцінювання персоналу [5].

Важливу роль у системі управління талантами відіграють керівники організацій, які виступають не лише координаторами діяльності персоналу, а й наставниками, здатними створювати умови для професійного розвитку працівників та реалізації їх потенціалу. Саме від ефективності управлінських рішень значною мірою залежить успішність функціонування системи управління талантами в організації [2].

Таким чином, управління талантами є комплексною багаторівневою концепцією, яка поєднує стратегічні та операційні аспекти управління персоналом. Її ефективне застосування сприяє підвищенню конкурентоспроможності організацій, розвитку інноваційного потенціалу та адаптації до сучасних викликів ринку праці. Особливої актуальності управління талантами набуває у сфері високих технологій та кібербезпеки, де дефіцит кваліфікованих фахівців є однією з найгостріших проблем сучасного технологічного середовища.

В таблиці 1.1 узагальнено основні риси різних підходів до управління талантами [5].

Таблиця 1.1

Наукові підходи до визначення управління талантами

Автор	**Визначення поняття**	**Ключові елементи**	**Переваги підходу**	**Обмеження**
Saadat Eskandari (2016)	Управління талантами як інтегрована система HR - процесів	Відбір, навчання, розвиток та утримання	Комплексний підхід	Недостатній акцент на стратегії
Donatiello, Larcker, Tazan (2017)	Таланти як ключовий фактор ефективності компанії	Управлінські кадри та лідерство	Орієнтація на результат	Фокус лише на топ - HR менеджменті
Friebel & Raith (2025)	Вплив керівників на розвиток талантів	Роль менеджерів та рішення	Реалістичний підхід	Залежність від суб'єктивності керівника
E.Michaels, H. Handfield - Jones, B. Axelrod	Процес залучення та утримання високоефективних працівників	Пошук, відбір, утримання талантів	Орієнтація формування конкурентних переваг	Недостатня увага до розвитку персоналу
M. Effron, M. Ort	Інтегрована система процесів спрямована на забезпечення організації талановитими працівниками	Рекрутинг, оцінювання, розвиток, мотивація	Комплексний підхід до роботи з персоналом	Недостатній акцент на стратегічному аспекті

Важливим етапом становлення концепції управління талантами стало формування ідеї «війни за таланти» (war for talent), яка виникла наприкінці XX століття. Вона підкреслює, що висококваліфіковані працівники є обмеженим

ресурсом, за який активно конкурують організації. У сучасних умовах ця тенденція лише посилюється, особливо у високотехнологічних галузях [1].

Суттєву роль у розвитку концепції відіграє також зміна характеру праці. Якщо раніше основна увага приділялася виконанню стандартних функцій, то сьогодні акцент зміщується на інноваційність, креативність та здатність до швидкого навчання. У таких умовах працівники з високим потенціалом стають ключовим активом організації.

Разом із тим у науковій літературі існує критика концепції управління талантами. Зокрема, деякі дослідники зазначають, що надмірна увага до «талантів» може призводити до нерівності серед працівників та зниження мотивації тих, хто не входить до цієї категорії. Крім того, складність визначення самого поняття «талант» ускладнює практичне застосування цієї концепції.

Ще одним важливим аспектом є роль керівників у процесі управління талантами. Вони виступають не лише як координатори роботи, але й як наставники, які впливають на розвиток працівників, їх мотивацію та кар’єрне зростання. Від ефективності управлінських рішень значною мірою залежить успіх реалізації системи управління талантами.

Таким чином, управління талантами є складною та багаторівневою концепцією, яка поєднує стратегічні та операційні аспекти управління персоналом. Її ефективне застосування дозволяє організаціям адаптуватися до сучасних викликів та забезпечувати стійкий розвиток.

Особливої актуальності управління талантами набуває у сфері кібербезпеки, де дефіцит кваліфікованих кадрів є однією з найбільш гострих проблем. У таких умовах ефективна система роботи з персоналом стає ключовим фактором забезпечення безпеки інформаційних систем.

1.2 Основні складові системи управління талантами в організації

Система управління талантами в організації є комплексною та включає ряд взаємопов’язаних процесів, які забезпечують ефективну роботу з персоналом.

Вона охоплює всі етапи взаємодії працівника з організацією – від залучення до утримання (Рис. 1.1).

Рис. 1.1. Система управління талантами в організації

Розглянемо кожен із етапів детальніше [5,8].

Залучення талантів

Залучення талантів є першим і одним із найважливіших етапів. Воно передбачає визначення потреби в кадрах, формування вимог до кандидатів та організацію процесу рекрутингу. У сучасних умовах особливого значення набуває використання цифрових технологій, що дозволяють значно розширити можливості пошуку.

Важливим інструментом є брендинг роботодавця *(employer branding)*, який сприяє формуванню позитивного іміджу компанії та підвищенню її привабливості для потенційних працівників. У сфері кібербезпеки цей фактор має вирішальне значення, оскільки конкуренція за спеціалістів є надзвичайно високою.

Адаптація персоналу

Після найму важливим етапом є адаптація працівників, яка сприяє їх швидкому включенню в робочий процес та інтеграції в організаційне середовище. Ефективна адаптація дозволяє зменшити рівень стресу, підвищити

продуктивність і знизити плинність кадрів, особливо на початковому етапі роботи. У сучасних організаціях процес адаптації набуває системного характеру та реалізується через спеціальні програми (onboarding). Вони можуть включати ознайомлення з корпоративною культурою, внутрішніми правилами, навчання основним робочим процесам, а також підтримку з боку наставників.

Наявність чітко структурованої системи адаптації є особливо важливою у сфері високих технологій, де нові працівники повинні швидко освоювати складні технічні завдання. Таким чином, адаптація виступає важливою передумовою ефективного використання потенціалу працівників та їх подальшого розвитку в організації.

Розвиток та навчання

Розвиток персоналу є ключовою складовою управління талантами, оскільки саме він забезпечує підвищення професійного рівня працівників та їх відповідність сучасним вимогам ринку праці. Цей процес включає навчання, підвищення кваліфікації, участь у тренінгах, сертифікаційних програмах та професійних курсах.

У сфері високих технологій розвиток персоналу має безперервний характер, оскільки знання та навички швидко застарівають. У зв’язку з цим компанії змушені інвестувати значні ресурси у навчання своїх працівників. Особливо це актуально для галузі кібербезпеки, де постійно з’являються нові загрози та технології захисту. Крім того, розвиток персоналу включає не лише технічні знання, але й так звані «м’які навички» (soft skills), такі як комунікація, критичне мислення та здатність працювати в команді. Це дозволяє працівникам ефективніше виконувати свої функції та адаптуватися до змін.

Оцінювання ефективності

Оцінювання ефективності працівників є важливим інструментом управління талантами, який дозволяє визначити рівень їх продуктивності, професійні досягнення та потенціал для подальшого розвитку. Воно створює основу для прийняття управлінських рішень щодо кар’єрного просування, навчання та мотивації персоналу. Сучасні методи оцінювання включають

використання систем ключових показників ефективності (KPI), метод 360 градусів, а також цифрові аналітичні інструменти. У сфері високих технологій оцінювання часто базується не лише на досягнутих результатах, але й на здатності працівника до інноваційної діяльності та швидкого навчання. Таким чином, ефективна система оцінювання дозволяє організації максимально реалізувати потенціал працівників і підвищити загальну ефективність діяльності.

Мотивація персоналу

Система мотивації є важливим елементом управління талантами, оскільки вона визначає рівень залученості працівників та їх готовність до досягнення високих результатів. Вона включає як матеріальні, так і нематеріальні стимули. До матеріальних стимулів належать заробітна плата, премії, бонуси та інші фінансові винагороди. Нематеріальні стимули включають можливості кар’єрного зростання, визнання досягнень, гнучкий графік роботи, комфортні умови праці та сприятливу корпоративну культуру. У сучасних умовах дедалі більшого значення набувають саме нематеріальні фактори, оскільки вони сприяють формуванню довгострокової мотивації та підвищують рівень задоволеності працівників. Це особливо актуально для сфери кібербезпеки, де висококваліфіковані спеціалісти мають широкий вибір можливостей працевлаштування.

Важливою складовою сучасної системи управління талантами є планування наступності (succession planning). Воно передбачає формування кадрового резерву для заміщення ключових посад у майбутньому. Організації визначають працівників із високим потенціалом та створюють для них індивідуальні програми розвитку. Використання планування наступності дозволяє мінімізувати ризики, пов'язані зі звільненням ключових працівників, та забезпечити безперервність управлінських процесів.

Утримання талантів

Утримання працівників є особливо важливим у висококонкурентних галузях, зокрема у сфері високих технологій та кібербезпеки, де дефіцит кваліфікованих кадрів постійно зростає. Втрата талановитих працівників може

призвести до значних фінансових витрат, зниження продуктивності та втрати критично важливих знань і компетенцій. У зв’язку з цим організації повинні створювати умови, які сприяють довгостроковій співпраці та професійній самореалізації працівників.

До основних умов утримання талантів належать конкурентний рівень оплати праці, система преміювання та соціальних гарантій. Водночас у сучасних умовах дедалі більшого значення набувають нематеріальні фактори мотивації. Серед них важливу роль відіграють можливості професійного та кар’єрного розвитку, участь у навчальних програмах, сертифікаціях, тренінгах і міжнародних проєктах.

Важливим чинником є також формування сприятливої корпоративної культури, яка базується на підтримці інноваційності, відкритої комунікації, взаємоповаги та командної роботи. Працівники значно частіше залишаються в організаціях, де вони відчувають свою цінність, мають можливість реалізовувати власний потенціал та брати участь у прийнятті рішень.

У сфері високих технологій особливого значення набуває забезпечення гнучких умов праці. До таких умов належать дистанційний або гібридний формат роботи, гнучкий графік, баланс між професійним та особистим життям (work-life balance), сучасне технічне забезпечення та комфортне робоче середовище. Це дозволяє підвищити рівень задоволеності працівників та зменшити ризик їх переходу до конкурентів.

Крім того, важливими інструментами утримання талантів є система визнання досягнень працівників, підтримка їх ініціативності, наставництво та створення чітких перспектив кар’єрного зростання. Для фахівців у сфері кібербезпеки особливо важливою є можливість працювати над інноваційними та складними проєктами, які дозволяють постійно розвивати професійні компетенції.

Таким чином, ефективне утримання талантів потребує комплексного підходу, що поєднує матеріальні стимули, професійний розвиток, комфортні умови праці та сприятливу організаційну культуру. Саме створення таких умов

дозволяє організаціям забезпечувати стабільність персоналу та підтримувати власну конкурентоспроможність.

Короткий зміст і значення етапів показані у таблиці рис. 1.2.

Таблиця 1.2.

Основні складові системи управління талантами

Елемент	**Зміст**	**Значення**
Залучення	Пошук і відбір	Формування кадрового потенціалу
Розвиток	Навчання і тренінги	Підвищення кваліфікації
Оцінка	Аналіз результатів	Виявлення потенціалу
Мотивація	Стимулювання	Підвищення продуктивності
Утримання	Умови праці	Зменшення плинності

Основні моделі управління талантами представлені у таблиці 1.3.

Таблиця 1.3.

Основні моделі управління талантами

Модель	**Основна характеристика**
McKinsey	Фокус на залученні та утриманні талантів
Talent Pipeline	Формування кадрового резерву
CIPD Model	Розвиток талантів на всіх рівнях організації
Integrated Talent Management	Інтеграція всіх HR-процесів

Як видно з таблиці 1.3, сучасні моделі управління талантами відрізняються підходами до організації роботи з персоналом та пріоритетними напрямами розвитку людського капіталу. Модель McKinsey («War for Talent») акцентує увагу на необхідності активного залучення та утримання висококваліфікованих працівників як ключового ресурсу конкурентоспроможності організації. Модель Talent Pipeline орієнтована на формування безперервного кадрового резерву та забезпечення наступності управлінських і професійних позицій [39, 40].

Модель Integrated Talent Management передбачає інтеграцію всіх HR-процесів в єдину систему, що дозволяє забезпечити узгодженість між залученням, розвитком, оцінюванням та утриманням персоналу. У свою чергу, модель CIPD Model робить акцент на розвитку талантів на всіх рівнях організації, підкреслюючи важливість інклюзивного підходу до управління людським капіталом [12,25].

1.3 Особливості управління талантами у сфері високих технологій

Сфера високих технологій характеризується високими темпами розвитку, інноваційністю та значною конкуренцією на глобальному ринку праці. У таких умовах управління талантами набуває специфічних рис, які суттєво відрізняють його від традиційних підходів до управління персоналом. Ключовим викликом для організацій є дефіцит кваліфікованих фахівців, особливо у сфері інформаційних технологій та кібербезпеки, де попит на професіоналів значно перевищує пропозицію [2].

Однією з головних особливостей є швидке моральне старіння знань і технологій. Це зумовлює необхідність безперервного навчання та постійного оновлення компетенцій працівників. Організації змушені інвестувати значні ресурси у професійний розвиток персоналу, впроваджувати системи корпоративного навчання, сертифікації та підвищення кваліфікації. У сфері кібербезпеки це має критичне значення, оскільки поява нових загроз потребує оперативного реагування та високого рівня технічної підготовки фахівців [8].

Ще однією важливою особливістю є глобалізація ринку праці. Сучасні цифрові технології дозволяють спеціалістам працювати дистанційно, що значно розширює можливості їх працевлаштування та одночасно посилює конкуренцію між роботодавцями на міжнародному рівні. Це ускладнює процес утримання талановитих працівників та підвищує значення ефективної системи мотивації та корпоративної культури.

Особливу увагу слід приділити дефіциту управлінських та технічних талантів. Дослідження Donatiello, Larcker та Tayan (2017), проведене серед директорів компаній Fortune 250, показало, що кількість осіб, здатних виконувати роль CEO або ефективно замінити ключових керівників, є вкрай обмеженою. У більшості випадків кількість потенційних кандидатів не перевищує 3–6 осіб у межах однієї організації. Це свідчить про надзвичайно вузький ринок висококваліфікованих управлінських талантів [2].

У контексті високотехнологічних галузей це має особливе значення, оскільки помилка у виборі або втрата ключового спеціаліста може призвести до значних фінансових, операційних та репутаційних ризиків. У сфері кібербезпеки дана проблема посилюється через складність професійних компетенцій, необхідність поєднання технічних, аналітичних та стратегічних навичок, а також постійну зміну характеру кіберзагроз.

Сучасні тенденції розвитку управління талантами у сфері високих технологій включають активне використання цифрових HR-технологій, штучного інтелекту для підбору персоналу, автоматизованих систем оцінювання компетенцій, а також розвиток віддалених форматів роботи. Окремого значення набуває формування сильної корпоративної культури, орієнтованої на інновації, навчання та довгострокове утримання ключових працівників.

Особливості управління талантами у сфері високих технологій представлені в таблиці. 1.4.

Таблиця 1.4.

Особливості управління талантами у сфері високих технологій

Характеристика	**Прояв у high-tech сфері**	**Вплив на управління талантами**
Високий попит спеціалістів	Дефіцит IT та кіберфахівців	Посилена конкуренції за таланти
Швидкий розвиток технологій	Постійне оновлення знань	Необхідність безперервного навчання

Продовження табл. 1.4.

Характеристика	**Прояв у high-tech сфері**	**Вплив на управління талантами**
Глобальний ринок праці	Можливість працювати віддалено	Розширення каналів рекрутингу
Висока мобільність працівників	Часта зміна роботи	Складність утримання персоналу
Інноваційний характер роботи	Потреба у креативності	Важливість розвитку soft skills

Таким чином, управління талантами у сфері високих технологій є стратегічно важливим напрямом діяльності організацій. Воно потребує комплексного підходу, що охоплює залучення, розвиток, мотивацію та утримання висококваліфікованих фахівців. Ефективність цих процесів безпосередньо впливає на конкурентоспроможність компаній та їх здатність адаптуватися до швидкозмінного технологічного середовища.

Висновки до розділу 1

У результаті дослідження теоретичних основ управління талантами встановлено, що в сучасних умовах розвитку цифрової економіки та глобалізації людський капітал стає одним із ключових чинників конкурентоспроможності організацій.

З’ясовано, що концепція управління талантами сформувалася як відповідь на посилення конкуренції за висококваліфікованих працівників і трансформацію ролі персоналу в діяльності підприємств. Аналіз наукових підходів показав, що управління талантами розглядається як стратегічний напрям управління персоналом, який поєднує процеси залучення, розвитку, мотивації та утримання працівників із високим потенціалом.

Дослідження поняття «талант» дозволило визначити, що талановиті працівники характеризуються високим рівнем професійних компетенцій, креативністю, здатністю до швидкого навчання та орієнтацією на досягнення результату. Водночас встановлено, що у науковій літературі відсутній єдиний підхід до трактування поняття «талант», що ускладнює формування універсальної системи оцінювання персоналу. Аналіз також показав, що концепція «війни за таланти» залишається актуальною, особливо у високотехнологічних галузях, де дефіцит кваліфікованих спеціалістів є одним із головних викликів сучасного ринку праці.

Проаналізовано основні складові системи управління талантами в організації. Встановлено, що ефективна система talent management охоплює взаємопов'язані процеси залучення, адаптації, розвитку, оцінювання, мотивації та утримання персоналу. Дослідження показало, що особливого значення набувають процеси безперервного навчання працівників, розвитку soft skills, впровадження цифрових HR-технологій та формування позитивного бренду роботодавця. З'ясовано, що утримання талантів потребує створення сприятливих умов праці, конкурентної системи мотивації, можливостей професійного та кар'єрного розвитку, ефективної корпоративної культури та підтримки балансу між професійним і особистим життям працівників.

Аналіз особливостей управління талантами у сфері високих технологій засвідчив, що дана сфера характеризується високою динамічністю, швидким оновленням знань і значною конкуренцією за кваліфікованих спеціалістів. Встановлено, що у сфері кібербезпеки проблема дефіциту талантів є особливо гострою через складність професійних компетенцій та постійну зміну характеру кіберзагроз.

Дослідження також підтвердило, що ефективне управління талантами у високотехнологічних організаціях має стратегічне значення, оскільки безпосередньо впливає на інноваційний потенціал, конкурентоспроможність та стійкість компаній у сучасному технологічному середовищі.

За підсумками дослідження зроблено висновок, що управління талантами є комплексною системою стратегічного управління людським капіталом, яка забезпечує формування довгострокових конкурентних переваг організації. Ефективне впровадження системи talent management сприяє підвищенню продуктивності працівників, розвитку інноваційного потенціалу підприємства та його здатності адаптуватися до сучасних викликів ринку праці.

РОЗДІЛ 2 ПЕРЕДУМОВИ НЕСТАЧІ КВАЛІФІКОВАНИХ КАДРІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

2.1 Сучасний стан та розвиток галузі кібербезпеки

У сучасних умовах цифровізації суспільства та стрімкого розвитку інформаційних технологій галузь кібербезпеки стала однією з ключових складових забезпечення стабільного функціонування держави, бізнесу та критичної інфраструктури. Зростання обсягів цифрових даних, активне використання хмарних сервісів, розвиток штучного інтелекту, Інтернету речей (IoT) та дистанційних форматів роботи суттєво підвищили рівень кіберризиків і водночас збільшили потребу в ефективних системах захисту інформації [16].

Сьогодні кібербезпека є не лише технічним, а й стратегічним напрямом діяльності організацій. Кіберзагрози можуть призводити до значних фінансових втрат, витоку конфіденційної інформації, порушення роботи підприємств та критичних інфраструктурних об’єктів [20].

Особливої актуальності проблема кіберзахисту набула в умовах зростання кількості кібератак на державні установи, банківський сектор, енергетичні компанії та міжнародні корпорації. Аналіз сучасних тенденцій показує, що галузь кібербезпеки продовжує активно розвиватися. За даними ISC2, кібербезпекові команди у більшості організацій стикаються з постійним зростанням навантаження через ускладнення кіберзагроз та швидке впровадження нових технологій. При цьому ключовою проблемою залишається нестача кваліфікованих спеціалістів та дефіцит необхідних навичок [33,34].

Основні передумови нестачі фахівців у галузі кібербезпеки показані на рис. 2.1 [16, 17].

Рис. 2.1. Основні передумови дефіциту кадрів у галузі кібербезпеки

Як видно з рис. 2.1, дефіцит кадрів у галузі кібербезпеки формується під впливом низки взаємопов ’язаних факторів. Однією з головних передумов є стрімке зростання кількості кіберзагроз та цифровізація суспільства, що призводить до постійного збільшення потреби у кваліфікованих фахівцях. Водночас система підготовки кадрів не встигає забезпечувати ринок праці необхідною кількістю спеціалістів.

Суттєвий вплив також мають швидкі темпи розвитку технологій, які потребують постійного оновлення знань і професійних компетенцій працівників. Додатковими чинниками є висока конкуренція між роботодавцями за талановитих спеціалістів, трудова міграція та глобалізація ринку праці, що створюють труднощі із залученням і утриманням персоналу.

Важливим фактором розвитку галузі є активне використання штучного інтелекту та автоматизованих систем кіберзахисту [18]. Сучасні організації впроваджують AI-рішення для виявлення загроз, аналізу аномальної активності та автоматизації процесів реагування на інциденти. Водночас використання AI створює нові виклики, оскільки кіберзлочинці також застосовують штучний інтелект для проведення складних атак.

Окремою особливістю розвитку галузі є її глобальний характер. Кібербезпека більше не обмежується межами окремої держави чи компанії, а перетворюється на міжнародну сферу співпраці [21].

Організації активно обмінюються інформацією про кіберзагрози, створюють спільні центри реагування на інциденти та впроваджують міжнародні стандарти захисту інформації. Разом із тим розвиток галузі супроводжується високою динамічністю змін. Технології та методи захисту швидко оновлюються, що вимагає від фахівців постійного професійного розвитку [21, 18].

У таких умовах безперервне навчання та підвищення кваліфікації стають обов'язковими елементами професійної діяльності кіберспеціалістів.

У таблиці 2.1. представлено перелік і короткий опис найбільш затребуваних професій у галузі кібербезпеки [16, 17].

Таблиця 2.1.

Найбільш необхідні спеціалісти у сфері кібербезпеки

Посада	**Основні обов'язки**	**Рівень попиту**
Аналітик кібербезпеки	Моніторинг і аналіз загроз	Високий
Тестувальник на проникнення	Тестування систем на вразливості	Високий
SOC - аналітик	Реагування на кіберінциденти	Високий
Інженер інформаційної безпеки	Захист мереж і серверів	Високий
Фахівець з цифрової криміналістики	Розслідування кіберзлочинів	Середній

Таким чином, сучасна галузь кібербезпеки характеризується швидким розвитком, високим рівнем інноваційності та постійним ускладненням кіберзагроз. Це формує стійкий попит на висококваліфікованих спеціалістів і підвищує значення ефективного управління талантами у сфері кібербезпеки.

2.2 Динаміка попиту на кваліфікованих кіберфахівців на ринку праці

Сучасний ринок праці у сфері кібербезпеки характеризується високим рівнем попиту на кваліфікованих фахівців [16]. Зростання кількості кіберзагроз, цифровізація бізнес-процесів та активний розвиток інформаційних технологій формують стійку потребу організацій у спеціалістах із захисту інформації [16].

На рис. 2.2. показана динаміка дефіциту кіберфахівців у світі впродовж 2019-2025 рр.

Рис. 2.2. Динаміка дефіциту кіберфахівців у світі (2019-2025 рр.) [33,34]

На рисунку видно, що:

- кількість кіберфахівців зросла з 2,8 млн у 2019 р. до 5,5 млн у 2025 р., тобто на 2,7 млн осіб (майже вдвічі);
- дефіцит кадрів зріс з 3,1 млн до 4,8 млн осіб, тобто на 1,7 млн осіб або приблизно на 55 %.

Отже, дані рис. 2.2 свідчать про стійке зростання як кількості фахівців з кібербезпеки, так і дефіциту кадрів у галузі. Протягом 2019–2025 рр.

чисельність кіберфахівців у світі збільшилася з 2,8 млн до 5,5 млн осіб, тобто на 2,7 млн осіб. Водночас дефіцит кадрів зріс з 3,1 млн до 4,8 млн осіб, або на 1,7 млн осіб [33,34]. Це свідчить про те, що темпи зростання попиту на спеціалістів з кібербезпеки перевищують темпи підготовки та залучення нових працівників. Таким чином, проблема нестачі кваліфікованих кадрів залишається актуальною та потребує впровадження ефективних підходів до управління талантами в галузі кібербезпеки.

Додатково слід зазначити, що середній час закриття вакансії у сфері кібербезпеки становить від 3 до 6 місяців, що суттєво перевищує показники інших IT-напрямів. Це підтверджує високий рівень дефіциту спеціалістів та складність рекрутингу.

Аналіз світового ринку праці свідчить, що кількість вакансій у сфері кібербезпеки щороку зростає. Особливо затребуваними є спеціалісти з мережевої безпеки, аналізу кіберзагроз, реагування на інциденти, хмарної безпеки, пентестингу й управління ризиками [18]. Значний попит також спостерігається на фахівців із безпеки штучного інтелекту та захисту хмарних інфраструктур.

Дослідження ISC2 показало, що більшість організацій відчувають нестачу як технічних, так і нетехнічних компетенцій. Роботодавці все більше звертають увагу не лише на технічні знання кандидатів, але й на їх здатність працювати в команді, критично мислити та швидко адаптуватися до змін [33].

На рис. 2.3 наведено основні компетенції, якими повинен володіти сучасний фахівець з кібербезпеки. Вони охоплюють як професійні технічні знання (hard skills), так і особистісні та комунікативні навички (soft skills), що забезпечують ефективне виконання професійних обов’язків в умовах постійної зміни кіберзагроз.

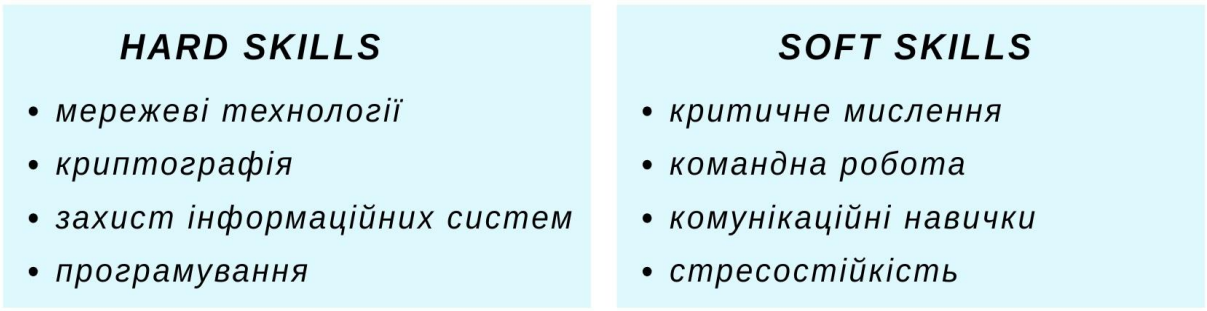

Рис. 2.3. Основні компетенції фахівця з кібербезпеки [16, 18].

Однією з тенденцій сучасного ринку праці є зміна підходів до підготовки кадрів [27]. Організації дедалі частіше інвестують у внутрішнє навчання працівників, програми наставництва, стажування та перекваліфікацію спеціалістів із суміжних галузей. Це пов’язано з тим, що традиційна система освіти не завжди встигає адаптуватися до швидких змін у сфері кібербезпеки [28].

Важливою особливістю ринку є глобальна конкуренція за таланти [19]. Завдяки розвитку дистанційної роботи спеціалісти можуть працювати на міжнародні компанії незалежно від країни проживання. Це розширює можливості працевлаштування для працівників, але одночасно ускладнює процес утримання талантів для роботодавців.

Аналіз також показує, що значна частина організацій стикається з труднощами у формуванні ефективних команд кібербезпеки через обмежені бюджети та складність пошуку спеціалістів із практичним досвідом [22]. У результаті компанії змушені переглядати підходи до рекрутингу й активніше розвивати внутрішні кадрові резерви.

Окремою проблемою ринку праці залишається недостатній рівень різноманітності персоналу. Жінки та представники окремих соціальних груп залишаються недостатньо представленими у сфері кібербезпеки, що обмежує потенційні можливості розширення кадрового резерву галузі [24].

На рис. 2.4 показано взаємозв’язок між зростанням попиту на ІТ-фахівців та наслідками дефіциту талантів на ринку праці. Схема демонструє основні

реакції організацій на нестачу кваліфікованих кадрів та інструменти, які використовуються для їх залучення й утримання.

Рис. 2.4.Вплив зростання попиту на ІТ-фахівців на формування дефіциту талантів

Таким чином, аналіз ринку праці показує, що попит на кіберспеціалістів продовжує зростати, а дефіцит кваліфікованих кадрів залишається одним із головних викликів сучасної галузі кібербезпеки.

Це обумовлює необхідність удосконалення системи підготовки персоналу, розвитку корпоративного навчання та впровадження сучасних підходів до управління талантами.

2.3 Причини та наслідки дефіциту фахівців з кібербезпеки

Однією з найбільш гострих проблем сучасної галузі кібербезпеки є дефіцит кваліфікованих кадрів. Попит на спеціалістів у сфері кіберзахисту значно перевищує пропозицію, що створює серйозні ризики для діяльності організацій та функціонування інформаційних систем [16].

Основною причиною дефіциту фахівців є стрімкий розвиток цифрових технологій та збільшення кількості кіберзагроз. Організації активно впроваджують хмарні сервіси, цифрові платформи, системи автоматизації та

штучний інтелект, однак темпи підготовки спеціалістів не відповідають швидкості технологічних змін.

У результаті виникає розрив між потребами ринку праці та кількістю підготовлених кадрів. Ще однією важливою причиною є швидке моральне старіння професійних знань [26]. У сфері кібербезпеки технології та методи захисту постійно змінюються, що вимагає безперервного навчання працівників. Багато організацій не мають достатніх ресурсів для системного професійного розвитку персоналу, що призводить до дефіциту актуальних компетенцій.

За даними ISC2, 95% організацій повідомляють про наявність принаймні одного дефіциту навичок у своїх кібербезпекових командах [16].

Суттєвою проблемою також є завищені вимоги роботодавців до кандидатів [22]. Багато компаній очікують від молодих спеціалістів наявності практичного досвіду, сертифікацій та широкого спектра технічних компетенцій навіть для початкових посад. Це ускладнює доступ нових працівників до професії та звужує кадровий резерв галузі. Додатковими чинниками дефіциту є професійне вигорання працівників, високий рівень стресу та надмірне робоче навантаження [20].

Через нестачу персоналу спеціалісти часто змушені виконувати великий обсяг роботи, працювати понаднормово та постійно реагувати на нові кіберінциденти. Це негативно впливає на рівень задоволеності працею та сприяє зростанню плинності кадрів. Наслідки дефіциту фахівців мають як економічний, так і безпековий характер.

Нестача кваліфікованих кадрів призводить до зростання ризику кіберінцидентів, помилок у налаштуванні систем безпеки та зниження ефективності реагування на атаки.

За даними ISC2, 88% організацій повідомили про виникнення щонайменше одного серйозного кібербезпекового наслідку через дефіцит навичок у командах [34]. Крім того, дефіцит кадрів підвищує фінансові витрати організацій, оскільки компанії змушені збільшувати витрати на рекрутинг, навчання та утримання персоналу.

У багатьох випадках організації використовують послуги зовнішніх консультантів або аутсорсингових компаній для компенсації нестачі внутрішніх ресурсів.

Однією з причин також є високий рівень професійного стресу та емоційного вигорання працівників. Фахівці з кібербезпеки постійно працюють в умовах підвищеної відповідальності, необхідності швидкого реагування на кіберінциденти та безперервного контролю інформаційних систем. Це створює значне психологічне навантаження та негативно впливає на утримання спеціалістів у галузі.

У науковій літературі значна увага приділяється впливу стилю керівництва на ефективність працівників та їх бажання залишатися в організації. Зокрема, у праці “The Dark and Destructive Side of Leadership” зазначається, що деструктивні форми управління можуть призводити до зниження мотивації персоналу, конфліктів у колективі, професійного вигорання та звільнення працівників [25]. Автори також наголошують, що токсична поведінка керівників є однією з причин погіршення організаційного клімату та втрати кваліфікованих кадрів.

Для сфери кібербезпеки ця проблема є актуальною, оскільки спеціалісти працюють у критично важливому середовищі, де помилки можуть призвести до значних фінансових втрат, витоку конфіденційних даних або порушення роботи державних та корпоративних систем. Відсутність підтримки з боку керівництва, надмірний контроль або постійний психологічний тиск сприяють збільшенню плинності кадрів у галузі.

Крім того, дефіцит фахівців у сфері кібербезпеки посилюється через швидкий розвиток технологій та постійне зростання кількості кіберзагроз. Організації потребують працівників із сучасними знаннями у сфері захисту даних, аналізу загроз, реагування на інциденти та роботи зі штучним інтелектом у кібербезпеці. Однак система освіти та підготовки кадрів не завжди встигає адаптуватися до нових вимог ринку праці.

Однією з організаційних причин дефіциту кадрів у сфері кібербезпеки є неефективне управління персоналом та негативний вплив деструктивного стилю лідерства.

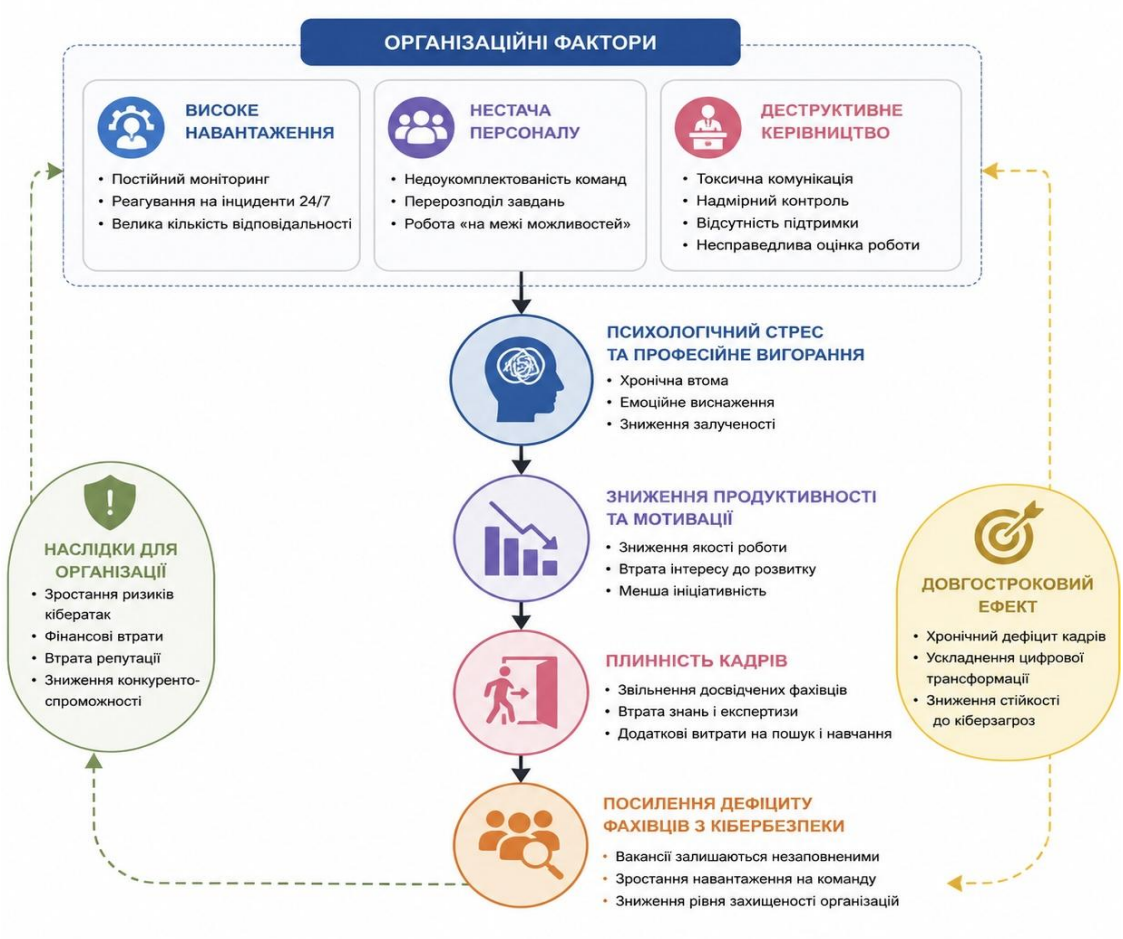

Рис. 2.5. Вплив організаційних факторів на дефіцит кадрів у сфері кібербезпеки [36].

Як показано на рисунку 2.5, організаційні проблеми та деструктивне керівництво можуть мати довгостроковий негативний вплив на кадровий потенціал галузі кібербезпеки. Погіршення психологічного стану працівників призводить до зниження мотивації та ефективності роботи, що в результаті посилює дефіцит кваліфікованих спеціалістів.

У сучасних організаціях керівники відіграють ключову роль у формуванні робочого середовища, мотивації працівників та забезпеченні ефективної командної взаємодії. У праці *"The Dark Side and Leader Derailment"* досліджується поняття «крах лідерства» (leader derailment), яке характеризує втрату керівником професійної ефективності через авторитарний стиль

управління, надмірний контроль, емоційну нестабільність або неспроможність підтримувати ефективну комунікацію з працівниками [28,33]. Автори наголошують, що такі управлінські проблеми можуть негативно впливати на психологічний клімат у колективі та знижувати рівень довіри між працівниками й керівництвом [34].

Таблиця 2.2.

Ознаки деструктивного лідерства та їх вплив на сферу кібербезпеки

Ознаки деструктивного лідерства	**Прояв у роботі організації**	**Наслідки**
Авторитарний стиль управління	Надмірний контроль працівників	Зниження ініціативності
Відсутність підтримки персоналу	Ігнорування проблем працівників	Погіршення психологічного клімату
Неефективна комунікація	Непорозуміння в команді	Помилки під час реагування на інциденти
Надмірне навантаження	Перевтома працівників	Професійне вигорання
Емоційна нестабільність керівника	Конфлікти та напруження	Плинність кадрів

У сфері кібербезпеки дана проблема має особливе значення, оскільки робота спеціалістів пов’язана з високим рівнем відповідальності, постійним стресом та необхідністю швидкого прийняття рішень. Неефективне керівництво може призводити до перевантаження працівників, професійного вигорання та втрати мотивації [18].

У результаті збільшується ризик звільнення кваліфікованих фахівців та посилюється кадровий дефіцит у галузі.

Крім того, проблеми управління негативно впливають на здатність організації забезпечувати належний рівень кіберзахисту. Відсутність підтримки працівників, погана координація команди та високий рівень плинності кадрів можуть знижувати ефективність реагування на кіберінциденти та підвищувати вразливість інформаційних систем.

У сучасній науковій літературі нестача кіберкадрів також пояснюється через концепцію життєвого циклу дефіциту талантів (Talent Gap Lifecycle), яка включає чотири стадії:

- формування попиту
- недостатня підготовка
- кадровий дефіцит
- реакція організацій через навчання і рекрутинг.

Дана модель пояснює, чому дефіцит кадрів у кібербезпеці має системний і довготривалий характер.

Для більш детального аналізу факторів, що впливають на нестачу кваліфікованих фахівців у сфері кібербезпеки, у табл. 2.3 систематизовано основні причини кадрового дефіциту, їх характеристики та наслідки для організацій [16-20].

Таблиця 2.3.

Основні причини дефіциту кадрів у сфері кібербезпеки

Причини	**Характеристика**	**Наслідки для організацій**
Стрімкий розвиток технологій	Швидке оновлення цифрових технологій та кіберзагроз потребує постійного оновлення знань	Нестача спеціалістів із актуальними компетенціями
Недостатня кількість підготовлених фахівців	Освітні програми не встигають адаптуватися до потреб ринку	Зростання конкуренції між роботодавцями

Продовження табл. 2.3.

Причини	Характеристика	Наслідки для організацій
Глобалізація ринку праці	Можливість дистанційної роботи сприяє міжнародній міграції кадрів	Відтік висококваліфікованих працівників
Високий рівень професійного вигорання	Постійний стрес і відповідальність у сфері кібербезпеки	Плинність кадрів та зниження продуктивності
Високі вимоги до компетенцій	Необхідність поєднання технічних, аналітичних та управлінських навичок	Ускладнення процесу рекрутингу
Зростання кількості кібератак	Підвищення попиту фахівців із захисту інформації	Перевантаження наявних працівників

Таким чином, дефіцит фахівців із кібербезпеки є комплексною проблемою, яка зумовлена технологічними, освітніми та організаційними чинниками. Її подолання потребує вдосконалення системи професійної підготовки, розвитку корпоративного навчання й реалізація ефективних стратегій управління талантами.

Таблиця 2.4.

Порівняння традиційного управління персоналом та управління талантами

Критерій	Традиційне управління персоналом	Управління талантами
Основна мета	Забезпечення кадрових потреб	Формування стратегічного людського капіталу
Орієнтація	Поточна діяльність	Довгостроковий розвиток

Продовження табл. 2.4.

Критерій	Традиційне управління персоналом	Управління талантами
Підхід до працівників	Усі працівники розглядаються однаково	Акцент на високопотенційних працівниках
Навчання	Періодичне	Безперервне
Мотивація	Переважно матеріальна	Комплексна система стимулювання
Кар'єрний розвиток	Обмежений	Індивідуальні траєкторії розвитку
Роль керівника	Контроль і координація	Наставництво та розвиток талантів

Як показано в таблиці 2.4, управління талантами суттєво відрізняється від традиційного управління персоналом своєю стратегічною спрямованістю та орієнтацією на довгостроковий розвиток людського капіталу [1,5,8]. На відміну від традиційного підходу, який зосереджується переважно на забезпеченні поточних кадрових потреб, управління талантами передбачає виявлення, розвиток і утримання працівників із високим потенціалом. Особлива увага приділяється безперервному навчанню, індивідуальному кар’єрному розвитку та комплексній системі мотивації. Такий підхід сприяє формуванню конкурентних переваг організації та є важливим інструментом подолання дефіциту кадрів у галузі кібербезпеки.

Висновки до розділу 2

Аналіз сучасного стану галузі кібербезпеки дозволяє зробити висновок, що ця сфера є однією з найважливіших та найдинамічніших складових цифрової економіки. Стрімкий розвиток ІТ, поширення хмарних сервісів, дистанційної

роботи, штучного інтелекту та Інтернету речей суттєво підвищують рівень кіберризиків і водночас формують постійно зростаючу потребу у висококваліфікованих спеціалістах із кіберзахисту. Кібербезпека сьогодні є не лише технічним напрямом діяльності, а стратегічним елементом забезпечення стабільності держави, бізнесу та критичної інфраструктури.

У ході дослідження встановлено, що сучасна галузь кібербезпеки характеризується високою швидкістю розвитку та постійним ускладненням кіберзагроз. Організації активно впроваджують автоматизовані системи захисту, рішення на основі ШІ та міжнародні стандарти безпеки. Разом із тим розвиток нових технологій створює додаткові виклики, оскільки кіберзлочинці також використовують сучасні інструменти для проведення складних кібератак. У таких умовах особливого значення набуває професійна підготовка кадрів, здатних швидко адаптуватися до змін та ефективно реагувати на нові загрози.

Дослідження причин дефіциту кадрів у сфері кібербезпеки показало, що дана проблема має комплексний характер. Однією з головних причин є невідповідність між темпами розвитку цифрових технологій та швидкістю підготовки фахівців. Освітні системи та корпоративне навчання не завжди встигають адаптуватися до нових вимог ринку праці, у результаті чого виникає значний дефіцит актуальних професійних компетенцій. Важливими чинниками також є швидке моральне старіння знань, високі вимоги роботодавців до кандидатів, нестача практичного досвіду у молодих спеціалістів та обмежені можливості професійного розвитку.

Окрему увагу приділено організаційним факторам дефіциту кадрів. Встановлено, що професійне вигорання, високий рівень стресу, надмірне робоче навантаження та деструктивні стилі управління негативно впливають на мотивацію працівників і сприяють зростанню плинності кадрів. Неефективне керівництво, психологічний тиск та відсутність підтримки з боку менеджменту можуть призводити до погіршення організаційного клімату, втрати кваліфікованих спеціалістів та зниження ефективності команд кібербезпеки. Для

галузі кібербезпеки ця проблема є особливо актуальною через високий рівень відповідальності та постійне психологічне навантаження на працівників.

Аналіз ринку праці підтвердив, що попит на фахівців із кібербезпеки продовжує стрімко зростати у світовому масштабі. Найбільш затребуваними залишаються спеціалісти з мережевої безпеки, аналізу кіберзагроз, реагування на інциденти, хмарної безпеки, тестування на проникнення та управління ризиками. Крім технічних знань, роботодавці дедалі більше цінують навички комунікації, критичного мислення, здатність працювати в команді та швидко адаптуватися до нових умов. Водночас глобалізація ринку праці та розвиток дистанційної роботи посилюють конкуренцію за таланти між організаціями та країнами.

У результаті дослідження було встановлено, що дефіцит кадрів у сфері кібербезпеки має значні економічні та безпекові наслідки. Нестача спеціалістів підвищує ризик кіберінцидентів, знижує ефективність реагування на атаки, збільшує фінансові витрати організацій та негативно впливає на рівень захищеності інформаційних систем. Для компенсації кадрового дефіциту компанії змушені збільшувати витрати на рекрутинг, корпоративне навчання, а також залучати зовнішніх консультантів та аутсорсингові компанії.

Таким чином, результати проведеного аналізу свідчать, що проблема дефіциту фахівців у сфері кібербезпеки є однією з ключових загроз подальшому розвитку цифрового суспільства та ефективному функціонуванню сучасних організацій. Для її подолання необхідним є комплексний підхід, який включає вдосконалення системи професійної освіти, розвиток програм безперервного навчання, підтримку корпоративного розвитку персоналу, створення сприятливого психологічного клімату в організаціях та впровадження сучасних підходів до управління талантами. Лише за умови ефективного поєднання освітніх, технологічних та управлінських рішень можливо забезпечити стабільне формування кадрового потенціалу галузі кібербезпеки та підвищити рівень захищеності сучасного інформаційного середовища.

РОЗДІЛ 3 РОЛЬ УПРАВЛІННЯ ТАЛАНТАМИ У ПОДОЛАННІ ДЕФІЦИТУ КВАЛІФІКОВАНИХ КІБЕРФАХІВЦІВ

3.1 Стратегія залучення талантів у кібербезпеці

У сучасних умовах цифровізації економіки та стрімкого зростання кількості кіберзагроз питання залучення талановитих фахівців у сферу кібербезпеки набуває стратегічного значення для організацій. Дефіцит кваліфікованих кадрів змушує компанії конкурувати між собою за спеціалістів, формуючи так звану «війну за таланти». Поняття “War for Talent” було запропоноване ще у 1997 році консультантами компанії McKinsey та відображало ускладнення процесу пошуку і утримання висококваліфікованих працівників [5, 8, 22].

На сучасному етапі ця проблема стала особливо гострою саме для кібергалузі. В умовах високої конкуренції компанії змушені переглядати традиційні підходи до рекрутингу [38]. Якщо раніше основна увага приділялася професійним навичкам та досвіду роботи, то сьогодні важливими стають потенціал працівника, здатність до швидкого навчання, адаптивність та готовність працювати в умовах постійних технологічних змін [22, 24].

Американський дослідник Джейкоб Морган у книзі *The Employee Experience Advantage* наголошує, що сучасні працівники очікують від компаній не лише високої заробітної плати, а й позитивного досвід роботи (employee experience) - сукупності вражень працівника від роботи в організації [41]. Це включає корпоративну культуру, технологічне забезпечення, можливості професійного розвитку та психологічний комфорт. Саме тому сучасні стратегії залучення талантів у кібербезпеці повинні бути орієнтовані на формування привабливого середовища праці [22].

Одним із ключових напрямів залучення кіберфахівців є розвиток HR-бренду організації. Компанії, які позиціонують себе як інноваційні роботодавці, отримують значно більше шансів привернути увагу перспективних спеціалістів

[42]. Особливо це актуально для молодого покоління працівників, які звертають увагу на корпоративні цінності, соціальну відповідальність компанії та можливості професійного зростання.

Важливу роль відіграє також співпраця бізнесу з університетами та освітніми платформами. Організації активно впроваджують програми стажування, навчальні лабораторії, хакатони та студентські практики для раннього виявлення талантів [44,48].

Основні стратегії залучення кваліфікованих фахівців у кібербезпеці та їх короткі характеристики представлені у табл. 3.1. [22, 24].

Таблиця 3.1.

Основні сучасні стратегії залучення талантів у кібербезпеці

Стратегія	**Характеристика**	**Очікуваний результат**
HR-брендинг	Формування позитивного іміджу роботодавця	Зростання кількості кандидатів
Співпраця з університетами	Стажування, дуальна освіта, хакатони	Формування кадрового резерву
Гнучкі умови праці	віддалена/гібридна робота, гнучкий графік	Підвищення привабливості компанії
Позитивний досвід роботи	Комфортне середовище праці та культура	Підвищення лояльності працівників
Пошук кваліфікованих працівників	Активний пошук талантів через LinkedIn, GitHub	Швидше закриття вакансій
Реферальні програми	Залучення працівників до пошуку кандидатів	Зниження витрат на рекрутинг

Одним із найбільш ефективних методів залучення талантів у сфері кібербезпеки є створення інноваційного середовища роботи. Кіберфахівці прагнуть працювати над складними й нестандартними завданнями, брати участь у реальних проєктах і мати можливість постійно вдосконалювати свої компетенції [46].

Важливим для залучення кваліфікованих працівників є сформувати привабливий імідж компанії-роботодавця шляхом створення сприятливих умов праці (Рис. 3.1).

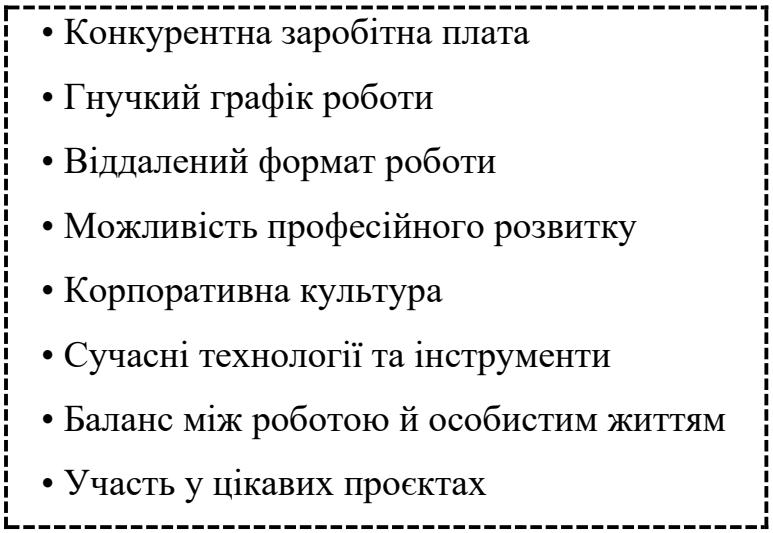

Рис. 3.1. Фактори привабливості роботодавця для кіберфахівців

Натомість для утримання кваліфікованого персоналу з кібербезпеки необхідно реалізувати низку додаткових заходів, які показані на рис. 3.2. [22, 25].

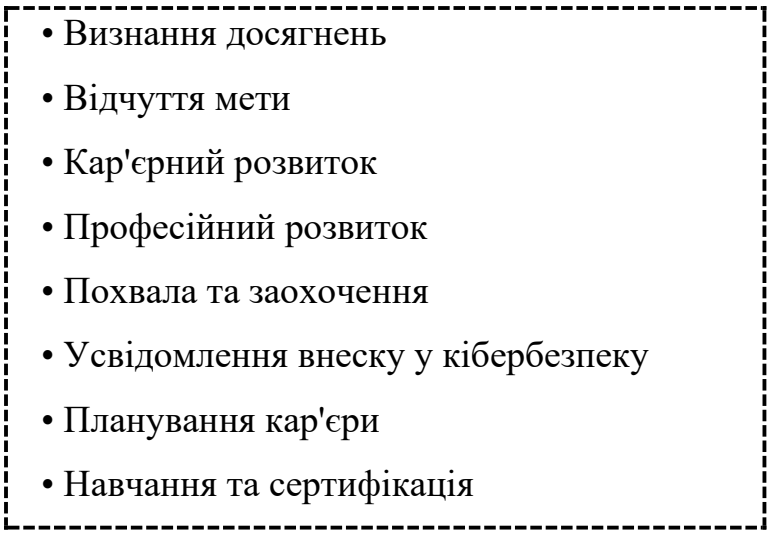

Рис. 3.2. Фактори утримання талантів у сфері кібербезпеки

Таким чином, сучасна стратегія залучення талантів у сфері кібербезпеки повинна базуватися на комплексному підході, який поєднує конкурентні умови праці, формування позитивного досвіду роботи, інвестиції в навчання та створення інноваційної корпоративної культури.

3.2 Інструменти ефективного утримання кіберспеціалістів

Ефективне управління талантами передбачає не лише залучення кваліфікованих спеціалістів, а й створення умов для їхнього професійного розвитку та довгострокового утримання в організації. Для компаній сфери кібербезпеки втрата висококваліфікованого фахівця означає не лише фінансові витрати на пошук нового працівника, а й ризики втрати критично важливих знань та досвіду [24].

Одним із головних інструментів утримання талантів є система безперервного професійного розвитку. Кібербезпека є галуззю, яка надзвичайно швидко змінюється, тому спеціалісти повинні постійно оновлювати свої знання та навички. Організації, які інвестують у навчання персоналу, мають вищий рівень залученості працівників та нижчу плинність кадрів. Інвестування у професійний розвиток не лише підвищує рівень компетентності працівників, а й позитивно впливає на їхню мотивацію та лояльність до роботодавця.

Серед основних методів професійного розвитку кіберфахівців виділяють:

- сертифікаційні програми;
- корпоративне навчання;
- менторство;
- онлайн-курси;
- участь у міжнародних конференціях;
- внутрішні тренінги;
- симуляції кіберінцидентів;
- хакатони та CTF-змагання [24-26].

У таблиці 3.2. представлений короткий опис згаданих методів професійного розвитку кіберфахівців.

Таблиця 3.2.

Інструменти професійного розвитку кіберфахівців

Інструмент	Сутність	Переваги
Сертифікація (CISSP, CEH, CompTIA)	Підтвердження професійних компетенцій	Підвищення кваліфікації
Корпоративне навчання	Внутрішні програми розвитку	Адаптація до потреб компанії
Менторство	Передача досвіду старшими колегами	Швидший професійний розвиток
Онлайн-курси	Coursera, Udemy, Cisco Networking Academy	Гнучкість навчання
Кіберполігони	Практичне моделювання атак	Формування практичних навичок
Хакатони та CTF	Командні змагання з кібербезпеки	Розвиток аналітичного мислення

Особливо важливим фактором утримання талантів є створення сприятливого психологічного середовища та підтримки ментального здоров’я. Робота у сфері кібербезпеки часто супроводжується високим рівнем стресу, емоційним вигоранням та значним навантаженням. Саме тому компанії повинні забезпечувати підтримку працівників, дбати про баланс між роботою і особистим життям (work-life balance) і впроваджувати програми добробуту персоналу.

Згідно з концепцією позитивного робочого досвіду, працівники залишаються в організації тоді, коли відчувають власну цінність, мають можливість впливати на рішення компанії та бачать перспективи професійного розвитку [22, 24-26].

Одним із важливих засобів утримання талантів є система визнання професійних досягнень працівників. Як зазначає Дж. Морган, що однією з ключових складових позитивного досвіду працівника є формування легітимного відчуття мети (legitimate sense of purpose) [41]. Воно виникає тоді, коли співробітник усвідомлює не лише свої функціональні обов'язки, а й значення

власного внеску в загальний результат діяльності організації. У таких умовах працівники сприймають свою роботу не як набір окремих завдань, а як важливу складову реалізації місії компанії.

Працівники повинні відчувати, що їхня робота є помітною, цінною та значущою для організації. Визнання не обмежується матеріальними винагородами, а включає увагу керівництва до потреб працівників, підтримку їхніх професійних досягнень та створення атмосфери поваги. Цей аспект є особливо важливим, оскільки робота спеціалістів часто залишається непомітною для більшості співробітників компанії [39]. Водночас саме від їхньої діяльності залежить захист інформаційних систем, збереження конфіденційних даних та безперервність бізнес-процесів. Саме тому керівництву необхідно демонструвати взаємозв'язок між роботою кіберфахівців та безперервністю бізнес-процесів, захистом даних клієнтів, фінансовою стабільністю та репутацією організації. Ефективним інструментом реалізації такого підходу є регулярне інформування працівників про результати їхньої роботи, залучення до стратегічних проєктів організації, участь у процесах ухвалення рішень та визнання досягнень команди інформаційної безпеки.

Регулярне визнання результатів роботи кіберфахівців сприяє підвищенню рівня їхньої залученості, задоволеності працею та бажання продовжувати професійну діяльність в організації.

3.3 Практичні рекомендації щодо вдосконалення системи управління талантами у галузі кібербезпеки

За результатами проведеного дослідження встановлено, що проблема дефіциту кадрів у сфері кібербезпеки потребує комплексного підходу до управління талантами.

Для підвищення *ефективності кадрової політики* організаціям доцільно впроваджувати сучасні інструменти залучення, розвитку та утримання працівників. Значна частина проблем, пов’язаних із плинністю кадрів та низькою

задоволеністю працівників, виникає через неефективне управління. Тому під час призначення керівників підрозділів кібербезпеки доцільно оцінювати не лише їхні технічні знання, а й лідерські компетенції, емоційний інтелект та навички управління персоналом [37].

Регулярні опитування персоналу дозволяють своєчасно виявляти проблеми в організаційній культурі, рівні навантаження та взаємодії між працівниками й керівниками. Отримані результати можуть використовуватися для коригування HR-стратегії та вдосконалення робочого середовища.

На основі концепції аналітики персоналу (People Analytics) доцільно рекомендувати організаціям кібербезпеки впроваджувати *систему аналітики персоналу*, яка дозволить: прогнозувати потребу в нових спеціалістах; визначати причини дефіциту кадрів; оцінювати ефективність програм навчання; виявляти фактори, що впливають на утримання талантів; формувати індивідуальні траєкторії професійного розвитку [22, 24-26].

Таблиця 3.3.

Використання аналітики персоналу в управлінні талантами у сфері кібербезпеки

Напрям аналізу	**Мета**	**Очікуваний результат**
Аналіз залученості працівників	Виявлення рівня мотивації	Зниження плинності кадрів
Аналіз продуктивності	Визначення ефективності роботи	Підвищення результативності команд
Аналіз професійного розвитку	Виявлення потреб у навчанні	Формування індивідуальних програм розвитку
Аналіз причин звільнення	Визначення ризиків втрати талантів	Покращення системи утримання персоналу
Аналіз компетенцій	Виявлення дефіциту навичок	Планування підготовки кіберфахівців

Напрямом вдосконалення системи управління талантами є *формування сильної корпоративної культури*. Працівники сфери кібербезпеки значною мірою орієнтуються на атмосферу в колективі, рівень підтримки з боку керівництва та можливість професійної самореалізації. Організації повинні формувати середовище, засноване на довірі, взаємній повазі, підтримці та відкритій комунікації [41].

Особливо важливим є створення *механізмів анонімного повідомлення* про конфлікти, випадки токсичної поведінки чи інші проблеми, які можуть негативно впливати на працівників.

Розвиток системи безперервного навчання. Організаціям рекомендується впроваджувати індивідуальні траєкторії професійного розвитку, підтримувати сертифікацію працівників та забезпечувати доступ до сучасних навчальних платформ. Співпраця з університетами, створення стажувань, підтримка міжнародних сертифікацій та розвиток внутрішніх освітніх програм сприятимуть підготовці нових спеціалістів і зменшенню кадрового дефіциту.

Важливим напрямом удосконалення системи управління талантами є *створення прозорих механізмів кар'єрного розвитку*. Працівники повинні розуміти можливості професійного зростання в межах організації та бачити перспективи свого майбутнього. Наявність чітко визначених кар'єрних траєкторій підвищує мотивацію працівників та сприяє їхньому довгостроковому утриманню.

Більшість організацій концентруються на пошуку вже готових експертів, що призводить до посилення конкуренції на ринку праці та зростання витрат на рекрутинг. У зв'язку з цим доцільним є формування *довгострокового кадрового резерву* шляхом співпраці із закладами вищої освіти, професійними школами, навчальними центрами та спеціалізованими кіберлабораторіями. Компанії можуть створювати програми стажувань, дуальної освіти, літні школи з кібербезпеки та власні академії підготовки фахівців. Такий підхід дозволяє не лише забезпечити організацію майбутніми кадрами, але й формувати необхідні компетенції ще на етапі навчання майбутніх працівників.

Важливе значення має *цифровізація HR-процесів*. Використання HR-аналітики, автоматизованих платформ рекрутингу та систем оцінювання компетенцій дозволяє підвищити ефективність роботи з персоналом.

Таблиця 3.4.

Рекомендації щодо вдосконалення системи управління талантами

Напрям	Рекомендації	Очікуваний ефект
Рекрутинг	Використання ШІ та пошуку талантів	Скорочення часу найму
Навчання	Безперервний розвиток компетенцій	Підвищення кваліфікації
Корпоративна культура	Формування позитивного робочого досвіду	Зростання лояльності
Мотивація	Гнучкі бонусні системи	Зменшення плинності кадрів
HR-аналітика	Використання аналітики персоналу	Прогнозування ризиків
Співпраця з університетами	Програми стажувань і практик	Формування кадрового резерву

Удосконалення системи управління талантами є впровадження *HR-аналітики.* Використання аналітичних інструментів дозволяє прогнозувати потребу в персоналі, оцінювати ефективність програм навчання, визначати ризики звільнення працівників та своєчасно виявляти перспективних співробітників. У сфері кібербезпеки HR-аналітика може застосовуватися для моніторингу рівня професійних компетенцій, аналізу результатів сертифікації, оцінювання продуктивності працівників та планування їх кар'єрного розвитку [38].

Застосування цифрових HR-рішень забезпечує більш обґрунтоване прийняття управлінських рішень та сприяє підвищенню ефективності системи управління талантами.

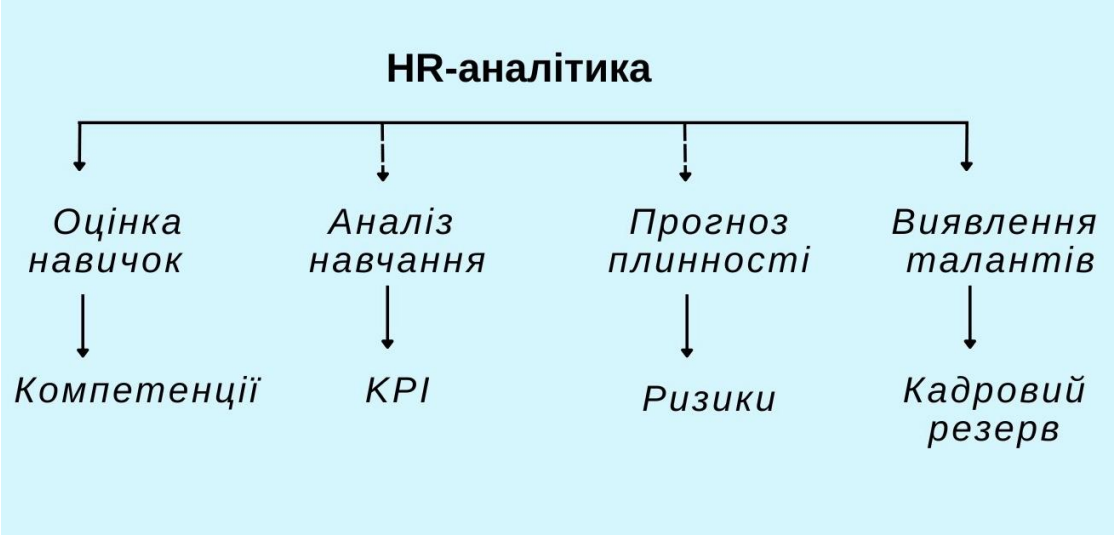

Рис. 3.3. Використання HR-аналітики в управлінні талантами

Формування відчуття значущості роботи. Сучасні дослідження свідчать, що працівники більшою мірою схильні залишатися в організації, якщо розуміють суспільну та професійну значущість своєї діяльності.

Дж. Морган підкреслює, що працівники повинні бачити зв'язок між своєю роботою та місією організації. Формування такого відчуття мети має особливе значення. Працівники повинні усвідомлювати, що їхня діяльність спрямована не лише на виконання технічних завдань, а й на забезпечення безпеки цифрового середовища, захист інформаційних ресурсів організації та протидію сучасним кіберзагрозам [41].

Особливого значення в сучасних умовах набуває *формування позитивного досвіду працівника* (Employee Experience) [41]. Відповідно до цієї концепції рівень залученості, продуктивності та лояльності персоналу значною мірою залежить від того, наскільки працівники відчувають підтримку організації, можливості для професійного розвитку та усвідомлюють цінність власного внеску у досягнення стратегічних цілей. Для сфери кібербезпеки це має особливе значення, оскільки висококваліфіковані спеціалісти часто обирають роботодавця не лише за рівнем матеріальної винагороди, а й за можливістю професійної самореалізації, професійного зростання та участі у вирішенні важливих завдань інформаційної безпеки.

На основі концепції позитивного досвіду працівника доцільно рекомендувати організаціям впроваджувати систему формування індивідуальної професійної місії працівників за аналогією до моделі V2MOM, яка використовується в Salesforce [41].

Дана модель дозволяє узгодити особисті цілі працівника зі стратегічними цілями організації, сприяє підвищенню рівня залученості персоналу та формує більш усвідомлений підхід до професійного розвитку (Табл. 3.5) [41].

Таблиця 3.5.

Елементи моделі професійного розвитку кіберфахівця

Елемент		**Зміст**
V	Vision (бачення)	Професійні цілі працівника
V	Values (цінності)	Особисті та корпоративні цінності
M	Methods (методи)	Шляхи досягнення поставлених цілей
O	Obstacles (перешкоди)	Ризики та бар'єри професійного розвитку
M	Measures (результати)	Показники оцінювання досягнень

Використання такого підходу дозволяє працівникам краще розуміти власну роль у досягненні стратегічних цілей організації та підвищує рівень їхньої залученості. Крім того, модель сприяє узгодженню індивідуальних професійних прагнень із потребами організації, що позитивно впливає на мотивацію працівників, розвиток кар’єри та довгострокове утримання персоналу.

Важливим елементом сучасної системи управління талантами є створення ефективних *механізмів утримання висококваліфікованих працівників.* В умовах глобального дефіциту кіберфахівців організації повинні приділяти особливу увагу факторам, які впливають на задоволеність персоналу та його готовність продовжувати професійну діяльність саме в межах конкретної організації [37].

Доцільним є також розвиток міжнародної співпраці у сфері підготовки кіберфахівців. Компанії можуть залучати працівників до міжнародних програм обміну досвідом, стажувань та професійних сертифікацій.

Комплексний підхід до управління талантами у сфері кібербезпеки представлений на рис. 3.4.

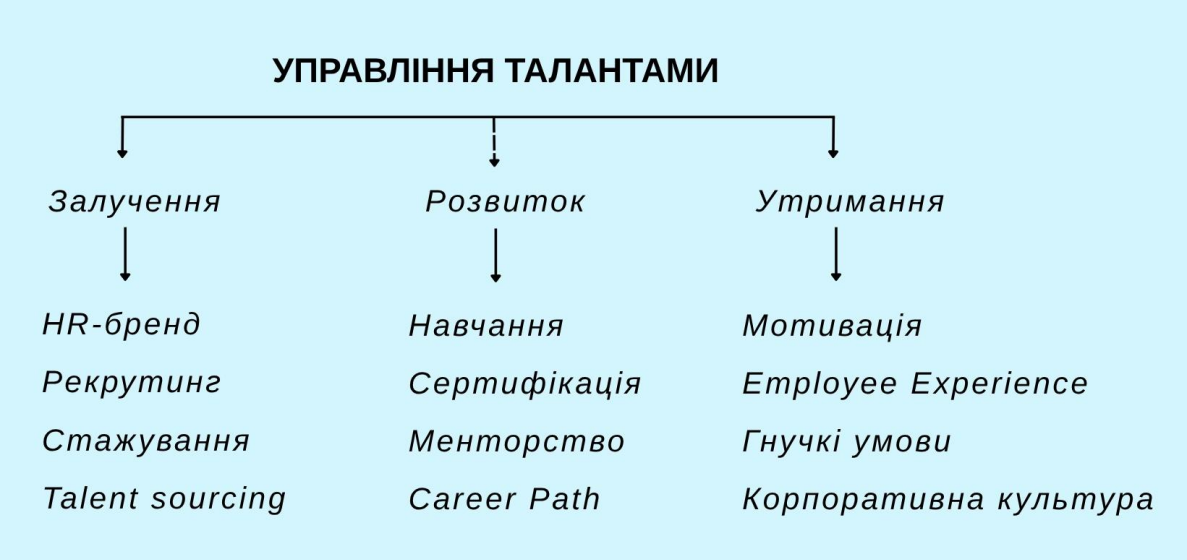

Рис. 3.4. Комплексна система управління талантами у сфері кібербезпеки

Формування бренду роботодавця у сфері кібербезпеки. В умовах дефіциту кіберфахівців особливого значення набуває бренд роботодавця. Організації конкурують між собою не лише рівнем заробітної плати, а й репутацією, можливостями професійного розвитку, корпоративною культурою та умовами праці. Сильний бренд роботодавця сприяє зменшенню витрат на рекрутинг, підвищує кількість якісних кандидатів і покращує рівень утримання працівників.

Для формування позитивного бренду роботодавця організаціям доцільно:

- популяризувати історії професійного успіху співробітників;
- демонструвати можливості навчання та сертифікації;
- брати участь у професійних конференціях та кіберфорумах;
- підтримувати освітні ініціативи;
- розвивати корпоративну культуру інновацій і безперервного навчання [13,36,41].

Таким чином, ефективна система управління талантами є одним із ключових інструментів подолання дефіциту кадрів у сфері кібербезпеки.

Організації, які інвестують у розвиток employee experience, професійне навчання та сучасні HR-технології, отримують конкурентні переваги на ринку праці та здатні забезпечити стабільний розвиток в умовах цифрової трансформації.

Поєднання сучасних підходів до рекрутингу, розвитку, мотивації та утримання персоналу дозволяє сформувати стійку систему управління талантами, здатну забезпечити довгострокову ефективність діяльності організації та її готовність до протидії сучасним кіберзагрозам.

Висновки до розділу 3

У розділі 3 досліджено можливості використання управління талантами як одного з ключових інструментів подолання дефіциту кадрів у сфері кібербезпеки.

В умовах цифрової трансформації економіки та постійного зростання кількості кіберзагроз проблема нестачі висококваліфікованих спеціалістів набуває стратегічного значення як для окремих організацій, так і для держави загалом. Дослідження дозволило визначити основні напрями вдосконалення системи управління талантами, спрямовані на залучення, розвиток і утримання кіберфахівців.

Встановлено, що ефективна стратегія залучення талантів у сфері кібербезпеки повинна базуватися на комплексному підході, який поєднує сучасні методи рекрутингу, розвиток бренду роботодавця, співпрацю із закладами освіти та формування позитивної репутації організації на ринку праці. Аналіз сучасних тенденцій показав, що традиційні підходи до підбору персоналу поступово втрачають ефективність, оскільки висококваліфіковані кіберфахівці дедалі частіше оцінюють роботодавця не лише за рівнем матеріальної винагороди, але й за можливістю професійної самореалізації, участі в інноваційних проєктах та перспективами кар’єрного розвитку.

Успішне залучення талантів передбачає створення привабливого середовища праці, у якому працівники можуть реалізувати свій потенціал та отримати можливості для безперервного професійного зростання. Дослідження

також показало, що важливою складовою сучасної системи управління талантами є професійний розвиток працівників.

З’ясовано, що стрімкий розвиток технологій та постійна поява нових кіберзагроз обумовлюють необхідність безперервного навчання та вдосконалення професійних компетенцій фахівців із кібербезпеки. У зв’язку з цим організаціям доцільно впроваджувати комплексні програми розвитку персоналу, які включають професійні тренінги, сертифікацію, участь у спеціалізованих конференціях, хакатонах, кібернавчаннях і міжнародних програмах обміну досвідом.

Встановлено, що систематичне інвестування у розвиток компетенцій працівників сприяє не лише підвищенню рівня їхньої кваліфікації, а й формуванню довгострокової лояльності до організації.

З’ясовано, що одним із найважливіших чинників подолання дефіциту кіберфахівців є ефективна система утримання талантів. Аналіз сучасних наукових підходів дозволив зробити висновок, що матеріальна мотивація залишається важливим елементом системи управління персоналом, однак її недостатньо для забезпечення довгострокової прихильності працівників до організації. Значно більшого значення набувають можливості професійного розвитку, справедлива система оцінювання результатів праці, визнання досягнень працівників, гнучкі умови роботи, сприятливий психологічний клімат та підтримка балансу між професійним і особистим життям.

Особливу увагу у дослідженні приділено концепції позитивного досвіду роботи, яка останніми роками набуває все більшого поширення в системах управління талантами провідних світових компаній. Встановлено, що позитивний досвід працівника безпосередньо впливає на рівень його залученості, продуктивності та лояльності. Для кіберфахівців це має особливе значення, оскільки їхня професійна діяльність пов’язана з високим рівнем відповідальності, постійним навчанням і роботою в умовах підвищеного психологічного навантаження. Саме тому формування комфортного робочого середовища, забезпечення сучасними технологічними інструментами і

створення сприятливої корпоративної культури розглядають як важливі інструменти зниження плинності кадрів з кібербезпеки. У процесі дослідження обґрунтовано доцільність використання моделі індивідуального професійного розвитку працівників за аналогією до концепції V2MOM.

Узгодження особистих цілей працівника зі стратегічними цілями організації дозволяє підвищити рівень залученості персоналу та сприяє більш усвідомленому професійному розвитку. Використання такої моделі дає можливість працівникам чітко розуміти власну роль у забезпеченні кібербезпеки організації та бачити перспективи свого кар'єрного зростання, сприяє зміцненню їхньої організаційної прихильності та позитивно впливає на прагнення залишатися в компанії протягом тривалого часу. Аналіз сучасних підходів до управління талантами також показав важливість формування у працівників відчуття значущості власної діяльності.

За підсумками дослідження розроблено практичні рекомендації щодо вдосконалення системи управління талантами у сфері кібербезпеки, зокрема впровадження сучасних програм розвитку та навчання персоналу, використання інструментів HR-аналітики для прогнозування кадрових потреб, формування кадрового резерву, розвиток міжнародної співпраці у сфері підготовки кіберфахівців, удосконалення системи адаптації нових працівників і впровадження заходів щодо профілактики професійного вигорання.

Таким чином, результати дослідження підтверджують, що ефективна система управління талантами є одним із найважливіших інструментів подолання дефіциту кіберфахівців. Комплексне поєднання заходів із залучення, розвитку, мотивації та утримання персоналу дозволяє організаціям формувати конкурентні переваги на ринку праці, забезпечувати високий рівень кадрового потенціалу та підвищувати ефективність протидії сучасним кіберзагрозам.

У сучасних умовах саме людський капітал стає ключовим фактором забезпечення кіберстійкості організацій, а ефективне управління талантами – необхідною передумовою їхнього стабільного розвитку і конкурентоспроможності.

ВИСНОВКИ

У кваліфікаційній роботі досліджено управління талантами як інструмент подолання дефіциту кадрів у галузі кібербезпеки.

За результатами проведеного дослідження досягнуто поставленої мети та виконано визначені завдання.

У ході дослідження встановлено, що управління талантами є важливим стратегічним напрямом управління персоналом, який охоплює процеси залучення, розвитку, мотивації та утримання працівників. Ефективна система управління талантами сприяє формуванню кадрового потенціалу організації, підвищенню її конкурентоспроможності та забезпеченню стійкого розвитку.

Проаналізовано сучасний стан галузі кібербезпеки та передумови нестачі кваліфікованих фахівців. Встановлено, що основними причинами дефіциту кадрів є стрімке зростання попиту на спеціалістів з кібербезпеки, недостатні темпи підготовки нових кадрів, швидкий розвиток технологій та висока конкуренція за талановитих працівників на світовому ринку праці. Визначено, що дефіцит фахівців негативно впливає на рівень захищеності організацій та створює додаткові ризики для їх діяльності.

Дослідження показало, що управління талантами відіграє важливу роль у подоланні кадрового дефіциту в галузі кібербезпеки. Використання сучасних підходів до рекрутингу, професійного розвитку, навчання, наставництва та мотивації дозволяє організаціям залучати й утримувати кваліфікованих працівників, а також створювати умови для їх професійного зростання.

За результатами роботи запропоновано рекомендації щодо вдосконалення системи управління талантами у сфері кібербезпеки, зокрема розвиток програм безперервного навчання, використання сучасних HR-технологій, посилення співпраці між роботодавцями та закладами освіти, формування кадрового резерву та впровадження ефективних механізмів мотивації персоналу.

Таким чином, проведене дослідження підтвердило, що управління

талантами є одним із ключових інструментів подолання дефіциту кадрів у галузі кібербезпеки та важливою умовою забезпечення ефективного функціонування і розвитку сучасних організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Винничук Р. О. Особливості навчання працівників у системі талант-менеджменту: світова практика та рекомендації. Економіка і суспільство. 2018. Вип. 16. С. 647–652.

2. Драган О. І., Пилипенко М. Л. Розвиток управління талантами в системі менеджменту персоналу підприємства. Економіка та суспільство. 2021. Вип. 33. С. 318–324.

3. Кузнецова Н. Б. Концепція управління талантами в системі менеджменту знань. Соціально-трудові відносини: теорія та практика. 2014. № 2(8). С. 181–187.

4. Продіус О. І., Журавель А. І., Сітор М. О. Талант-менеджмент як невід'ємна складова успіху організації. Економіка: реалії часу. 2013. № 1(6). С. 172–177.

5. Татаревська М. С., Сорока О. В. Проблеми та перспективи управління талантами в сучасних організаціях. Вісник соціально-економічних досліджень. 2013. Вип. 4(51). С. 160–164.

6. Adair J. Effective Leadership. London : Pan Books, 1983.

7. Alexander B. K. A Case for Change: Assessment of an Evidence-Based Leadership Development Program. Dissertation Abstracts International Section A. 2014. Vol. 74. No. 9.

8. Allen L. A. An Evaluation of a Shared Leadership Development Training Program. ProQuest Dissertations & Theses Global, 2010.

9. Antonakis J., Fenley M., Liechti S. Can Charisma Be Taught? Tests of Two Interventions. Academy of Management Learning & Education. 2011. Vol. 10. No. 3. P. 374–396.

10. Arthur W. Jr., Bennett W. Jr., Edens P. S., Bell S. T. Effectiveness of Training in Organizations: A Meta-analysis of Design and Evaluation Features. Journal of Applied Psychology. 2003. Vol. 88. P. 234–245.

11. Baldwin T. T., Ford J. K. Transfer of Training: A Review and Directions

for Future Research. Personnel Psychology. 1988. Vol. 41. P. 63–105.

12. Barthol R. P., Zeigler M. Evaluation of a Supervisory Training Program with How Supervise. Journal of Applied Psychology. 1956. Vol. 40. P. 403–405.

13. Bentz V. J. Research Findings from Personality Assessment of Executives. In: Personality Assessment in Organizations. New York : Praeger, 1985. P. 82–144.

14. Bentz V. J. The Sears Experience in the Investigation, Description, and Prediction of Executive Behavior. In: Measuring Executive Effectiveness. New York : Appleton-Century-Crofts, 1967. P. 147–206.

15. Blume B. D., Ford J. K., Baldwin T. T., Huang J. L. Transfer of Training: A Meta-analytic Review. Journal of Management. 2010. Vol. 36. P. 1065–1105.

16. Chartered Institute of Personnel and Development. Megatrends: The Trends Shaping Work and Working Lives. London : CIPD, 2013.

17. Copeland C. Employee Tenure Trends, 1983–2014. EBRI Notes. 2015. Vol. 36. No. 2. P. 2–3.

18. Dobbs R., Lund S., Madgavkar A. Talent Tensions Ahead: A CEO Briefing. McKinsey Quarterly. 2012.

19. Donatiello N., Larcker D. F., Tayan B. CEO Talent: A Dime a Dozen, or Worth Its Weight in Gold? Stanford Graduate School of Business, 2017.

20. Donatiello N., Larcker D., Tayan B. CEO Succession Planning: Current State of the Art and How to Improve It. Stanford : Stanford Closer Look Series, 2017.

21. Einarsen S. V., Fosse T. H. The Dark and Destructive Side of Leadership: A Behavioral Perspective. New York : Routledge, 2019.

22. Einarsen S. V., Skogstad A., Aasland M. S. The Dark Side and Leader Derailment. In: The Dark and Destructive Side of Leadership: A Behavioral Perspective. New York : Routledge, 2019. P. 15–34.

23. Elliot A. J., Thrash T. M. Approach-Avoidance Motivation in Personality: Approach and Avoidance Temperaments and Goals. Journal of Personality and Social Psychology. 2002. Vol. 82. No. 5. P. 804–818.

24. European Union Agency for Cybersecurity (ENISA). Cybersecurity Skills Development in the EU. Luxembourg : Publications Office of the European Union,

2024. URL: https://www.enisa.europa.eu/publications

25. Fosse T. H., Skogstad A. Faultlines, Failure, and Fracture: The Dark Side of Team Dynamics. In: The Dark and Destructive Side of Leadership: A Behavioral Perspective. New York : Routledge, 2019. P. 95–118.

26. Goupil F. et al. Towards Understanding the Skill Gap in Cybersecurity. ACM, 2022.

27. Gøtzsche-Astrup O., Jakobsen J., Furnham A. The Higher You Climb: Dark Side Personality and Job Level. Scandinavian Journal of Psychology. 2016.

28. Harms P. D., Spain S. M., Hannah S. T. Leader Development and the Dark Side of Personality. Leadership Quarterly. 2011.

29. Harris S., Krueger A. B. A Proposal for Modernizing Labor Laws for Twenty-First Century Work. The Hamilton Project, 2015.

30. Hogan R., Hogan J. Assessing Leadership: A View from the Dark Side. International Journal of Selection and Assessment. 2001.

31. Hogan R., Hogan J., Barrett P. Good Judgment: The Intersection of Intelligence and Personality. CRC Press, 2008.

32. International Information System Security Certification Consortium (ISC2). Cybersecurity Workforce Study 2023. Alexandria, VA : ISC2, 2023. URL: https://www.isc2.org/research/workforce-study

33. ISC2. 2024 ISC2 Cybersecurity Workforce Study. 2024.

34. ISC2. 2025 ISC2 Cybersecurity Workforce Study. 2025.

35. Katz L. F., Krueger A. B. The Rise and Nature of Alternative Work Arrangements in the United States, 1995–2015. Cambridge : NBER, 2016.

36. KPMG International. War for Talent – Time to Change Direction. 2014.

37. Mann A., Harter J. The Worldwide Employee Engagement Crisis. Gallup. 2016.

38. Mechkat A., Weise P. War for Talents in der IT-Branche: Personalbeschaffung durch gezielte Abwerbung in den Jahren 1998–2001. Berlin, 2001.

39. Mechkat A., Weise P. War for Talents in der IT-Branche. Wiesbaden :

Deutscher Universitäts-Verlag, 2002.

40. Michaels E., Handfield-Jones H., Axelrod B. The War for Talent. Boston : Harvard Business School Press, 2001.

41. Morgan J. The Employee Experience Advantage. Hoboken, NJ : John Wiley & Sons, 2017.

42. Saadat V., Eskandari Z. Talent Management: The Great Challenge of Leading Organizations. International Journal of Organizational Leadership. 2016.

43. Society for Human Resource Management. 2016 Employee Job Satisfaction and Engagement. Alexandria, VA : SHRM, 2016.

44. The World's Most Innovative Companies. Forbes. 2016.

45. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva : World Economic Forum, 2025. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2025

46. Zumbrun J., Sussman A. L. Proof of a Gig Economy Revolution Is Hard to Find. The Wall Street Journal. 2015.