КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА ЕКОНОМІКИ ПІДПРИЄМСТВА

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему:

Консалтинговий супровід у формуванні стратегії підготовки фахівців з кібербезпеки

студента 2-го курсу СО «Магістр»
денної форми навчання
освітньо-професійної програми
Бізнес-консалтинг
ВАЛЬЧУНА Іллі Олександровича

Науковий керівник
к.е.н., доцент. МАГОМЕДОВА Аліна Магомедівна

Засвідчую, що в цій дипломній
роботі немає запозичень із праць
інших авторів без відповідних посилань

Студент

(підпис)

Робота допущена до захисту в ЕК рішенням кафедри економіки підприємства від

«19 » грудня 2023р. , протокол № 6.

Завідувач кафедри економіки підприємства,
доктор економічних наук, професор
ФИЛЮК Галина Михайлівна _____

(підпис)

Київ – 2023

ЗМІСТ

ВСТУП

У динамічному світі, де технологічний прогрес стрімко впливає на усі аспекти нашого життя, ми стаємо свідками настання нової ери людських взаємовідносин. Інформаційна революція, глобалізація та швидкий розвиток інновацій перетворюють спосіб, яким ми спілкуємося, працюємо та взаємодіємо один з одним. У такому прогресивному світі фахівці майбутнього виступають ключовими суб’єктами та джерелами цього перетворення. Глобальні виклики та можливості, що виникають від цієї еволюції, надають спеціалістам усіх галузей важливу роль у формуванні нових парадигм в трудових, освітніх відносинах. Дослідження цієї теми відкриває перед нами не лише можливі перспективи змін у способі життя, але і наголошує на значущості підготовки фахівців до викликів, які приносить ця нова епоха взаємодії та співпраці.

Підприємництво стає ключовим стимулом для розвитку та адаптації. Підприємницька діяльність виявляється не лише каталізатором економічного зростання, але й важливим чинником формування нових форм взаємодії між людьми. Розглядаючи підприємництво як силу, що мобілізує і трансформує суспільство, ми можемо з'ясувати, як воно впливає на динаміку та характер нового етапу розвитку господарських відносин.

Проблема між сучасним технологічним світом та людьми, які не готові до змін, стає важливим викликом сучасності. Швидкий темп технологічного розвитку часто ставить людей перед проблемою адаптації до нових умов. Люди, які не готові до змін, можуть відчувати себе неповноцінними і навіть втрачати робочі місця. При цьому вони можуть розглядати технології як загрозу, а не як інструмент для поліпшення життя.

Консалтинг може відігравати ключову роль у вирішенні цих проблем. Консультанти здатні працювати як посередники між технологічними рішеннями та кінцевими користувачами, сприяючи взаєморозумінню та впровадженню технологій в спосіб, який враховує потреби та переживання користувачів.

Щоб керувати індивідуальним та колективним процвітанням, бізнес потребує нового способу мислення для прийняття рішень. Допомогти йому впоратися з цим завданням може бізнес-консалтинг. Згідно з інформацією провідної світової компанії з питань інформаційних технологій та консультацій Gartner, «Ринок консалтингу зріс на 14,0% у доларах США до 266,3 мільярдів доларів у 2022 році. Консалтингові послуги мали високий попит, оскільки клієнти продовжували прискорювати цифрову трансформацію свого бізнесу, водночас збільшуючи свою залежність від зовнішніх консультантів через брак кадрів» [42].

Тенденції останнього десятиліття показують невідворотність цифровізації та автоматизації економічно-суспільних процесів. Щорічно різноманітні види діяльності від державного до приватного секторів переносяться з матеріальної в цифрову форму. Це полегшує ведення справ та пришвидшує надання послуг. Проте подібна масштабна цифрова трансформація потребує надійного підґрунтя, яке забезпечить конфіденційність та цілісність всіх систем. Головну роль в цьому відіграє кібербезпека та захист інформації. Впроваджуючи цифрову трансформацію кожна компанія так чи інакше зіштовхується з тим же питанням кібербезпеки. Відповідно до першого щорічного звіту Державної служби спеціального зв’язку та захисту інформації України за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2021 року в Україні було детектовано 41 млн підозрілих подій та 147 кіберінцидентів. Цілями ураження були як державні, так і приватні установи. Вже у наступному 2022 році було детектовано 181 млн підозрілих подій інформаційної безпеки, зафіксовано та оброблено 415 кіберінцидентів. Фактичний рівень загроз зріз майже в тричі.

Уповноважені органи з питань інформаційної та кібербезпеки закликає керівників підприємств, установ і організацій тримати на особистому контролі питання кіберзахисту своїх інформаційно-комунікаційних систем. У зв'язку з цим у 2021 році почав активно розвиватися ринок кібербезпеки [1].

Дану проблему всі вирішують по-різному, проте ключовим є наявність кваліфікованих кадрів, здатних компетентно та фахово підійти до питання забезпечення надійності та безпеки процесів цифровізації. Дієвість протистояння кібернетичним загрозам, забезпечення безпеки повноцінного функціонування державних та приватних організацій, прав людини і громадянина в інформаційно-комунікаційному просторі забезпечується в першу чергу завдяки професійності та кваліфікованості фахівців, що є основою для формування дієвості всієї системи кібербезпеки. Відповідно постає питання формування такої ж кваліфікованої та компетентної системи підготовки кадрів.

Виникнення принципово нових видів економічної діяльності, зумовлених стрімким прогресом науки і техніки, сприяло появі абсолютно нових видів економічної діяльності та професій, які здатні забезпечувати їх діяльність. Паралельно до цього процесу у відповідь реагували і заклади вищої освіти, які запускали нові спеціальності та розробляли навчальні програми які корелюють з вимогами ринку.

Актуальність магістерської роботи полягає у тому, що результатом її роботи буде принципово новий, раніше не використовуваний метод та засіб аналітичного аналізу ринку кібербезпеки з врахуванням наявної пропозиції на ринку та попиту.

Теоретично-методична база дипломної роботи ґрунтується на дослідженнях вітчизняних та зарубіжних вчених, нормативно-правових актах (кодекси, закони) матеріалах українських наукових конференцій, статистичних матеріалах науково-

дослідницьких центрів, на дослідженнях найбільших міжнародних аудиторських компаніях «Великої четвірки».

Вивчення теоретичних аспектів у бізнес-консалтингу присвячені роботи таких вчених: О.Марченко, Е.Цибульська, К.Краус, К.Уолш, Я.Ізмайлов, Ю.Апелло. Аналіз теоретичних матеріалів показав, що консалтингові послуги поширені в переважній більшості сфер підприємницької діяльності та, за умови виконання якісної роботи консультантами, можна досягти значних результатів підвищення ефективності діяльності як в приватному секторі, так і в публічному.

Метою дипломної роботи є дослідити особливості і тенденції у сфері кібербезпеки та на їх основі запропонувати інструменти щодо вдосконалення процесу підготовки фахівців з кібербезпеки на основі консалтингового супроводу.

Для конкретизації мети, було сформовано наступні завдання дослідження:

1. Ознайомитись з особливостями ринку консалтингових послуг в Україні
2. Визначити сутність та особливості сфери кібербезпеки в Україні
3. Обґрунтувати роль консалтингу у забезпеченні господарської діяльності
4. Визначити необхідне ресурсне забезпечення та хід реалізації консалтингового проєкту
5. Розробити інструмент для оцінки трудових ресурсів з кібербезпеки
6. Проаналізувати результати імплементації розробленого інструменту
7. Надати пропозиції щодо підвищення ефективності підготовки кадрів
8. Обґрунтувати актуальність впровадження дуальної освіти як способу трансформації вищої освіти
9. Розробити оцінювання ефективності стратегії підготовки фахівців з кібербезпеки

Об’єктом дослідження є консалтинговий проєкт щодо розробки та використання інструменту, який дозволяє проаналізувати ключові параметри розвитку трудових ресурсів з кібербезпеки в Україні.

Предметом дослідження є теоретико-методичні рекомендації щодо розробки та формування стратегії підготовки фахівців з кібербезпеки.

В процесі підготовки моделі даних та проведенні аналізу отриманих даних застосовувалися методи статистичної та експертної оцінки. Для досягнення мети роботи застосовувалися також методи графічної візуалізації, конкретизації, порівняння та прогнозування.

Практична цінність отриманих результатів дослідження ґрунтується на можливості їх застосування для розробки стратегічних документів стосовно розвитку ринку кібербезпеки України, при реформуванні вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації».

Наукова новизна даного дослідження полягає у розробці та реалізації нового підходу та аналітичного інструменту для отримання консолідованої інформації щодо попиту та пропозиції на ринку кібербезпеки України.

Матеріали роботи були апробовані на двох міжнародних конференціях:

1. Міжнародна наукова конференція «Гальчинські читання».
2. Міжнародна науково-практична конференція «Дуальна форма здобуття освіти: підсумки запровадження пілотного проєкту у закладах вищої та фахової передвищої освіти України».

Робота складається зі вступу, трьох основних розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дипломної роботи сягає 78 сторінок, в який не включено список використаної літератури із 52 найменувань.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ КОНСАЛТИНГОВИХ ПОСЛУГ

1.1 Особливості ринку консалтингових послуг в Україні.

Бізнес-консалтинг — це дуже важливий елемент у сучасному світі підприємництва та управління. Швидкі темпи змін у бізнес-середовищі, розвиток технологій і підвищення рівня конкуренції є причиною того, що консалтингові послуги з кожним роком стають все важливішими для різних форм господарювання. Бізнес-консультанти відіграють ключову роль у допомозі компаніям в підвищенні ефективності їх діяльності, розробці стратегій, вирішенні складних проблем . Завдяки своїй експертизі і об'єктивному погляду з-зовні, консультанти можуть донести нові ідеї, кращі світові практики, сприяти впровадженню інновацій та вдосконаленню бізнес-процесів. Важливо підкреслити, що бізнес-консалтинг — це не лише вирішення проблем, але й інвестиція в успіх компанії, забезпечуючи їй конкурентні переваги в сучасному динамічному світі бізнесу.

Однак будь-яка діяльність починається з правового регулювання. Чим же є консалтинг в існуючій в Україні законодавчій та нормативній базі? Визначення консалтингу, консалтингових послуг - немає. Наприклад, є визначення маркетингових послуг, що може бути близьким до консалтингу. Маркетингові послуги - це послуги, надані фахівцями у сфері маркетингу, що полягають у наданні порад, розробці стратегій та впровадженні ефективних маркетингових рішень для підприємств. Консультанти в цій галузі допомагають компаніям аналізувати їх маркетингові потреби, визначати цілі та розробляти плани дій, спрямовані на досягнення стратегічних бізнес-цілей. Вони можуть працювати в різних напрямках, включаючи цифровий маркетинг, аналітику та стратегічне планування, сприяючи покращенню ефективності маркетингових зусиль компаній

[2]. Однак, їх коло досить широке й часто виходить за межі консультування. Із бізнес-консалтингом їх пов’язує хіба що розробка системи можливих ефективних рішень та їх впровадження, участь у формуванні стратегій.

Якщо спиратися на визначення вітчизняних науковців, пов’язаних з дослідження бізнес-консалтингу, можна відзначити визначення О. Марченко. Вона формує поняття бізнес-консалтингу як діяльність консультантів різних спеціалізацій з метою надання компетентних послуг відповідно до запиту клієнта. Кінцева задача таких послуг – вирішення явних та прихованих проблем клієнта, для зміцнення його конкурентоспроможності та покращення фінансового стану. Бізнес-консультанти, за її визначенням, провадять підприємницьку діяльність [3].

Проте, визначення американського професора Е.Верландера є більш узагальнюючим та обширним: «Консультування є стратегічним заходом, який дозволяє людям і організаціям краще адаптуватися до мінливих умов середовища». В своїй книжці «Практика професійного консультування» він зосереджує увагу на питанні управлінні змінами. Зміни є джерелом життєвої сили консалтингу, оскільки організації виживають лише завдяки успішним змінам. Реальність цієї взаємної потреби лежить в основі суті консалтингу. Консультанти вирішують проблеми, створені могутніми силами змін у середовищі організації, і таким чином самі створюють зміни [43].

За допомогою використання класифікації видів економічної діяльності можна виокремити секції видів діяльності, що можуть відносяться до бізнес-консалтингу. Найбільш популярні на українському ринку консультаційних послуг було проаналізовано в таблиці 1.1. В ній представлено основні показники надання консультаційних послуг в Україні за 2019–2021 роки. Наведені дані в таблиці 1.1 дозволяють зрозуміти орієнтовні щорічні обсяги доходів, які охоплюють обрані

види консалтингових послуг. Проте варто зауважити, що вони є орієнтовними та не відображають повноту всіх реальних показників.

Таблиця 1.1

Обсяг реалізованих консультаційних послуг в Україні

у 2019 – 2021 рр., млн. грн

Назва виду послуги	Код за КВЕД	2021 р.	2020 р.	2019 р.
Діяльність у сфері бухгалтерського обліку й аудиту; консультування з питань оподаткування	69.2	1038.7	787.1	1445.2
Консультування з питань керування	70.2	697.6	649.3	643.0
Діяльність у сферах архітектури та інжинірингу, надання послуг технічного консультування	71.1	2757.7	2292.8	2395.6
Дослідження кон'юнктури ринку та виявлення громадської думки	73.2	637.7	1308.4	513.4

Джерело: розроблено автором за даними [4] та [5]

Ринок консалтингових послуг в Україні сформувався у період після отримання незалежності в 1991 році. В свою чергу ринок консалтингових послуг - це економічний сегмент, де фахівці-консультанти надають свої послуги підприємствам, організаціям та іншим клієнтам з метою покращення їхнього бізнесу чи вирішення конкретних завдань. Цей ринок включає в себе широкий спектр послуг, які можуть охоплювати різні аспекти управління, стратегічного планування, фінансів, маркетингу, технологій, правової підтримки, управління змінами, розвитку персоналу та інше. Консультанти працюють в ролі зовнішніх експертів, надаючи клієнтам професійні поради та допомагаючи вирішувати

стратегічні, операційні та управлінські завдання. Послуги консультантів можуть бути тимчасовими та направленими на вирішення конкретних проблем, або довгостроковими, охоплюючи стратегічне партнерство та комплексне вдосконалення бізнес-процесів. Основні види консалтингових послуг включають: управлінський консалтинг, фінансовий консалтинг, інформаційно-технологічний консалтинг, маркетинговий консалтинг, кадровий консалтинг, правовий консалтинг, податковий консалтинг. Відтак ринок консалтингових послуг постійно розширюється та адаптується до змін у бізнес-середовищі та технологічних тенденцій.

Період 1990-х років в Україні був періодом значних економічних трансформацій та переходу від планової до ринкової економіки. Процес відокремлення від СРСР, отримання незалежності та впровадження нових економічних та правових систем супроводжувався численними викликами та невизначеністю. У такому контексті підприємства потребували професійного консалтингу. Ринок консалтингових послуг активно розвивався як за рахунок створення нових українських консалтингових компаній, так і за рахунок приходу на вітчизняний ринок міжнародних лідерів у цій сфері [6].

В Україні налічується близько 300 українських компаній, що спеціалізуються на бізнес-консалтингу. За основними рейтингами до лідерів українського ринку відносять: Baker Tilly, EBS, Pro-Consulting, Nota Group, Firm.ua, Innova Group, Key Solutions [7]. Активно завоювали ринок консалтингових послуг з 90-х років і компанії «Великої четвірки», що займають більшу частку ринку консалтингових послуг.

На ринку консалтингових послуг в Україні спостерігається значний розвиток. З одного боку, це викликано різноманіттям нових бізнес-можливостей та необхідністю ефективного впровадження стратегій у відповідь на зростання

конкуренції. Спостерігається великий попит на консалтингові послуги з боку підприємств, які прагнуть вирізнятися та досягти успіху в умовах постійних змін. З іншого боку, розквіт технологій, включаючи цифровізацію діяльності підприємств, спонукає менеджмент шукати спеціалізовану експертизу саме в консультантах. Зміцнення конкурентної боротьби в галузі також відбувається через глобалізацію бізнесу та розвиток міжнародних відносин. Також, спостерігається тенденція консолідації ринку, де поглинання та придбання інших консалтингових компаній призводять до появи сильніших та більш конкурентоздатних утворень. Важливим фактором в посиленні конкурентної боротьби є також підвищення кваліфікацій консультантів та їхня готовність до постійного професійного розвитку. Ті консалтингові компанії, які можуть швидко реагувати на зміни та пропонувати інноваційні стратегії, стають лідерами на ринку, забезпечуючи собі перевагу в мінливому середовищі.

Міжнародні компанії «Великої четвірки» демонструють домінування на сучасному ринку консалтингових послуг і фактично визначають політику консалтингової індустрії України. Прикладом такої активної експансії виступають: EY, PwC, KPMG, Deloitte. Велика четвірка вирізняється своєю глибокою експертизою та високим рівнем професійності в області консалтингу. Ці компанії не просто виконують завдання, вони визначають стандарти у своїй галузі, надаючи клієнтам не тільки послуги, але і стратегічні рішення для подальшого розвитку. Крім класичного аудиту, вони активно проводять податкове планування, фінансовий консалтинг, розробку стратегій та впровадження технологічних рішень. Це дозволяє компаніям отримувати комплексне обслуговування, охоплюючи всі аспекти управління. Завдяки своїм глобальним ресурсам та представництвам в різних країнах, ці компанії можуть забезпечити клієнтам підтримку на міжнародному рівні та допомогти їм адаптуватися до різних ринкових умов. Велика четвірка завжди на передових позиціях у впровадженні

новітніх технологій та використанні аналітичних інструментів для забезпечення більш точного та ефективного аудиту, аналізу фінансів та стратегічного планування.

1.2 Сутність та особливості сфери кібербезпеки в Україні

Кібербезпека в сучасному світі стала важливою та невід'ємною складовою суспільного та економічного розвитку. Україна, як і багато інших країн, постала перед багатьма викликами, пов'язаних із кіберзагрозами. Зростання кількості та складності кібератак, крадіжки конфіденційної інформації, а також інші форми кіберзлочинності створюють необхідність у розбудові ефективної системи кібербезпеки.

В даному контексті важливо розглядати сферу кібербезпеки в Україні як стратегічну складову, яка впливає на різноманітні сфери, включаючи економіку, національну безпеку та захист особистих даних громадян. Зростання залежності від інформаційних технологій вимагає постійного удосконалення заходів кіберзахисту, а також розвитку кадрового потенціалу в цій галузі. Важливо вивчати сутність та особливості сфери кібербезпеки в Україні не лише, розглядаючи організаційну структуру, методи та технології захисту, а також і роль державних та приватних суб'єктів у забезпеченні кібербезпеки країни. Висвітлення цих аспектів дозволить краще зрозуміти виклики, перед якими стоїть Україна у сфері кібербезпеки, та розробити ефективні стратегії для захисту кіберпростору країни.

Ринок кібербезпеки - це динамічна та важлива галузь, що об'єднує різноманітні суб'єкти та процеси для захисту інформації та комп'ютерних систем від кіберзагроз [44].

Ключові складові ринку кібербезпеки:

1. Підготовка кадрів. Заклади вищої освіти виконують важливу функцію у підготовці кадрів для сфери кібербезпеки. Студенти, які отримують освіту в галузі кібербезпеки, стають експертами, готовими вирішувати завдання з захисту інформації.

2. Роботодавці та компанії. Індустрія кібербезпеки включає велику кількість роботодавців і компаній, що надають послуги забезпечення кібербезпеки. Це можуть бути фахові служби безпеки, розробники програмного забезпечення, консультанти з кібербезпеки та інші.

3. Дослідження та інновації. Науково-дослідницька діяльність має суттєвий вплив на впровадження нових технологій та підходів у сфері кібербезпеки. Дослідження можуть бути проведені в закладах вищої освіти, дослідницьких центрах та приватних компаніях.

4. Законодавство та нормативна база. Законодавство і нормативні акти визначають правила та стандарти для забезпечення кібербезпеки на рівні країни та міжнародному рівні [8].

5. Міжнародні організації. Організації та агенції, такі як INTERPOL, Європейська агенція з кібербезпеки (ENISA) та інші, займають важливе місце у співпраці та обміні інформацією між країнами для боротьби з міжнародними кіберзагрозами [45].

Ці складові взаємодіють, створюючи багатоаспектний ринок кібербезпеки, який реагує на постійні зміни у кіберзахисті та забезпечує безпеку інформації на різних рівнях.

Розвиток ринку кібербезпеки в Україні має велике стратегічне значення з ряду причин. Україна знаходиться в складній геополітичній ситуації, і кіберзагрози можуть використовуватися для атак на національні інтереси. Розвинені системи

кібербезпеки є необхідним елементом оборони держави. Захист національної безпеки України у сфері кібербезпеки визначається тим, що кіберзагрози стають критично важливим елементом гібридної війни, що використовується для впливу на політичні та військові рішення країни. Кібершпигунство стає одним із основних елементів захисту національних інтересів, адже державні структури використовують кіберрозвідку для здобуття конфіденційної інформації щодо стратегічних питань, військових планів та можливих загроз. Захист електронної системи управління та оборонних потужностей важливий для забезпечення функціонування країни в умовах електронної залежності та автоматизації [9]. Витік чи порушення даних інформаційних систем може призвести до серйозних наслідків для національної безпеки. Дуже важливою складовою сфери кібербезпеки є активний розвиток кіберзахисту об'єктів критичної інфраструктури, таких як енергетика, транспорт та телекомунікації. Атаки на ці об'єкти можуть призвести до великих збитків та порушення нормального функціонування держави. Важливо розробляти і впроваджувати стратегії кіберзахисту на рівні країни, сприяти освіті та навчанню в сфері кібербезпеки, а також активно співпрацювати з міжнародними партнерами для обміну інформацією та спільної боротьби з кіберзагрозами [46].

В умовах цифрової економіки захист від кіберзагроз стає ключовим фактором економічної стабільності. Кібератаки можуть викликати серйозні фінансові втрати для підприємств та завдати шкоду економічному розвитку країни. В умовах цифрової трансформації та активного використання інформаційних технологій для ведення бізнесу, через наслідки кібератак економічна стійкість України може бути під серйозним ударом через можливі серйозні фінансові втрати для підприємств та економіки в цілому. Кібератаки можуть призвести до витоку важливих комерційних даних, втрати фінансових активів та порушення інтелектуальної власності, що загрожує конкурентоспроможності компаній [10]. В свою чергу, критична інфраструктура, така як енергетика, транспорт та інформаційні системи,

взаємопов'язана і формує собою велику, ба більше, найважливішу частину економіки. Економічна стійкість залежить і від ефективності кіберзахисту в банківській сфері, яка обробляє великі обсяги фінансових транзакцій. Атаки на банківські системи можуть призвести до витоку особистих фінансових даних та збитків для клієнтів та банків. Також важливо врахувати цілісність та конфіденційність інформації. Забезпечення ефективної кібербезпеки є важливим для збереження довіри громадськості та іноземних інвесторів. Витік конфіденційної інформації, особливо в сфері електронного урядування та онлайн-сервісів, може підірвати довіру та викликати збитки для бізнесу та іміджу країни[11]. В контексті економічної безпеки варто звернути увагу на те, що у світі, де технологічні засоби визначають економічний прогрес, інновації та розробка нових технологій у сфері кібербезпеки визначають загальну конкурентоспроможність. Кібернетичний захист високотехнологічних виробництв, дослідницьких центрів та інноваційних стартапів є ключовим для забезпечення сталого економічного зростання [12].

З усіх складових ринку кібербезпеки в Україні, варто особливу увагу звернути на те, що є основою для якісного його функціонування – фахівці з кібербезпеки.

Навчання майбутніх фахівців з інформаційної та кібербезпеки у закладах вищої освіти може вважатися однією з ключових складових, яка вносить свій вклад у розвиток ефективного ринку кібербезпеки. Підготовка кадрів у галузі кібербезпеки є важливою його складовою. Заклади вищої освіти грають ключову роль у формуванні експертів, здатних формувати та реалізовувати стратегії захисту в інформаційних системах. Здобувачі освіти отримують фундаментальні знання з комп'ютерних наук, криптографії, мережевої безпеки та інших важливих областей. Крім теоретичних аспектів, практичні навички важливі для розвитку професіоналізму та високої компетенції. Вони можуть набувати практичний досвід через лабораторні роботи, стажування та участь у заходах з кібербезпеки. Важливо також зазначити, що зростання інтересу до спеціальності 125 «Кібербезпека та

захист інформації» в закладах вищої освіти свідчить про зростання усвідомлення абітурієнтами важливості цієї галузі. Успішно завершивши навчання, випускники стають важливим резервом для компаній та різноманітних установ, які зацікавлені у висококваліфікованих кадрах в сфері кібербезпеки та захисту інформації. Отримавши відповідні знання та навички випускники щороку стають джерелом розвитку цього сектору. Підготовлені кадри можуть працювати в ролі аналітиків, адміністраторів мереж, етичних хакерів, консультантів з кібербезпеки тощо. Система підготовки кадрів у закладах вищої освіти є критично важливою для зміцнення захисту інформації та інфраструктури в цифровому світі.

1.3 Роль консалтингу у забезпеченні господарської діяльності.

У високотехнологічному середовищі сучасної господарської діяльності проблема забезпечення кібербезпеки стала першочерговим завданням. Із загостренням небезпеки від кіберзагроз, що постійно зростають відповідно до розвитку інформаційних технологій, консалтинг у сфері кібербезпеки стає стратегічно необхідним компонентом організаційного управління.

Ключовою місією консультантів у галузі кібербезпеки є систематичний аналіз потенційних загроз та вразливостей, що можуть виникнути в інформаційному просторі. Консультанти активно залучаються до оцінки ризиків та формулювання стратегічних заходів з метою усунення чи зменшення впливу потенційних кіберзагроз. До сфери компетенції консультантів також входить впровадження передових технологічних рішень, спрямованих на підвищення рівня безпеки інформаційних систем. Вони активно працюють над вдосконаленням інфраструктури безпеки, впровадженням шифрування та систем контролю доступу. Ба більше, консультанти ведуть навчання персоналу з питань

кібербезпеки, сприяючи формуванню внутрішньої культури безпеки в організації. У цьому контексті, внесок консалтингу визначається не лише реакцією на існуючі загрози, але й прогнозуванням потенційних атак у майбутньому.

Питання, з якими стикаються консультанти, часто є складними, пов’язаними з процесами, що знаходяться в самому серці стратегії та мети організації. Таким чином, консультування є важливим та дуже відповідальним завданням. Тому окрему увагу слід приділити питанню стратегії.

Формування стратегії — це складний процес, який включає в себе кілька ключових етапів. Нижче подано загальний огляд етапів формування стратегії.

1. Аналіз середовища. Перший етап полягає в оцінці зовнішнього та внутрішнього середовища. Зовнішній аналіз включає вивчення ринку, конкурентів, економічних та технологічних тенденцій. Внутрішній аналіз спрямований на визначення сильних та слабких сторін організації.

2. Визначення місії та візії. Визначення чіткої місії (сутності існування організації) та візії (очікуваного майбутнього стану) допомагає встановити цільові орієнтири для стратегії.

3. Формулювання цілей та завдань. Цілі мають бути чіткими та досяжними, а завдання — конкретними кроками для досягнення цих цілей. Це допомагає правильно та ефективно спрямувати зусилля команди.

4. Вибір стратегії. На основі аналізу формулюються варіанти стратегій. Це може включати в себе вибір конкурентної стратегії (наприклад, лідерство в галузі чи диференціація) та інші стратегічні напрямки.

5. Розробка та виконання планів. Створюються конкретні плани дій для реалізації обраної стратегії. Це може включати в себе розробку детальних бізнес-планів, маркетингових стратегій та інших планів.

6. Моніторинг та контроль. Процес стратегічного управління вимагає постійного моніторингу реалізації стратегії та вжиття заходів для виправлення негативних факторів чи непередбачених обставин.

7. Оцінка та зміни. Після виконання стратегії проводиться оцінка результатів. Якщо цілі не досягнуті, можливий перегляд та зміна стратегії.

Ці етапи можуть відрізнятися залежно від конкретного підходу та контексту організації. Важливо також зауважити, що формування стратегії — це гнучкий процес, і організації можуть регулювати свої стратегії відповідно до змін у середовищі [18].

Розглянемо консалтингові послуги аналітичного типу, що стануть основою для виконання завдань цієї роботи. Переважна частина даних завдань пов’язані з першим етапом формування стратегії – аналізом середовища. Аналітика виступає важливим інструментом прийняття рішень, допомагаючи керівникам компаній адаптуватися до змін у ринкових умовах, оптимізувати бізнес-процеси та досягати стратегічних цілей [21].

Важливість консалтингових послуг аналітичного типу у сучасному бізнес-середовищі важко переоцінити. Аналітичний консалтинг виступає важливим інструментом для підтримки стратегічного розвитку та досягнення успіху підприємств. Ось деякі ключові аспекти важливості таких послуг:

1. Інформовані рішення:
   - Консультанти, які спеціалізуються на аналітиці, надають підприємствам інсайти на основі об'єктивних даних та глибокого аналізу.
   - Забезпечують керівництво інформацією, яка необхідна для прийняття обґрунтованих стратегічних рішень.
2. Адаптація до змін:

- Допомагають керівникам підприємств ефективно реагувати на зміни внутрішнього та зовнішнього середовища.
- Аналізують тренди та прогнозують можливі виклики, допомагаючи керівникам компаній підготуватися до змін.

3. Оптимізація бізнес-процесів:
   - Використовують аналітичні інструменти для ідентифікації можливостей оптимізації та покращень у внутрішніх процесах.
   - Допомагають підприємствам досягти ефективності та знизити витрати.
4. Фінансовий успіх:
   - Забезпечують точний фінансовий аналіз, допомагаючи розробити стратегії для підвищення прибутковості та управління фінансами.
   - Визначають оптимальні інвестиційні можливості.
5. Ризик-менеджмент:
   - Ідентифікують потенційні ризики та розробляють стратегії їхнього управління.
   - Знижують вірогідність негативних наслідків для підприємства.
6. Конкурентоспроможність:
   - Сприяють розробці маркетингових стратегій, ґрунтуючись на аналізі ринку та конкурентів.
   - Забезпечують керівників підприємства інструментами для збереження або підвищення його конкурентоспроможності.
7. Інновації:
   - Сприяють впровадженню інновацій та новітніх технологій через стратегічний аналіз потреб підприємства та його готовності до змін.

Усі ці аспекти консалтингових послуг аналітичного типу спрямовані на досягнення стратегічних цілей підприємства, оптимізацію внутрішніх процесів та забезпечення конкурентоспроможності в динамічному бізнес-середовищі.

Аналітичний консалтинг не лише надає компетентний аналіз, а й стає основою для формування та реалізації вдалих стратегій розвитку.

Аналітичний консалтинг є ключовим інструментом для підприємств, бажаючих не лише адаптуватися до змін на ринку, але й активно прогнозувати його розвиток. Він дозволяє приймати обґрунтовані рішення, максимізуючи успішність стратегічних ініціатив і забезпечуючи стійкість у конкурентному середовищі. Цілком зрозуміло, що в сучасному бізнес-середовищі консалтингові послуги аналітичного типу стають необхідністю для підприємств будь-якого розміру та галузі. Аналітичний консалтинг дозволяє підприємствам виходити за межі стандартних стратегій та приймати рішення на основі глибокого розуміння їхнього внутрішнього потенціалу, внутрішнього та зовнішнього середовища. Сучасне підприємство, яке прагне досягти конкурентоспроможності та інновацій, повинно не лише виявляти проблеми, але й передбачати можливості. Аналітичні консультанти забезпечують відповіді на ключові питання, що стосуються стратегічного розвитку, ефективного управління ресурсами та взаємодії з ринковими трендами [22].

Варто звернути увагу і на оцінку якості консалтингових послуг. У професійному співтоваристві і у клієнтів не склалося чітких уявлень про те, що таке якість консалтингових послуг, які критерії їх оцінки. Якість консалтингових послуг – поняття суб'єктивне, оскільки кожен клієнт і консультант мають свої поняття якості і цінності консультування. Воно обумовлене ефективною побудовою стосунків клієнта і консультанта. Крім того, кінцевий продукт консультування – це порада, реальне впровадження або зміна, яка має місце в організації.

Підсумовуючи, консалтингові послуги аналітичного типу не тільки структурують інформацію для кращого прийняття рішень, але й стимулюють

бізнес до постійного вдосконалення та адаптації. Вони формують основу для стратегічного планування, допомагаючи підприємствам визначити своє місце в ринковому ландшафті та максимізувати свій потенціал розвитку. Таким чином, консалтингові послуги аналітичного типу стають ключовим інгредієнтом успіху та стійкості сучасних підприємств.

Аналіз професійних та гнучких навичок бізнес-консультантів

Аналіз професійних та гнучких навичок бізнес-консультантів слід починати з визначення принципу та структури їх роботи. Робота бізнес-консультанта значною мірою відрізняється від стандартних видів діяльності, де чітко прописані посадові вимоги та обов'язки [13]. Основна діяльність більшості консультантів сконцентрована на чотирьох головних постулатах, зображених на малюнку 1.

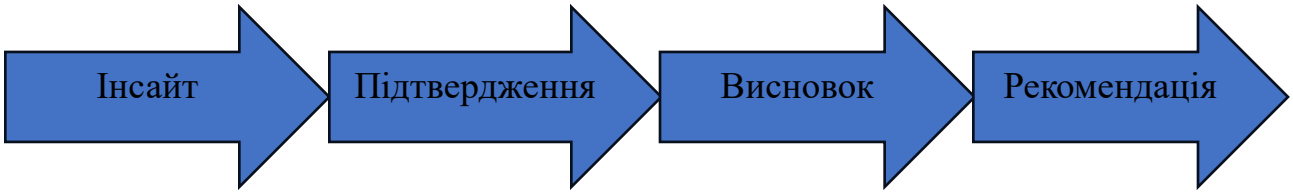

Рисунок 1.1 Типова задача консультанта

Джерело: розроблено за даними [14]

Роль консультантів полягає в тому, щоб допомагати керівникам компаній знаходити рішення для їхніх стратегічних та операційних задач. У цій ролі консультанти служать агентами змін, ставлячи правильні запитання, визначаючи актуальні проблеми, збираючи та аналізуючи факти, розробляючи план дій, шукаючи рішення та консультуючи щодо їх реалізації.

На початку виконання проєкту дуже важливо, при проведенні колективних та персональних мозкових штурмів, сконцентрувати свою увагу на знаходженні ідей,

інсайтів, здогадок щодо причини виникнення тієї чи іншої проблеми клієнта, або можливі шляхи вирішення проблем які стоять перед консультантом для ефективного виконання проєкту. Це є ключова і чи не найголовніша задача будь-якого консультанта. На виокремлених та структурованих інсайтах, здогадках, ідеях будується весь подальший проєкт та залежать всі висновки та рекомендації які будуть надаватися. До цього етапу важливо залучати всіх учасників проєктної команди. Таке колективне залучення дозволить сформувати більшу кількість пропозицій з максимально можливою неупередженістю за рахунок диверсифікації світоглядів та різноманітністю думок [15]. Також, це є важливим складником побудови активно налаштованої команди, адже кожен її член з самого початку бере участь в розробці стратегічних рішень. Проте варто звернути увагу на важливу роль керівника команди. Він має з неупередженістю валідувати озвучені інсайти та ідеї, щоб в кінці залишити тільки найбільш точні та перспективні для подальшої роботи. В кінці завжди має бути сформований чіткий висновок по виконаному проєкту у відповідності до сформованої мети на початку проєкту. Також, важливою особливістю роботу консультантів є формування рекомендацій для клієнта. Беручи їх до уваги, клієнт підвищить свої шанси щодо успішного виконання трансформації в своїй компанії чи установі та підвищення ефективності подальшого функціонування даних трансформацій [16].

Щоб підтвердити інсайт, думку чи ідею, консультант має володіти необхідними професійними компетенціями. В залежності від напряму діяльності консультанта відрізняється перелік необхідних компетенцій, якими він має володіти. Попри різні напрями діяльності, консультант повинен володіти і різними методами та інструментами управління, зокрема стратегічного. Наприклад, разом із застосуванням традиційних інструментів (SWOT-аналіз, PEST-аналіз тощо) консультант повинен оволодівати передовими прогресивними методиками, які дають нові можливості для більш ефективного опрацювання та представлення

даних. При умові ефективного оволодіння різними методиками, можна розраховувати на максимальну доцільність в підборі методів консультування [17].

В даному дослідженні робота була аналітичною, тому з професійних навичок слід виділити наступні:

1. Володіння аналітичними інструментами MS Excel та Power BI
2. Володіння інструментами збору інформації Google Forms, KoboToolbox

Попри звичайні професійні обов'язки, особливу увагу приділяють гнучким навичкам бізнес-консультантів. Переважна більшість всієї роботи консультанта — це спілкування із замовниками та їхніми співробітниками. Дуже важливим складником успішного виконання завдань проєкту є вміння грамотно вибудовувати комунікацію як всередині компанії, так із замовником та його представниками. Важливість гнучких навичок в роботі консультанта визначається сучасним характером бізнес-середовища, яке вимагає від фахівців високого рівня адаптації та вміння ефективно пристосовуватися до змін [18]. Консультант повинен бути здатний адаптувати свій підхід до різноманітних ситуацій та уміти швидко реагувати на зміни в обставинах. Гнучкість дозволяє знаходити творчі та ефективні рішення навіть у складних випадках, де просте рішення не очевидне. Консультант повинен ефективно взаємодіяти з різними типами клієнтів, колег, та іншими зацікавленими сторонами. Вміння адаптувати стиль комунікації до різних аудиторій сприяє побудові ефективних відносин та забезпечує високий рівень ясності та розуміння думок консультанта. В цілому, гнучкі навички є важливою основою для успішної роботи консультанта, оскільки вони дозволяють ефективно функціонувати в динамічному, та часто складному, середовищі, ефективно взаємодіяти з різними стейкхолдерами та досягати очікуваних результатів [19].

Варто виокремити важливу та характерну для українського ринку консалтингових послуг проблему. Основна проблема замовників консалтингових

послуг в Україні – невпевненість у кваліфікації, здібностях та глибини знань у людей, які будуть консультувати їх по діяльності їх же бізнесу або установи. У підсумку консультантам досить складно інтегруватися в компанію або установу клієнта настільки грунтовно, щоб бути максимально ефективним замовнику. Представники бізнесу слабо довіряють стороннім фахівцям, відчувають страх перед передачею процесу управління зовнішнім консультантам. Водночас, консультанти часто чітко не розуміють, якого ефекту можна досягти за допомогою їхньої діяльності [20].

Висновки до розділу 1

Теоретичні основи формування консалтингових послуг в Україні вказують на динамічний розвиток цього сектору у країні. Попит на консалтинг стабільно зростає, і компанії все більше визнають важливість експертної допомоги в управлінні стратегією та оптимізації бізнес-процесів. Інтеграція з міжнародними стандартами стає ключовим елементом для забезпечення високої якості консалтингових послуг. Важливим напрямком розвитку є не лише розширення спектру послуг, але й перехід від традиційного уявлення про консультанта як експерта до ролі стратегічного партнера. Консалтинг в Україні стає не лише послугою, але й активною співпрацею, спрямованою на досягнення успіху та вирішення складних завдань бізнесу.

Професійність бізнес-консультанта визначається сильними аналітичними та стратегічними навичками, здатністю ефективно спілкуватися та пристосовуватися до змін. Гнучкість у роботі, високий рівень комунікацій та етичні стандарти є ключовими факторами успіху. Компетентний консультант взаємодіє з клієнтами,

адаптується до нових умов і несе відповідальність за свої рекомендації, що формує довіру та дозволяє досягати успіху в динамічному бізнес-середовищі.

Роль консалтингу у забезпеченні господарської діяльності підприємств є визначальною для їхнього успіху та стійкості в конкурентному середовищі. Консультанти забезпечують експертною підтримкою, спрямованою на оптимізацію стратегій, підвищення ефективності операцій та вирішення конкретних проблем. Основна перевага консалтингу полягає в тому, що він надає об'єктивну та часто не просто передбачувану перспективу ведення господарської діяльності з максимальною ефективністю. Консультанти, володіючи різноманітним досвідом та знаннями, допомагають підприємствам адаптуватися до змін у ринкових умовах, розробляючи стратегії росту та впроваджуючи інноваційні підходи.

В свою чергу, ринок кібербезпеки в Україні визначається суттєвими особливостями, що обумовлені особливостями технологічного розвитку та геополітичного контексту країни. Серед ключових особливостей ринку кібербезпеки в Україні варто виділити постійну необхідність адаптації до нових методів кібератак та впровадження передових технологій для захисту інформації. Державні інституції та бізнес-структури активно залучаються до вирішення цих завдань. Співпраця з професійними консультантами та використання їхнього досвіду стає необхідною складовою для підтримки високих стандартів національного кіберзахисту. В цілому, ринок кібербезпеки в Україні є важливим компонентом національної безпеки та високотехнологічного розвитку. Специфіка його функціонування вимагає від учасників гнучкості, інновацій та ефективності для успішного вирішення викликів кіберзагроз та забезпечення стабільності в цифровому середовищі.

РОЗДІЛ 2

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ КОНСАЛТИНГОВОГО ПРОЄКТУ

2.1 Ресурсне забезпечення та етапи реалізації консалтингового проєкту

До компанії звернулася Установа 1, на основі багаторічної співпраці з отримання консалтингових послуг. Вони досліджували глобальні питання, пов'язані з галуззю кібербезпеки України, і потребували професійних консультаційних послуг з аналізу ринку кібербезпеки, який охоплює як попит на цю діяльність так і на пропозицію, яка задовольняє потреби всіх суб'єктів ринку. Роль саме консалтингових послуг в цьому проєкті була дуже значною, адже для успішного виконання поставленого завдання необхідна залученість професіоналів з кібербезпеки, для консультаційної підтримки всіх етапів робіт. Наша компанія як раз мала таку компетенцію та необхідні можливості для задоволення всіх потреб замовника. Кінцевим продуктом даного проєкту має стати з нуля розроблений інструмент за допомогою якого можна глибоко та з максимально можливою об'єктивністю оцінювати попит та пропозицію на ринку кібербезпеки України. Одна з ключових вимог – високо автоматизація інструменту, яка передбачала б мінімум затрат ручного втручання користувачів щодо збирання, аналізу та представлення статистичної інформації як попиту на фахівців з кібербезпеки, так і пропозиції які надає ринок.

Основною метою розробки та створення даного інструменту є можливість оцінки наявних трудових ресурсів на ринку кібербезпеки України.

Дана оцінка відбуватиметься на основі даних, зібраних від закладів вищої освіти (ЗВО), які готують спеціалістів зі спеціальності 125 Кібербезпека та захист

інформації щодо пропозиції даних спеціалістів. Окрім того, у даному інструменті для аналізу також мають використовуватися дані щодо попиту на спеціалістів з кібербезпеки, які представлені як вакансії, які розміщують роботодавці, в пошуках спеціалістів з кібербезпеки на відповідних джерелах даних.

Основні цілі та завдання даного інструменту полягають у наступному:

- Оцінити обсяг ринку спеціалістів зі спеціальності 125 “Кібербезпека/Кібербезпека та захист інформації” протягом 2018-2022 років
- На основі отриманих даних та аналізу побудувати зрозумілу у користуванні детальну візуалізацію в Power BI для аналізу та прийняття подальших рішень.

У результаті створення даного інструменту кінцевий користувач отримає актуальний та детальний аналіз попиту та пропозиції ринку спеціалістів з кібербезпеки за 2018-2022 роки з можливістю проведення аналогічного дослідження у майбутньому. Створений інструмент буде зручним та зрозумілим у користуванні як і тим, хто має мінімальний досвід користування Power BI, так і просунутим користувачам.

Ресурсне забезпечення реалізації консалтингового проєкту

Першим кроком для формування переліку використаних технологій є опис мінімальних технічних вимоги до обладнання, за допомогою яких можливе виконання роботи та представлення результатів даного дослідження.

1. Процесор: 1,5 ГГц або вище, x86- або x64-розрядний.
2. Оперативна пам’ять: 1 ГБ (32-розрядна) або 2 ГБ (64-розрядна) або більше.

3. Дисплей: Мінімальна роздільна здатність 1024 x 768 пікселів.

4. Операційна система: Windows 10, Windows 8.1, Windows 8 або Windows 7 (SP1).

Перелік використаних програмних продуктів

Power BI та області його застосування в даному дослідженні:

- підключення через API до джерел даних;
- об'єднання і приведення інформації в єдину стандартизовану модель даних;
- обчислення необхідних параметрів на основі цих об'єднаних даних;
- побудова візуальних графіків, звітів [47].

Microsoft Excel та області його застосування в даному дослідженні:

- В Excel створювались різні види графіків і діаграм, які беруть дані для побудови з комірок таблиць;
- Excel використовувався як спосіб вивантаження статистичних даних;
- Excel містить багато математичних і статистичних функцій, завдяки чому його використовували для різноманітних розрахунків та прогнозів [52].

Microsoft Word та його області застосування в даному дослідженні:

- Введення, форматування та редагування тексту;
- Представлення результатів аналітичного огляду необхідних матеріалів [49];

KoboToolbox — це платформа для збору польових даних у складних умовах. Користувачі платформи варіюються від урядових організацій, пошуково-рятувальних команд, агентств ООН, великих і малих неурядових організацій до організації спеціалізованих на бізнес-консультаціях, бухгалтерських фірм.

З допомогою KoboToolbox було розроблено цифрові форми збору даних, які працюють як на мобільних пристроях, так і в веб-браузерах. Створення форм відбувалось за використанням специфікації XLSForm для забезпечення гнучкості при створенні більш складних і функціональних форм.

KoboToolbox дозволяє керувати даними, об’єднуючи їх. Потім ці дані можна завантажити в різних форматах для використання в програмах, таких як Excel, Power BI та інші. Можливо отримати доступ до даних просто завантаживши їх [50].

Нормативно-правовою основою для виконання консалтингового проєкту стали:

- Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру [23]
- Закон України "Про інформацію" [24]
- Закон України "Про доступ до публічної інформації" [25]

Опис виконаних робіт у розрізі етапів реалізації консалтингового проєкту

На початку виконання робіт була сформована команда з фахівців консультантів. За кожним із них був встановлений певний спектр роботи, з відповідними обов’язками та зонами відповідальності. Всі співробітники були підзвітні проєктному менеджерові, який, в свою чергу підзвітний партнеру компанії.

Розробка інструменту для оцінки потенціалу кадрів у секторі кібербезпеки включала наступні кроки:

1. Були зібрані первинні дані про кількість студентів, які навчалися за різними спеціальностями з кібербезпеки в Україні протягом 2018-2022 років, а також про студентів, які зараз навчаються у ЗВО України;
2. Розроблена архітектура інструментальної бази даних для обробки та аналізу зібраних даних;
3. Розроблений спеціальний інструмент для оцінки потенціалу робочої сили у секторі кібербезпеки на основі зібраних даних;
4. Проведений статистичний аналіз за допомогою інфографіки на основі зібраних даних за 2018-2022 рр. щодо оцінки потенціалу робочої сили у секторі кібербезпеки;
5. Розроблена Інструкція для користувачів щодо роботи в базі даних, процесу збору даних, завантаження даних до бази даних і оновлення налаштованого інструменту для оцінки потенціалу робочої сили;

Для того, щоб обрати необхідні ЗВО для отримання даних щодо особливостей навчального процесу на спеціальності 125 Кібербезпека та захист інформації були виконані наступні завдання:

1. Проаналізовано перелік ЗВО, які пропонують навчальні програми з кібербезпеки;
2. Обраховано частку кожного ЗВО в загальній кількості здобувачів;
3. Визначено пріоритетність списку найкращих закладів вищої освіти;
4. Затверджено перелік відібраних ЗВО в таблиці 1.1.

Таблиця 2.1

Список обраних ЗВО

№	Назва ЗВО	Частка кількості здобувачів
1	Національний авіаційний університет	10.63%
2	Національний університет 'Львівська політехніка'	8.73%
3	Державний університет інформаційно-комунікаційних технологій	8.48%
4	Харківський національний університет радіоелектроніки	6.74%
5	Національний технічний університет України 'Київський політехнічний інститут імені Ігоря Сікорського'	4.63%
6	Національний технічний університет 'Дніпровська політехніка'	3.79%
7	Вінницький національний технічний університет	3.57%
8	Київський національний університет імені Тараса Шевченка	2.99%
9	Державний торговельно-економічний університет	2.93%
10	Харківський національний університет внутрішніх справ	2.37%
11	Державний університет інтелектуальних технологій і зв'язку	2.30%
12	Національний університет 'Одеська політехніка'	2.25%
13	Приватний вищий навчальний заклад 'Європейський університет'	2.23%
14	Західноукраїнський національний університет	2.08%

Джерело: розроблено автором за даними [26]

Продовження таблиці в Додатках.

Для того, щоб отримати якісні та релевантні дані від ЗВО, необхідно якісно, чітко та зрозуміло підготувати можливі запитання. Для цього були виконані наступні завдання:

1. Підготовлено попередній шаблон із запитаннями для збору даних від ЗВО;
2. Проведено консультації щодо переліку запитань з вибраними ЗВО;
3. Оновлено перелік запитань за результатами обговорення;
4. Затверджено підготовлений шаблон з замовником;
5. Надіслано затверджений шаблон до обраних ЗВО;
6. Перевірено повноту даних після отримання відповідей.

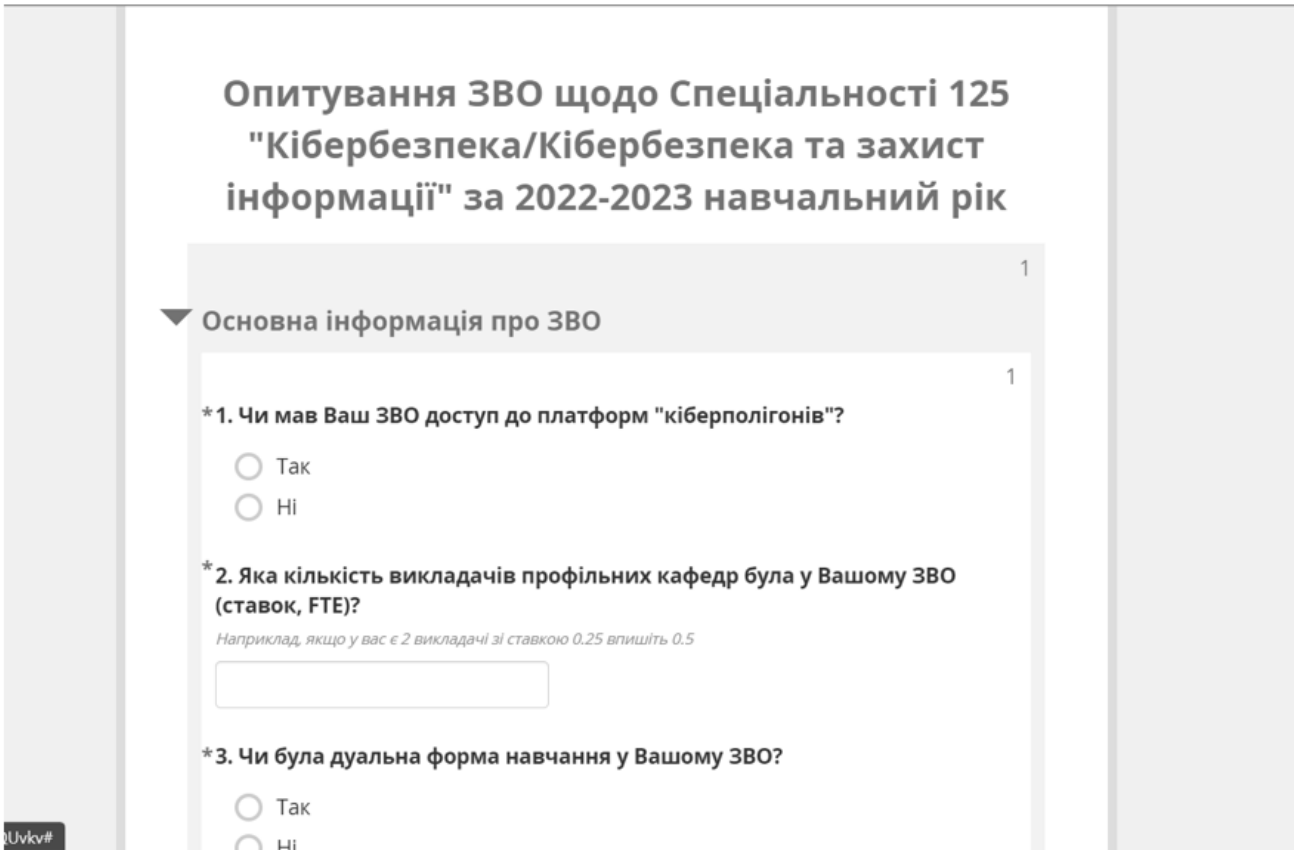

Рисунок 2.1 Зразок шаблону опитувальника для ЗВО

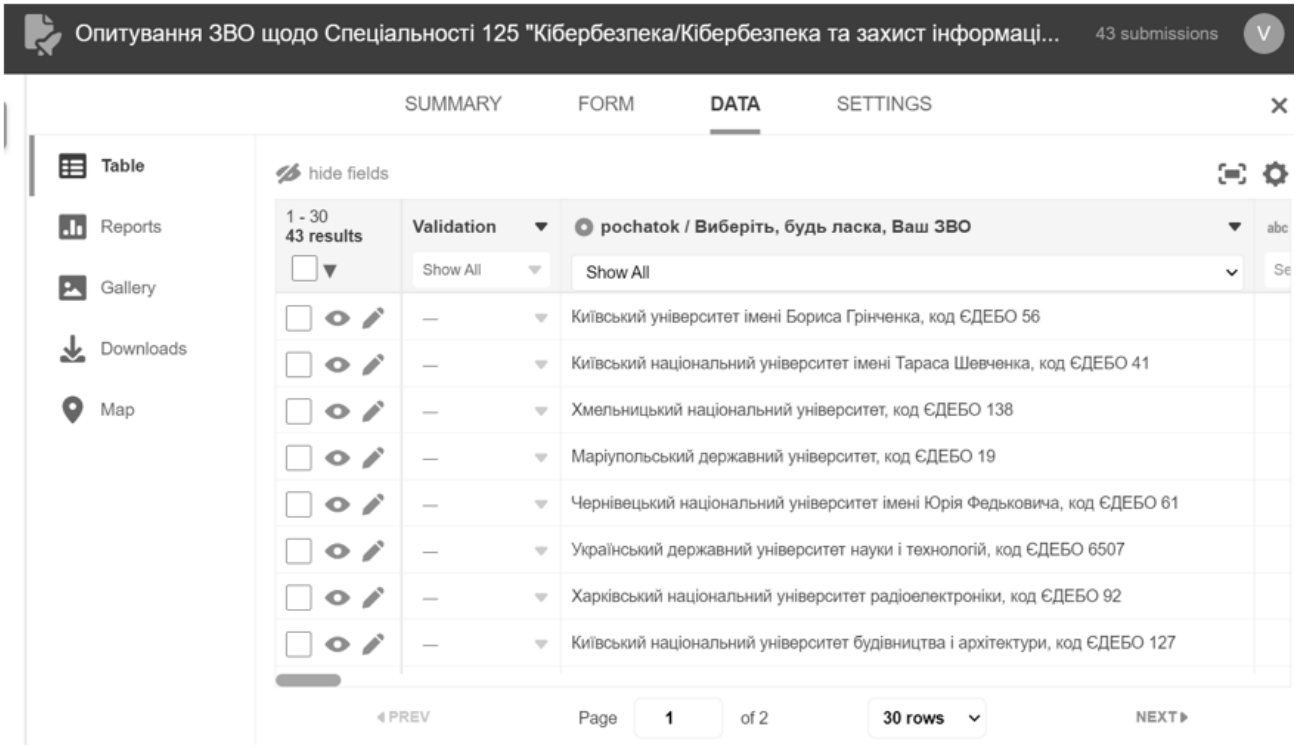

Рисунок 2.2 Частина отриманих відповідей від ЗВО

Для того, щоб отримати необхідні дані, на основі яких можливо робити аналітичні висновки щодо попиту було виконано ряд ключових завдань:

1. Визначено та затверджено підхід до збору даних про попит;
2. Направлено запит до Джерела 1 щодо інформації про попит;
3. Направлено запит до Джерела 2 щодо інформації про попит;
4. Направлено запит до Джерела 3 щодо інформації про попит;
5. Отримано необхідні дані.

Для ефективного використання зібраних статистичних даних були виконано ряд важливих кроків:

1. Проаналізовано зібрані дані;
2. Виконана нормалізація зібраних даних;
3. Визначено зв’язки між різними об’єктами даних у базі даних;

4. Організовано мозковий штурм, щоб визначити моделі потенційного використання зібраних наборів даних;

5. Проаналізовано достатність даних для виконання визначених моделей;

6. Розраховано ключові показники в рамках визначених моделей;

7. Створено користувацькі інтерфейси/інформаційні панелі, які відображають показники, індекси та показують тенденції.

2.2 Розробка інструменту для аналізу трудових ресурсів з кібербезпеки

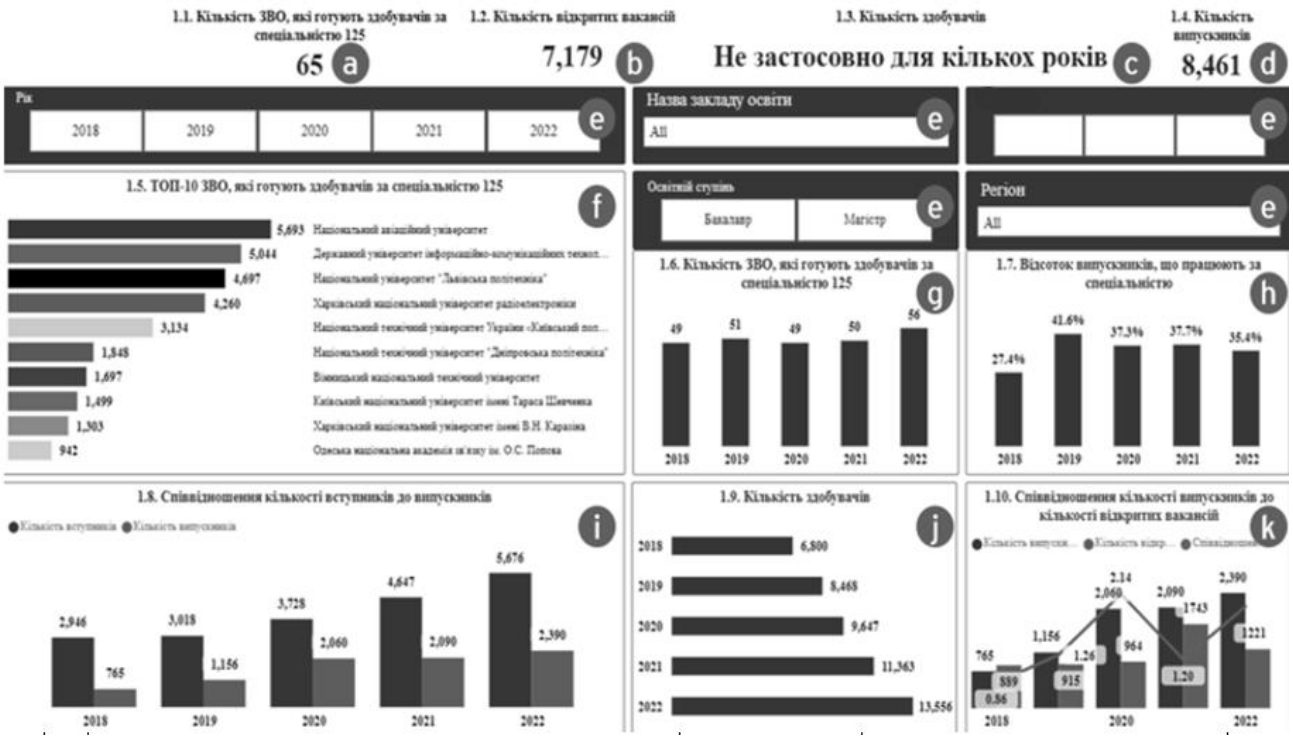

Рисунок 2.3 Відображення загальних показників попиту і пропозиції на ринку спеціалістів з кібербезпеки

a. Кількість ЗВО, які готують здобувачів за спеціальністю 125

Тип графіку - Card

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

b. Кількість відкритих вакансій

Тип графіку - Card

Візуальні фільтри - Рік, агрегатор, регіон

c. Кількість здобувачів

Тип графіку - Card

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

d. Кількість випускників

Тип графіку - Card

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

e. Наявні фільтри: рік, назва закладу освіти, освітній ступінь

f. ТОП-10 ЗВО, які готують здобувачів за спеціальністю 125

Опис - Використовується для відображення рейтингу ТОП-10 ЗВО з найбільшою кількістю здобувачів в рамках спеціальності 125 “Кібербезпека/Кібербезпека та захист інформації”

Тип графіку - Clustered bar chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

g. Співвідношення кількості вступників до випускників

Опис - Використовується для відображення співвідношення кількості вступників до випускників у розрізі років

Тип графіку - Line and clustered column chart

Візуальні фільтри - Назва закладу освіти, освітній ступінь, регіон

h. Кількість ЗВО, які готують здобувачів за спеціальністю 125

Опис - Використовується для відображення кількості ЗВО, які готують здобувачів за спеціальністю 125 ”Кібербезпека/Кібербезпека та захист інформаці” по роках

Тип графіку - Clustered column chart

Візуальні фільтри - Назва закладу освіти, освітній ступінь, регіон

i. Відсоток випускників, що працюють за спеціальністю

Опис - Використовується для відображення відсотку випускників, що працюють за спеціальністю після закінчення ЗВО

Тип графіку - Clustered column chart

Візуальні фільтри - Назва закладу освіти, освітній ступінь, регіон

j. Кількість здобувачів

Опис - Використовується для відображення кількості здобувачів, що навчалися за спеціальністю 125 “Кібербезпека/Кібербезпека та захист інформації” по роках

Тип графіку - Clustered bar chart

Візуальні фільтри - Назва закладу освіти, освітній ступінь, регіон

k. Співвідношення кількості випускників до кількості відкритих вакансій

Опис - Використовується для відображення кількості випускників, кількості відкритих вакансій та їх співвідношення у розрізі років

Тип графіку - Line and clustered column chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, агрегатор, регіон

Рисунок 2.4 Відображення показників, що стосуються пропозиції спеціалістів з кібербезпеки, яку формують заклади вищої освіти в Україні, які готують цих спеціалістів за спеціальністю 125 “Кібербезпека/Кібербезпека та захист інформації”

a. **Кількість вступників**

Тип графіку - Card

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

b. **Кількість здобувачів**

Тип графіку-Card

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

c. **Кількість випускників**

Тип графіку - Card

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

d. **Наявні фільтри:** Рік, назва закладу освіти, освітній ступінь, регіон

e. Співвідношення кількості вступників до випускників

Опис - Використовується для відображення кількості вступників, випускників, а також їх співвідношення по роках

Тип графіку - Line and clustered column chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

f. Кількість ЗВО, які готують здобувачів за спеціальністю 125

Опис - Використовується для відображення кількості ЗВО, які готують здобувачів за спеціальністю 125 “Кібербезпека/Кібербезпека та захист інформації” та темпів приросту відповідних ЗВО

Тип графіку - Line and clustered column chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

g. Кількість вступників

Опис - Використовується для відображення кількості вступників та темпів приросту вступників до попереднього року

Тип графіку - Line and clustered column chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

h. Кількість здобувачів

Опис - Використовується для відображення кількості здобувачів та темпу приросту здобувачів до попереднього року

Тип графіку - Line and clustered column chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

i. Кількість випускників

Опис - Використовується для відображення кількості випускників та темпів приросту випускників до попереднього року

Тип графіку - Line and clustered column chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

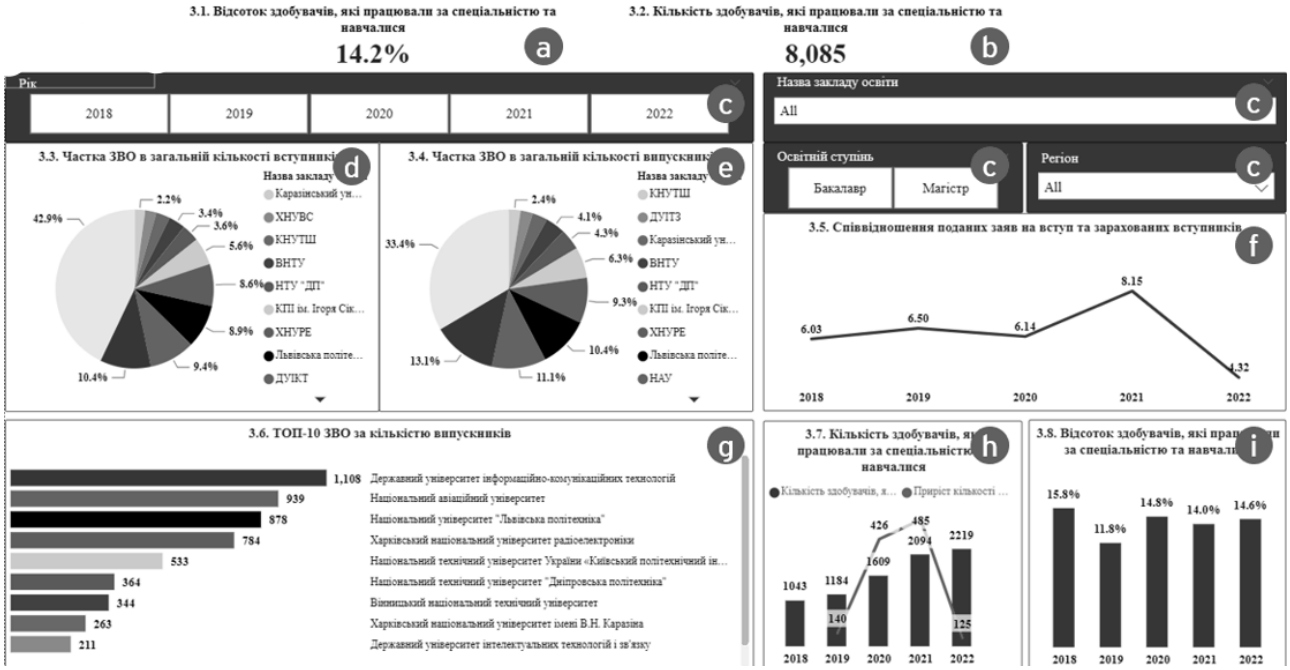

Рисунок 2.5 Відображення показників, що стосуються пропозиції спеціалістів з кібербезпеки на ринку Україні та закладів вищої освіти, які готують таких спеціалістів за спеціальністю 125 “Кібербезпека/Кібербезпека та захист інформації”

a. Відсоток здобувачів, які працювали за спеціальністю та навчалися

Тип графіку - Card

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

b. Кількість здобувачів, які працювали за спеціальністю та навчалися

Тип графіку - Card

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

c. Наявні фільтри: Рік, назва закладу освіти, освітній ступінь, регіон

d. Частка ЗВО в загальній кількості вступників

Опис - Використовується для відображення частки ЗВО (ТОП-10) в загальній кількості вступників на спеціальність 125 “Кібербезпека/Кібербезпека та захист інформації”

Тип графіку - Pie chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

e. Частка ЗВО в загальній кількості випускників

Опис - Використовується для відображення частки ЗВО (перші ТОП-10) в загальній кількості випускників спеціальності 125 “Кібербезпека/Кібербезпека та захист інформації”

Тип графіку - Pie chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

f. Співвідношення поданих заяв на вступ та зарахованих вступників

Опис - Використовується для відображення співвідношення поданих заяв на вступ та зарахованих вступників на спеціальність 125 “Кібербезпека/Кібербезпека та захист інформації”

Тип графіку - Line chart

Візуальні фільтри - Назва закладу освіти, освітній ступінь, регіон

g. ТОП-10 ЗВО за кількістю випускників

Опис - Використовується для відображення ТОП-10 ЗВО за кількістю випускників спеціальності 125 “Кібербезпека/Кібербезпека та захист інформації”

Тип графіку - Clustered bar chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

h. Кількість здобувачів, які працювали за спеціальністю та навчалися

Опис - Використовується для відображення кількості здобувачів спеціальності 125 “Кібербезпека/Кібербезпека та захист інформації”, які працювали за спеціальністю та паралельно навчалися та приросту кількості таких здобувачів, у відношенні до попереднього року (у розрізі років)

Тип графіку - Line and clustered column chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

i. Відсоток здобувачів, які працювали за спеціальністю та навчалися

Опис - Використовується для відображення відсотку здобувачів спеціальності 125 “Кібербезпека/Кібербезпека та захист інформації”, які працювали за спеціальністю та навчалися у розрізі років

Тип графіку - Line and clustered column chart

Візуальні фільтри - Рік, назва закладу освіти, освітній ступінь, регіон

2.3 Аналіз результатів імплементації розробленого інструменту

Спеціальність 125 «Кібербезпека та захист інформації» до 2022 року викладалась приблизно в п’ятидесяти ЗВО. Кількість ЗВО, що пропонують навчання на даній спеціальності, у 2022 році зросла на 12%.

Зростання кількості ЗВО, у яких викладається спеціальність 125 «Кібербезпека та захист інформації», в 2022 році є реакцією ЗВО на високу популярність кібербезпеки серед вступників та діджиталізацію України в цілому.

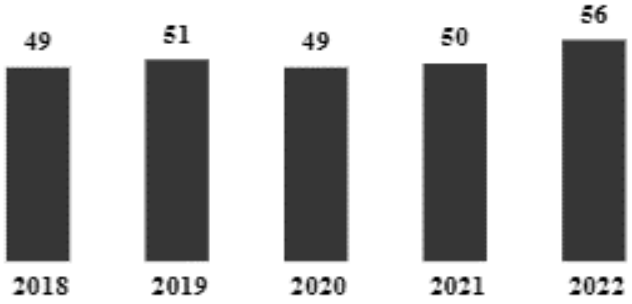

Рисунок 2.6 Кількість ЗВО, які готують здобувачів за спеціальністю 125 «Кібербезпека»/ «Кібербезпека та захист інформації»

Порівнюючи 2018 та 2022 роки, 8 з 10 ЗВО з переліку ТОП-10 зберегли свої позиції. Збереження позицій 8 з 10 ЗВО у переліку ТОП-10 свідчить про наявність сталої бази для підготовки спеціалістів з кібербезпеки. Також це опосередковано свідчить про збереження якості та стандартів освіти, яку надають дані ЗВО.

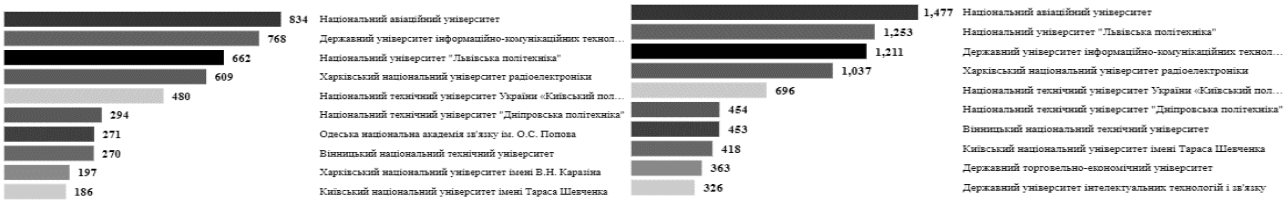

Рисунок 2.7 ТОП-10 ЗВО, які готували здобувачів за спеціальністю 125 «Кібербезпека»/ «Кібербезпека та захист інформації»

Загальна кількість вступників зросла на 92.6% за п’ять років. Спостерігається зменшення темпів зростання вступників у 2022 році на 2.6% в порівнянні з 2021 роком.

На динаміку кількості вступників за 2021-2022 роки вплинули:

- падіння кількості вступників-бакалаврів з 3 745 (у 2021 році) до 3 623 (у 2022 році);
- зростання кількості вступників- магістрів з 902 (у 2021 році) до 2 053 (у 2022 році).

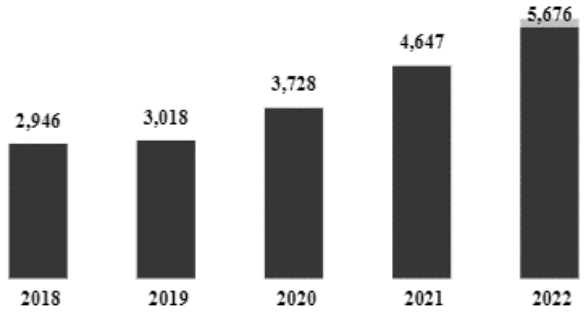

Рисунок 2.8 Загальна кількість вступників

Зросла кількість вступників серед магістрів у 2022 році: з 902 (у 2021 році) до 2 053 (у 2022 році). Ріст становить 127.6%.

Значно зросла кількість вступників невеликих та комерційних ЗВО, що може пояснюватися можливістю надання їм відстрочки від мобілізації. Наприклад, Приватний вищий навчальний заклад «Європейський університет» збільшив набір магістрів з 11 (в 2021) до 118 (в 2022) та ввійшов до ТОП-5 ЗВО за кількістю вступників-магістрів

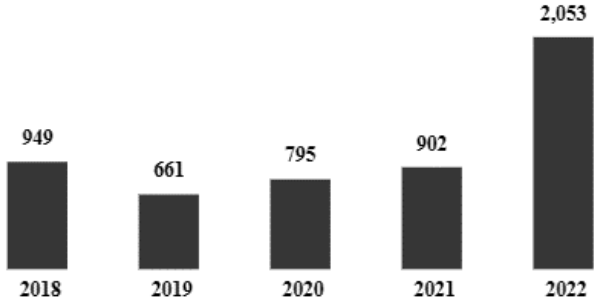

Рисунок 2.9 Загальна кількість вступників на магістратуру

На падіння кількості вступників-бакалаврів передусім вплинув початок повномасштабного вторгнення. А саме: значне зменшення вступників у Харківській області (-233 в порівнянні з 2021 роком, що становить 6,2%) та їх частковий перерозподіл між центральними та західними регіонами.

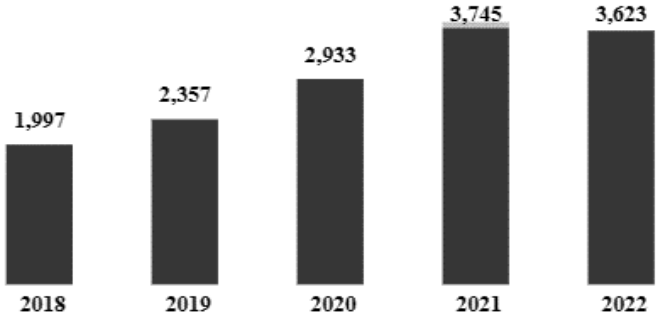

Рисунок 2.10 Загальна кількість вступників на бакалаврат

Щорічно збільшується кількість вступників, що обирають контрактну форму навчання. Збільшення кількості вступників контрактної форми навчання в 2021 році на 39.2% та у 2022 році на 34.5% в порівнянні з попереднім роком.

ЗВО збільшують набір на контрактні місця для отримання додаткового фінансування, враховуючи популярність спеціальності. Підвищення платоспроможності населення України дало змогу навчатися на контрактній основі більшій частині здобувачів. Повномасштабне вторгнення в 2022 році

прискорило ріст кількості контрактних місць через можливість отримання відстрочки від мобілізації на час навчання.

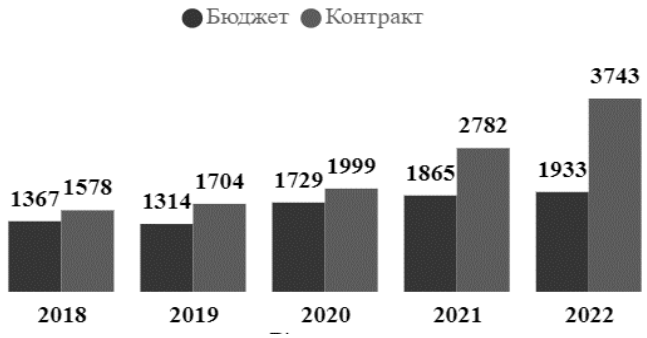

Рисунок 2.11 Форма оплати навчання

Таблиця 2.2

Відсоток та приріст вступників за формою оплати навчання на бюджетній та контрактній основі протягом 2018 – 2022 рр.

Рік	Вступники на бюджет	Вступники на контракт	Всього вступники	Вступники на бюджет, %	Вступники на контракт, %	Приріст бюджет, %	Приріст контракт, %
2018	1 367	1 578	2 945	46.4%	53.6%		
2019	1 314	1 704	3 018	43.5%	56.5%	-3.9%	8.0%
2020	1 729	1 999	3 728	46.4%	53.6%	31.6%	17.3%
2021	1 865	2 782	4 647	40.1%	59.9%	7.9%	**39.2%**
2022	1 933	3 743	5 676	34.1%	65.9%	3.6%	**34.5%**

Джерело: розроблено автором за даними [35]

Низькі показники кількості випускників-бакалаврів. Наприклад, кількість випускників-бакалаврів становила 33 у 2018 та 120 в 2019 роках. Зростання на 917% кількості випускників-бакалаврів у 2020 році.

Спеціальність 125 «Кібербезпека та захист інформації» з’явилася в 2016 році завдяки Постанові МОН «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015. Враховуючи стандартний цикл бакалаврату, що становить 4 роки, перший масовий випуск бакалаврів відбувся саме в 2020 році, що і пояснює виявлений «стрибок». Наявність випускників за освітнім ступенем бакалавр у 2018 та 2019 років була пов’язана зі здобувачами, які навчалися на заочній формі та/або в яких основа вступу була молодший спеціаліст (тому навчання на бакалавраті закінчилось за два роки)

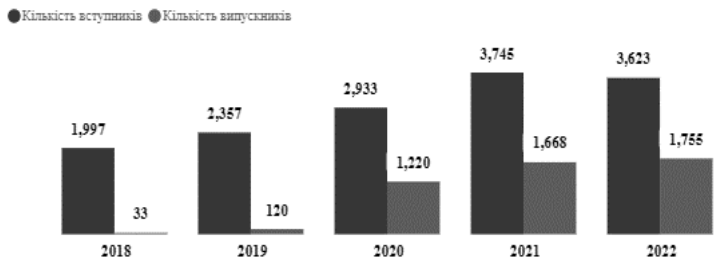

Рисунок 2.12 Кількість вступників та випускників за освітнім ступенем бакалавр

Тенденції до збільшення кількості здобувачів на одну викладацьку ставку. Зростання кількості здобувачів на одну викладацьку ставку на 34% у 2019 році та на 17% в 2021 році. Причиною збільшення кількості здобувачів на одну викладацьку ставку у 2019 році було збільшення кількості вступників на 2.4% та зниженням кількості викладацьких ставок профільних кафедр на 6.8%

Причиною до збільшення кількості здобувачів на одну викладацьку ставку у 2021 році було збільшення кількості вступників на 24.7% та збільшення кількості викладацьких ставок профільних кафедр всього на 1%. ЗВО поступово реагують

на збільшення кількості вступників, збільшуючи кількість викладацьких ставок профільних кафедр, проте із запізненням в один рік.

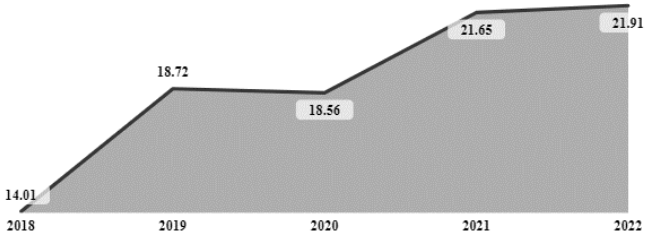

Рисунок 2.13 Кількість здобувачів на одну викладацьку ставку профільних кафедр

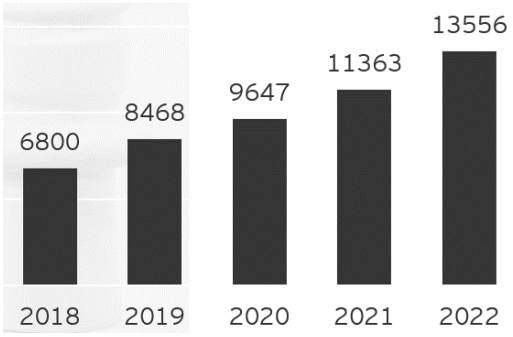

Рисунок 2.14 Загальна кількість вступників

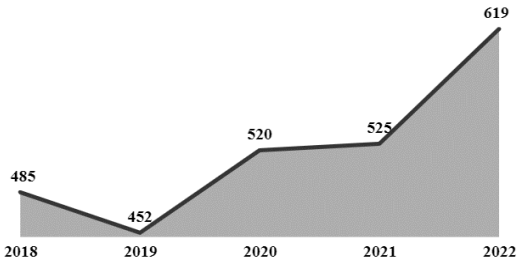

Рисунок 2.15 Кількість викладацьких ставок профільних кафедр

В 2022 році 23 із 42 опитаних ЗВО мають доступ до «кіберполігонів». Зростання кількості ЗВО, що мали доступ до платформ «кіберполігонів», становить близько 90% щорічно, починаючи з 2020 року.

Стабільне зростання кількості ЗВО, що мали доступ до платформ «кіберполігони», пов’язане зі збільшенням кількості фондів та спонсорів, які підтримують створення таких платформ для здобувачів

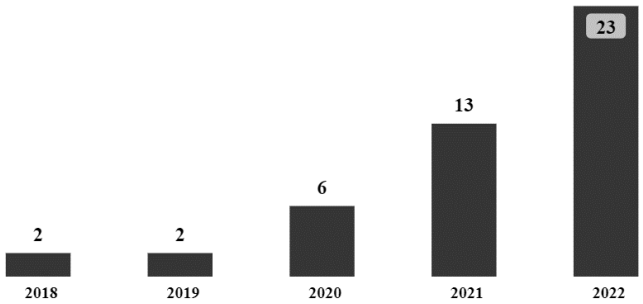

Рисунок 2.16 Кількість ЗВО, що мали доступ до платформ «кіберполігони»

В 2022 році здобувачі 28 із 42 опитаних ЗВО брали участь в CTF-змаганнях. Зростання кількості ЗВО, здобувачі яких брали участь в CTF-змаганнях, складає 58% в 2021 році, та 150% у 2022 році. Зростання кількості ЗВО, здобувачі яких брали участь в CTF-змаганнях, пов’язане зі збільшення обсягів додаткового фінансування та спонсорських програм в рамках організації таких подій

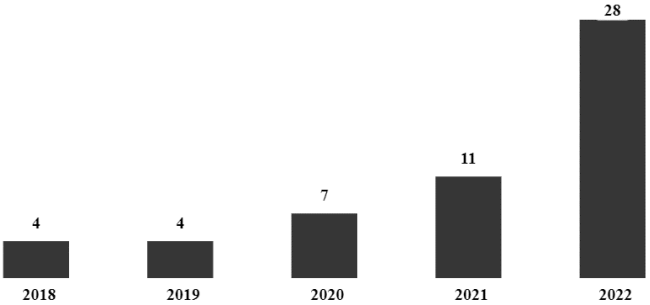

Рисунок 2.17 Кількість ЗВО, здобувачі яких брали участь в CTF-змаганнях

Збільшення частки ЗВО, що мають дуальну форму навчання за спеціальністю 125 «Кібербезпека та захист інформації» на 4% в 2020 та 2021 роках. У 2018 році КМУ схвалив Концепцію підготовки фахівців за дуальною формою здобуття освіти, яка була розрахована на 2018-2023 роки.

Тенденція до збільшення відсотку ЗВО, що мають дуальну форму навчання пояснюється популяризацією Міністерством освіти та науки України дуальної освіти через впровадження відповідного пілотного проєкту в Україні в 2015 році та його активний розвиток з 2019 року. Спостерігається зацікавленість реального сектору економіки у співпраці з ЗВО для підготовки спеціалістів, які отримують практичні знання. Такі здобувачі після закінчення навчання є більш конкурентними та краще підготовленими до роботи на реальному ринку

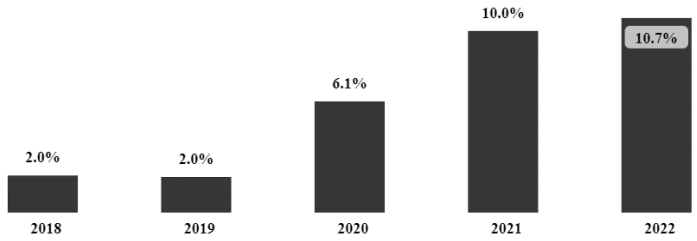

Рисунок 2.18 Відсоток ЗВО, що мають дуальну форму навчання

Зростання кількості вакансій на 80.8% у 2021 році. Падіння кількості вакансій на 29.9% в 2022 році.

В 2021 році бізнес реагував на стрімкий розвиток інформаційних технологій після пандемії COVID ростом кількості вакансій. На початку 2022 року компанії почали зменшувати витрати на штат співробітників і накопичувати резерви через повномасштабні воєнні дії в Україні

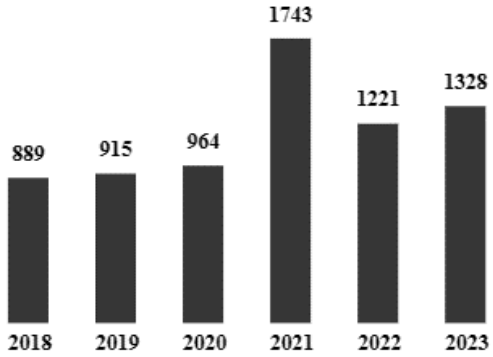

Рисунок 2.19 Кількість відкритих вакансій з кібербезпеки

Для розрахунку кількості ресурсів з кібербезпеки потрібно звертати увагу на падаючий відсоток випускників, що працюють за спеціальністю:

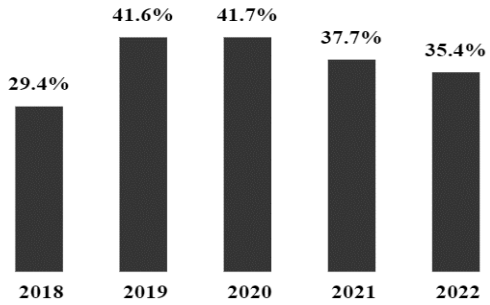

Рисунок 2.20 Відсоток випускників, що працюють за спеціальністю

Якщо поточний тренд (за 2020-2022 роки), а саме сповільнення падіння відсотку випускників, що працюють за спеціальністю, буде зберігатися, в 2023 році тільки третина випускників поповнить фактичну ресурсну базу. Також важливо пам’ятати, що дуже незначний відсоток випускників матиме необхідні для ринку кваліфікації в частині володіння технологіями та інструментами, знання галузевих стандартів та наявності професійних сертифікацій, які вимагають роботодавці.

Протягом п’яти років 3 з 10 ТОП професійних сертифікацій втратили свою вагу серед потреб роботодавців, але решта залишились настільки ж затребуваними. Фокус потреб ринку все більше зміщується від точкових до системних сертифікацій. Наприклад, зараз є популярним запит щодо Certified Cyber Security Architect, що свідчить по бажання компаній вибудовувати саме кібербезпекову архітектуру, а не вирішувати точкові питання. Підтримується потреба у спеціалістах, які спеціалізуються на безпеці хмарних рішень. ЗВО варто враховувати перелік найактуальніших сертифікацій, щоб за можливості коригувати власні навчальні програми. Це допоможе здобувачам отримувати знання близькі до реальних потреб ринку

Таблиця 2.3

ТОП сертифікацій, які вимагають роботодавці

2018	2023
EC-Council Certified SOC Analyst	EC-Council Certified SOC Analyst
Certified Information Systems Security Auditor	Certified Information Systems Security Professional
Certified Information Systems Security Professional	Certified Information Systems Security Auditor
Certified Information Systems Security Manager	Certified Information Systems Security Manager
EC-Council Certified Ethical Hacker	EC-Council Certified Ethical Hacker
Certified Cloud Security Professional	CompTIA Security+
Certified Information Privacy Professional	GIAC Continuous Monitoring Certification
Cisco Certified Network Professional – Security	Certified Cyber Security Architect
Information Security Manager	Certified Cloud Security Professional

GIAC Certified Windows Security Administrator	Information Security Manager

Джерело: розроблено автором на основі даних отриманих від Джерела 2

Низька пропозиція необхідних сертифікацій з боку здобувачів освіти. Великий попит ринку на сертифіковані кадри. Дефіцит високоспеціалізованих сертифікованих кадрів на ринку (0.14 відповідних здобувачів на одну вакансію в 2022 році). Низька персональна мотивація здобувачів щодо отримання сертифікацій, а також висока вартість сертифікацій, значні витрати часу, брак знань та досвіду. Надлишок низькоспеціалізованих кадрів на ринку (26 здобувачів на одну вакансію в 2022 році). Роботодавцям недостатньо, щоб потенційні кадри мали лише профільну освіту в ЗВО. Важливим є підтвердження здобутих знань шляхом отримання професійних сертифікацій.

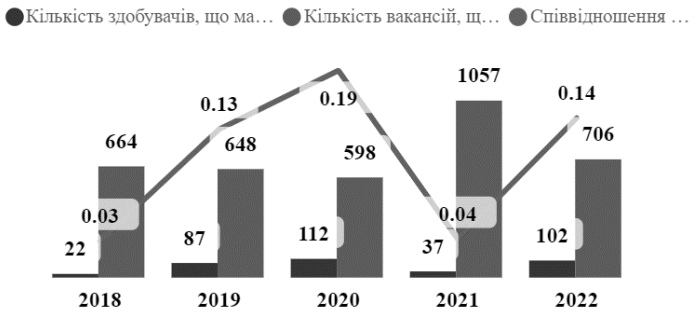

Рисунок 2.21 Співвідношення кількості здобувачів, що мають професійні сертифікації до кількості вакансій, що вимагають наявність таких сертифікацій

Дані про заробітну плату з 2018 по 2022 рік вказують на зростання доходів протягом цього періоду. Вона систематично збільшувалася впродовж цих п'яти років, що може свідчити про позитивні економічні тенденції.

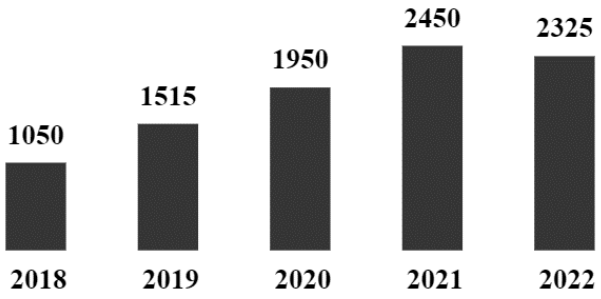

Рисунок 2.22 Середня щомісячна заробітна плата в доларах США

Якщо розглядати річний приріст у відсотках, можна визначити швидкість зростання. Наприклад, різниця між 2018 та 2019 становить більше 40%, а між 2020 та 2021 - близько 25%. Це може вказувати на те, що темпи зростання зменшилися. За 2022 рік спостерігається зменшення заробітної плати приблизно на 5%. Це може бути пов'язано з різними економічними чинниками, такими як вплив воєнної ситуації в країні. В середньому, заробітна плата за цей період зросла, але важливо врахувати інфляційний вплив та інші фактори для отримання точнішого порівняння динаміки зміни заробітної плати в сфері кібербезпеки.

Висновки до розділу 2

Реалізація консалтингового проєкту - це складний і багатоаспектний процес, що вимагає від команди консультантів високого рівня організації, ефективності та співпраці. Фундаментальним етапом є глибоке зрозуміння бізнес-потреб та викликів клієнта. Це дозволяє належним чином визначити обсяг проєкту та розробити ефективні стратегії. Чітке визначення мети, завдань, термінів та ресурсів є важливим для успішного виконання консалтингового проєкту. Планування визначає кількість етапів та послідовність їх виконання. Комунікація з клієнтом та всередині консалтингової команди грає ключову роль у вирішенні проблем, уточненні очікувань клієнта та в забезпеченні взаєморозуміння.

Реалізація консалтингового проєкту часто зустрічається з непередбаченими викликами. Гнучкість та готовність до адаптації дозволяють ефективно реагувати на зміни середовища. Ретельна та компетентна оцінка результатів та підготовка чітких звітів по результатам консалтингового проєкту допомагають не лише визначити успішність проєкту, а й надати клієнту рекомендації для подальших дій. Після завершення проєкту важливо провести аналіз, визначити проблемні моменти та вдосконалити методологію для подальших консалтингових проєктів. В цілому, успішна реалізація консалтингового проєкту вимагає сумісних зусиль всіх стейкхолдерів, професіоналізму та стратегічного підходу для досягнення конкретних цілей клієнта.

Реалізація консалтингового проєкту з розробки інструменту для оцінки наявних трудових ресурсів у кібербезпеці представляє собою важливу складову в формуванні стратегії підготовки фахівців з кібербезпеки. З такого проєкту можна зробити наступні висновки:

1. Зважаючи на зростаючий обсяг кіберзагроз і швидкий розвиток технологій, наявність ефективного інструменту для оцінки трудових ресурсів у сфері кібербезпеки є важливою частиною стратегії кіберзахисту.
2. Визначення конкретних показників для оцінки результатів використання інструменту дозволяє здійснити об'єктивний аналіз попиту та пропозиції на ринку кібербезпеки.
3. Реалізація інструменту включала в себе процес навчання та підготовки персоналу для його ефективного використання, що є важливим кроком у забезпеченні ефективності та безпеки його використання.
4. Реалізація проєкту відбувалася з точки зору його як складової стратегії довгострокового розвитку, з можливістю розширення функціональності та забезпечення необхідної технічної та організаційної підтримки.

РОЗДІЛ 3

ПРОПОЗИЦІЇ ЩОДО ФОРМУВАННЯ СТРАТЕГІЇ ПІДГОТОВКИ КАДРІВ У СФЕРІ КІБЕРБЕЗПЕКИ

3.1 Загальні пропозиції щодо підвищення ефективності підготовки кадрів

В сфері кібербезпеки, де кожен біт інформації може визначати межі безпеки або ризику, формування стратегії підготовки кадрів є критично важливим завданням для сучасних закладів вищої освіти. Це є складним викликом, оскільки кіберзагрози постійно еволюціонують, вимагаючи від освітніх програм гнучкості, інноваційності та високого ступеня адаптації [27]. Усвідомлюючи глобальний характер цього виклику, стратегія підготовки кадрів у сфері кібербезпеки повинна бути зорієнтована на те, щоб не лише відповідати поточним потребам галузі, але й передбачати майбутні тенденції та виклики. Вона повинна сприяти створенню кадрового потенціалу, здатного ефективно реагувати на нові загрози, і в той же час, надавати здобувачам освіти та новим спеціалістам можливість розвивати та вдосконалювати свої навички в сфері кібербезпеки. Основна мета такої стратегії – це створення навчального середовища, що поєднує теоретичні знання з реальними практичними викликами. Вона передбачає планування та впровадження інноваційних програм, орієнтованих на розвиток критичного мислення, аналітичних та технічних навичок, які є необхідними у сучасному кіберпросторі. Збудована на принципах академічної експертизи та практичного застосовування, ця стратегія також визнає важливість співпраці з реальним сектором економіки, де студенти можуть отримати практичний досвід і взаємодіяти з провідними фахівцями галузі [28]. Крім того, вона спрямована на створення умов для регулярного оновлення та адаптації навчальних програм до змін у кіберпросторі,

надаючи здобувачам освіти необхідний інструментарій для ефективної конкуренції та інновацій. Стратегія підготовки кадрів у сфері кібербезпеки – це важливий елемент забезпечення стійкості та безпеки в цифровому світі, де відправною точкою є не лише реагування на сучасні виклики, а й активна участь у формуванні високотехнологічного майбутнього [29].

В умовах стійкої загрози кібербезпеки, де втілення інновацій та розвиток технологій є невід'ємною частиною цифрового прогресу, стратегія повинна ставити під акцент не лише технічні аспекти. Вона має формувати не лише фахівців із глибоким технічним розумінням, але й експертів, які мають комплексне бачення кіберзагроз та здатні розрізняти етичні аспекти вирішення цих викликів [30]. Стратегія також має акцентувати увагу на розвитку креативності та інноваційного мислення серед студентів. Кібербезпека не тільки потребує засвоєння існуючих знань, але й вимагає вміння швидко адаптуватися до нових умов та ефективно вирішувати проблеми в ситуаціях невизначеності. Зокрема, стратегія повинна активно підтримувати дослідницьку роботу та створення центрів експертизи, що дозволяє здійснювати наукові розробки та вносити вагомий внесок у галузь. Співпраця зі спеціалізованими дослідницькими центрами та урядовими агентствами може значно підвищити якість досліджень та створити умови для впровадження інноваційних рішень у практичну діяльність [31]. Врешті-решт, стратегія підготовки кадрів повинна бути орієнтована на створення цілісного системного підходу, де освіта, дослідження, індустрія та уряд взаємодіють для спільного досягнення цілей кібербезпеки та забезпечення цифрової стійкості всієї країни.

Щоб сформулювати стратегію підготовки кадрів у сфері кібербезпеки, важливо враховувати різноманітні аспекти, які визначають успіх такої стратегії. Ось кілька пропозицій, які можуть бути враховані при формуванні такої стратегії:

1. Співпраця з реальним сектором економіки. Розвивати партнерства з профільними компаніями та організаціями у галузі кібербезпеки для створення освітніх програм, які враховують реальні вимоги ринку. Розвиток співпраці з компаніями та організаціями в галузі кібербезпеки створює додаткові можливості для стажування, участі у робочих проектах та отримання реального досвіду здобувачами освіти. Співпраця із профільними компаніями в галузі надає здобувачам освіти унікальну можливість отримати прямий доступ до актуальної експертизи та практичних викликів, що істотно збільшує ефективність їхньої підготовки. Це передбачає собою також і укладання довгострокових угод, співпрацю з компаніями щодо спільної розробки курсів, участь у стажуванні та програмах практики. Паралельно, такі партнерства дозволяють закладам вищої освіти більш точно визначити потреби реального сектору економіки та адаптувати свої навчальні програми під вимоги ринку. Це має забезпечити випускникам більш високий рівень готовності до викликів реального світу. Такий підхід до партнерства в сфері кібербезпеки допомагає збільшити реальну цінність освітнього процесу та підвищити конкурентоспроможність випускників на ринку праці. Збалансована комбінація теоретичних знань та практичного досвіду, отриманого завдяки залученню профільних підприємств у галузі кібербезпеки, робить таку стратегію ефективною для підготовки висококваліфікованих фахівців у сфері кібербезпеки [31].

2. Участь у змаганнях з кібербезпеки. Сприяти участі студентів у змаганнях з кібербезпеки, де вони можуть випробувати свої навички в реальних сценаріях. Участь у подібних змаганнях є ключовим елементом підготовки студентів у сфері кібербезпеки з численними перевагами. По-перше, це надає здобувачам освіти можливість застосовувати свої здобуті теоретичні знання в практичних умовах, де вони зіштовхуються з реальними кіберзагрозами. Відчуття

конкретних викликів стимулює розвиток технічних навичок та стратегічного мислення. Крім того, подібні змагання акцентують увагу на командній роботі, допомагаючи учасникам розвивати ефективні навички співпраці та взаємодії. Це важливо враховувати, оскільки більшість реальних завдань у кібербезпеці вимагають колективної роботи та обміну ідеями. Змагання також виступають як імітатор різноманітних сценаріїв з порушення кібербезпеки, що відображає реальні умови у галузі. Здобувачі освіти, беручи участь в таких заходах, отримують можливість опанувати навички реагування на різні кіберзагрози та забезпечення безпеки інформації [32].

Окрім того, важливо відзначити, що змагання з кібербезпеки привертають увагу провідних фахівців та компаній у галузі кібербезпеки. Це створює унікальну можливість для студентів взаємодіяти з професіоналами, отримувати консультації та розширювати свою мережу зв'язків.

3. Впровадження сертифікаційних програм. Впровадження програм із сертифікування здобувачів є елементом стратегії підготовки кадрів у кібербезпеці, спрямованим на створення повноцінного та конкурентоспроможного освітнього процесу. Цей пункт стратегії має великий потенціал вплинути на якість підготовки студентів та випускників, забезпечуючи їхню готовність відповідати на виклики сучасної кібербезпекової дійсності. Сертифікаційні програми повинні бути тісно інтегровані з академічними курсами. Це дозволяє здобувачам здобувати практичні знання паралельно з теоретичними, створюючи комплексний підхід до навчання. Сертифікаційні програми повинні ставити акцент на розвиток конкретних навичок, які є ключовими для професійного успіху в галузі кібербезпеки. Це може включати навички аналізу вразливостей, інцидентного реагування, етичного взлому та інші. Формувати подібні програми варто при серйозній консультації з провідними компаніями та експертами у сфері кібербезпеки, що дозволить адаптувати сертифікаційні програми до реальних

вимог галузі. Це також надає здобувачам освіти можливість отримати практичні поради та інсайти від практикуючих професіоналів. Стратегія повинна передбачати активну підготовку до важливих сертифікацій, таких як Certified Information Systems Security Professional, Certified Ethical Hacker, CompTIA Security+ та інші [33]. Це збільшує конкурентоспроможність випускників на ринку праці. Університети повинні забезпечити студентам необхідні ресурси для успішного проходження сертифікаційних програм, включаючи доступ до навчальних матеріалів, лабораторій та підготовчих курсів. Стратегія повинна передбачати механізми оцінки успішності здобувачів в сертифікаційних програмах та систему постійного вдосконалення курсів на основі отриманого досвіду та актуальних змін у сфері кібербезпеки. Впровадження цих аспектів в стратегію сертифікаційних програм надає не лише академічний, але і практичний фундамент для підготовки кіберспеціалістів, готових до викликів та високих стандартів галузі [34].

3.2 Розвиток дуальної освіти як ключовий етап реалізації стратегії підготовки фахівців з кібербезпеки

За роки незалежності України було сформовано безліч програм щодо реформ та стратегій в галузі вищої освіти. Деякі були написані та реалізовані, деякі залишались на папері. Проте головною проблемою є те, що загального успішного результату для системи вищої освіти це не принесло. В порівнянні з країнами сусідами, Україна в різноманітних освітніх рейтингах займає значно нижчі місця. Все це стало можливим через те, що більшість освітніх реформ в країні були поверхневими, які вирішували тактичні, а не стратегічні, завдання. Реформи, відсторонені від стратегічних пріоритетів, часто виявляються повністю

неефективними. Зміни без чіткої стратегії не мають шансу на будь-який вагомий внесок. Багато виникаючих проблем у сфері вищої освіти є безпосереднім результатом цього підходу. Прийняті рішення, які можуть здатися корисними, насправді призводять до непередбачених та негативних наслідків. Все це через неузгодженість та нестратегічність [35].

У цьому контексті можна зробити наступний висновок: система, що ґрунтується на принципах приватної власності, не тільки сприяє, але й утворює необхідні передумови для швидкого розвитку будь-яких процесів. Вона є більш ефективною. Підтвердженням цьому є світова динаміка розвитку економічних процесів [36]. З отриманням незалежності поряд з нашою офіційною державою розвивалася внутрішня держава, рушійною силою якої були підприємці, які стали середнім класом. Починаючи зі звичайних стихійних ринків та невеличких магазинів вони зараз переросли в приватні лікарні, школи та університети, агрокомплекси та великі логістичні компанії. І як не дивно, все до чого торкнулась рука підприємця стало ефективним, успішним та популярним серед як внутрішнього, так і зовнішнього споживача. До нас приїжджають із-за кордону для отримання якісних медичних послуг в приватних установах за найнижчими в Європі цінами по відношенню до якості, вітчизняні ІТ-рішення поступово займають лідируючі позиції в своїй ніші у світі, найбільша приватна транспортна компанія країни вже давно показала наочну різницю між силою державного та приватного управління.

Приватна ініціатива єдине, що може допомогти змінити та підвищити систему вищої освіти в Україні. Державні інвестиції стають пріоритетом лише у випадках, коли приватний капітал, з різних причин, неспроможний забезпечити ефективний розвиток та освоєння суспільно важливої галузі. Участь держави допускається лише при наявності демократичного контролю суспільством. Без

цього державна ініціатива поступово перестає відповідати інтересам громадян і стає схильною до трансформації в бюрократичну та номенклатурну системи [37].

Якщо економіка це основа для життєдіяльності держави, то освіта професійних кадрів – інструмент, який налаштовує життєдіяльність самої економіки. В Україні є профільне міністерство з питань освіти, існує безліч різноманітних територіальних органів з якості освіти, впроваджено численні закони та підзаконні регуляторні акти. Незважаючи на всі ці рішення, рівень вищої освіти в Україні по різноманітним міжнародним дослідженням є досить низьким [48].

Чому ж ми опинилися в такій ситуації? Проблема конкурентоздатності вищої освіти України пов'язана з неспроможністю своєчасно реагувати на зміни на сучасному ринку та всі глобальні виклики, які стоять перед економікою та суспільством в цілому [36].

Звісно, це не є першопричиною. До таких можна віднести і низьке фінансове забезпечення системи освіти, і недоліки в системах управління в закладах освіти. Проте не ефективне та не своєчасне реагування на зміни на ринку щодо актуальних компетентностей, які роботодавці хочуть бачити в своїх нових співробітниках є найсильнішим стримуючим ефектом в підготовці реально професійних фахівців. Вирішувати цю проблему взялися шляхом впровадження дуальної освіти. Як показує час - це було правильним рішенням, адже лише реальний бізнес може надати справді об’єктивну інформацію, що потрібно вивчати молодому фахівцю, щоб його знання практично застосовувалися на його робочому місці. Кожного року збільшувалася кількість як закладів освіти, які відкривали в себе дуальні програми навчання, так і кількість зацікавлених у співпраці роботодавців. Кількість зацікавлених та залучених компаній до формування дуальної освіти у партнерстві із ЗВО щороку збільшувалась і станом

на 2022 рік найбільше таких випадків кооперації зафіксовано в Києві і становить 175 залучених компаній [38].

Це свідчить про зацікавленість реального сектору економіки в співпраці з університетами. Основними мотивами, якими керується працедавець коли долучається до партнерства із закладами освіти через розробку дуальних програм навчання є: бажання отримати висококваліфікованих фахівців, не витрачати час на додаткове навчання, не витрачати час на психологічну адаптацію, формування позитивного іміджу компанії серед молодих фахівців. Рівень працевлаштування в (97%) після навчання на програмах з дуальної освіти значно перевищує рівень працевлаштування випускників, які навчалися на звичайних програмах (59%) [49].

Проте є ряд проблем, з якими зіштовхнулися студенти на дуальних освітніх програмах. Серед яких слід виокремити наступні:

1. Недостатня залученість компанії-партнера до викладання та створення навчальних програм.

2. Майже ідентичний обсяг матеріалу, який студенти освоюють на звичайних програмах до того обсягу, що університети вкладають в дуальні програми, які є скорочені за кількістю аудиторних годин.

3. Наближення формату викладання та атестації до заочного типу.

4. Недостатньо ефективна актуалізація навчального матеріалу до потреб які є на робочому місці студента.

5. Спосіб викладання по застарілим практикам.

6. Низький відсоток предметів, що викладаються безпосередньо співробітниками компанії-партнера.

Ці та інші недоліки певною мірою нівелюються реальною практичною діяльністю на робочому місці. В процесі виконання завдань всередині компанії-партнера молодий фахівець самостійно вивчає сучасні методики та кращі практики, які допомагають якісно виконувати поставлені завдання. Проте університетська складова в цій формі навчання має відігравати також значну, а головне – корисну роль. Академічні програми мають бути інтегровані із максимально можливим ступенем відповідності до реальних завдань, які студент буде отримувати на робочому місці. Також, важливим моментом, який необхідно враховувати при розробці дуальних програм є те, що дуальна освіта є формою денного навчання. Тобто такого, яке передбачає залучення студента до систематичного відвідування занять, написання атестаційних та практичних робіт. В свою чергу студент, як правило, працює на 8-годинній основі на місці своєї роботи в компанії-партнера. Необхідно зменшувати навантаження студента для ефективного виконання своїх обов'язків як перед університетом, так і перед основним місцем своєї роботи. Ефективним способом вирішення цих проблем було б не скорочення навчальної програми та вилучення певних предметів, а збільшення кількості предметів за які відповідальні компанії-партнери. В свою чергу університет був би певен, що матеріал доноситься до студента та засвоюється ним, адже компанії першочергово зацікавлені в якісному освоюванні необхідних знань своїми співробітниками. Відповідно у студента було б менше навантаження, тому що оцінка автоматично зараховувалась би до загального переліку заліків та іспитів. Таким чином зменшиться і відсоток можливих неактуальних предметів, які пропонує університет.

Як висновок, варто відзначити, що дуальна освіта – це свіжий подих в українській системі освіти. Вона має гарні відгуки від усіх залучених осіб. Найбільший її недолік – низька розповсюдженість. Якщо говорити про вищу освіту, то програми дуальної освіти впроваджені переважно на магістратурі. Таку

ефективну за рівнем працевлаштування студентів програму слід впроваджувати в якомога більших масштабах, в тому ж числі і на бакалавраті з молодших курсів. Так як основна мета з якою люди здобувають освіту – отримати роботу, буде набагато ефективніше знайомитися з практичною діяльністю за фахом якомога раніше. Можливо такий підхід зменшить невтішну статистику для української системи освіти, де понад 60% випускників працюють не за своїм фахом [49]. Навчаючись на застарілих програмах, студенти часто не розуміють для чого вони гають час відвідуючи університет, коли отримані знання просто ніде застосувати. Тому важливо впроваджувати дійсно працюючі міжнародні практики в українську систему освіти, щоб забезпечити висококваліфікованими та вмотивованими кадрами економіку України.

3.3 Особливості оцінювання ефективності стратегії підготовки фахівців з кібербезпеки

Оцінювання ефективності стратегії підготовки фахівців з кібербезпеки — це складний та багатоплановий процес, який включає в себе різноманітні аспекти. В галузі кібербезпеки, оцінка ефективності повинна враховувати різноманіття аспектів, включаючи академічні досягнення, практичні навички, взаємодію з індустрією, дослідження, участь у проектах тощо. З урахуванням швидкого розвитку технологій та загроз в сфері кібербезпеки, оцінювання повинно використовувати інноваційні методи, такі як використання технічних засобів, розробку економічних моделей, залучення авторитетних профільних консультантів тощо. Важливо враховувати думки та відгуки різних зацікавлених сторін, таких як здобувачі освіти, викладачі та роботодавці. Вони можуть надати свою точку зору на ефективність стратегії, зважаючи на свій практичний досвід, пов’язаний тим чи

іншим чином з галуззю кібербезпеки [39]. Ефективність стратегії краще оцінювати як систему, яка включає в себе всі аспекти підготовки фахівців, від навчання та викладання до практичного досвіду та взаємодії з реальним ринком праці. Важливою є і періодичність оцінювання. Оцінка може проводитися під час вступу до освітніх програм, в процесі навчання та після випуску нових фахівців з кібербезпеки. Це дозволяє своєчасно виявляти та виправляти можливі недоліки на різних рівнях здобування освіти [51]. Особливо важливо на початковому етапі приділяти увагу порівнянню стратегії підготовки кадрів з кібербезпеки з кращими міжнародними практиками. Це може полегшити визначення областей для покращення та впровадження інновацій. Оцінка ефективності повинна включати якісні та кількісні показники, а також оцінки від здобувачів освіти, викладачів, випускників, роботодавців та інших учасників освітнього процесу. На основі результатів оцінювання слід формувати чіткі звіти та рекомендації, які можна використовувати для вдосконалення стратегії підготовки фахівців. Ключовим етапом валідації ефективності розробленої стратегії є реакція ринку праці на нових фахівців з кібербезпеки після випуску із ЗВО. Оцінювання ефективності стратегії підготовки фахівців з кібербезпеки — це неперервний процес, спрямований на адаптацію до змін в галузі та забезпечення високої якості підготовки студентів до викликів кібербезпеки [41].

Ключові показники ефективності (КПЕ) допоможуть відстежувати та оцінювати успішність стратегії підготовки фахівців з кібербезпеки. Деякі можливі КПЕ та їх ваговий коефіцієнт представлені в таблиці 3.1. Критерії вимірювання повинні бути конкретними, зрозумілими та відображати результати поставлених цілей для кожного показника ефективності. Такі критерії можуть бути кількісними (наприклад, кількість, відсоток) або якісними (наприклад, рівень задоволеності здобувачів освіти, репутація ЗВО).

Таблиця 3.1

Ключові показники ефективності стратегії підготовки кадрів з кібербезпеки

№	Показник	Критерії вимірювання	Ваговий коефіцієнт показника
Внутрішні показники			
1	Рівень зайнятості випускників	Відсоток випускників, які знайшли роботу відразу після закінчення навчання	k=0.12
2	Рівень сертифікації	Кількість студентів, які отримали сертифікати відомих організацій з кібербезпеки (наприклад, CompTIA, CISSP)	k=0.1
3	Участь у стажуваннях	Кількість студентів, які беруть участь у стажуваннях в компаніях з кібербезпеки	k=0.08
4	Викладачі з практичним досвідом	Частка викладачів з практичним досвідом в галузі кібербезпеки	k=0.06
5	Активність здобувачів освіти у галузі	Кількість публікацій студентів та викладачів в області кібербезпеки	k=0.04
6	Оновлення технічного обладнання	Частота оновлення та модернізації лабораторного обладнання та інфраструктури	k=0.04
Зовнішні показники			
7	Участь у міжнародних рейтингах кібербезпеки	Позиція країни в міжнародних рейтингах з кібербезпеки та інформаційної безпеки	k=0.11
8	Рівень кібербезпеки державних систем	Зменшення кількості та серйозності кібератак на державні інформаційні системи та інфраструктуру	k=0.11
9	Розробка інновацій та стартапів	Визначення кількості інноваційних проектів або стартапів, які створені здобувачами освіти або випускниками	k=0.1
10	Залучення інвестицій у сфери кібербезпеки	Обсяг інвестицій у розвиток та вдосконалення галузі кібербезпеки в країні	k=0.09
11	Ринкова цінність диплому	Оцінка того, наскільки високо цінують роботодавці дипломи випускників одних ЗВО у порівнянні з іншими ЗВО	k=0.05
12	Залучення фінансування від приватного сектору	Сума фінансування або грантів, отриманих від приватного сектору для підтримки спеціальності 125	k=0.04
13	Кількість поданих та отриманих грантів	Співвідношення поданих та отриманих грантів для розвитку спеціальності 125	k=0.04
14	Повернення інвестицій (ROI) після навчання	Розрахунок вартості навчання на одного студента порівняно з подальшим доходом, який вони можуть забезпечити під час своєї кар'єри	k=0.02

Джерело: розроблено автором

Впровадження стратегії підготовки кадрів з кібербезпеки є складним завданням, яке повинно бути підтримано детальним аналізом. Саме в цьому контексті важливим елементом для комплексного аналізу даної стратегії може бути SWOT-аналіз, який допоможе систематизувати внутрішні і зовнішні фактори, що впливають на стратегію. Далі буде представлена таблиця 3.2, щоб визначити оптимальний напрямок розвитку стратегії підготовки кадрів з кібербезпеки.

Таблиця 3.2

SWOT-аналіз формування стратегії підготовки кадрів з кібербезпеки

Сильні сторони	**Можливості**
1. Високий рівень кваліфікації фахівців. Україна вже має певні групи висококваліфікованих фахівців з кібербезпеки, які можуть брати участь в підготовці нового покоління. **2. Розвинена інфраструктура кібербезпеки.** Наявність великої кількості компаній та організацій у галузі кібербезпеки в Україні, що можуть стати партнерами для практичного навчання та стажування студентів. **3. Технічні ЗВО.** Присутність технічних ЗВО, які можуть стати базовими інституціями для підготовки фахівців.	**1. Підтримка від бізнесу.** Залучення фінансової та технічної підтримки від компаній, що зацікавлені в розвитку інфраструктури та оновлення навчальних програм в галузі кібербезпеки. **2. Міжнародна співпраця.** Розширення міжнародних партнерств для обміну кращими практиками та залучення іноземних експертів. **3. Створення інноваційних лабораторій.** Розвиток власних інноваційних центрів та лабораторій для проведення досліджень у галузі кібербезпеки.
Слабкі сторони	**Загрози**
1. Фінансові обмеження. Обмежені фінансові ресурси можуть знизити можливості інвестування у сучасні технології та навчальні програми. **2. Слабка колаборація між ЗВО та підприємствами.** Недостатня співпраця між освітніми установами та підприємствами може ускладнити адаптацію навчальних програм до потреб ринку. **3. Повільна адаптація до змін в освітніх програмах.** Затримки в актуалізації та адаптації навчальних планів до останніх тенденцій у кібербезпеці.	**1. Відтік кадрів за кордон.** Збільшення попиту на фахівців в інших розвинених країнах може призвести до відтоку кваліфікованих кадрів. **2. Політична нестабільність.** Нестабільність у політиці може вплинути на фінансування та розвиток освітніх програм. Зміни в законодавстві, що регулює кібербезпеку, можуть вплинути на ефективність підготовки фахівців. **3. Еволюція загроз в кібербезпеці.** Постійна еволюція загроз у сфері кібербезпеки може вимагати постійного оновлення навчальних програм та методик.

Джерело: розроблено автором

Аналіз стратегії підготовки кадрів з кібербезпеки в Україні виявив, що країна має потенціал та інфраструктуру для розвитку відповідної галузі. Проте, існують виклики, такі як низьке фінансове забезпечення та політична нестабільність, що може обмежити повноцінне впровадження цієї стратегії. З метою забезпечення ефективності та стійкості стратегії важливо зосередити увагу на створенні стабільного фінансового фундаменту для розвитку освітніх програм та технічної бази. Тривалий успіх стратегії також залежить від ефективної комунікації та партнерства між ЗВО та реальним сектором економіки, а також від внесення інновацій та сучасних технологій у навчальний процес.

Висновки до розділу 3

Загалом, важливо розглядати процес підготовки кадрів як динамічний та адаптивний до вимог ринку праці. Застосування актуальних програм, інтерактивних методів навчання, партнерства з підприємствами та акцент на розвиток професійних та гнучких навичок сприяють створенню високоефективної системи підготовки, готової до викликів сучасного бізнесу та технологічного розвитку. Відзначаючи ключові аспекти підготовки кадрів, необхідно акцентувати на необхідності постійного оновлення та адаптації навчальних програм до зростаючих вимог ринку праці. Успішна підготовка кадрів вимагає тісної взаємодії з підприємствами. Спільні проекти, стажування та обмін досвідом забезпечують студентам можливість набуття практичних знань та адаптацію їх академічних знань до реальних конкретних потреб ринку праці. Особливу увагу приділено важливості розвитку дуальної форми навчання в закладах освіти. Дуальна форма навчання є інноваційним підходом до освіти, який поєднує академічне навчання і практичний досвід на робочому місці. За допомогою дуальної форми навчання

можна вирішити найважливішу проблему, з якими зіштовхуються здобувачі освіти – низький рівень практичних навичок до вирішення завдань на реальному ринку праці. Саме за допомогою дуальної форми навчання можна активно розвивати колаборацію між закладами вищої освіти і підприємствами. Досвід її впровадження показує позитивні відгуки від обох найбільш зацікавлених сторін в освітньому процесів – здобувачів освіти і роботодавців. В свою чергу, акцент на постійному навчанні, високій взаємодії з індустрією та розвитку комплексного набору навичок у здобувачів освіти створює фундамент для ефективної підготовки кадрів, готових до викликів і можливостей, що стоять перед сучасним ринком праці. Дані особливості підготовки кадрів є невід'ємною складовою у формуванні загальної стратегії з підготовки кадрів у сфері кібербезпеки.

Розроблена стратегія оцінювання підготовки кадрів у сфері кібербезпеки є направленою на забезпечення підвищення стандарту якості навчання. Заснована на різноманітних показниках ефективності, вона враховує широкий спектр аспектів, включаючи академічні досягнення, практичні навички, взаємодію з індустрією та реакцію ринку праці. Однією з ключових особливостей стратегії є її системний підхід. Оцінювання охоплює різні етапи навчання, починаючи від вступу до програми та завершуючи трудовим працевлаштуванням випускників. Це дозволяє своєчасно виявляти сильні та слабкі сторони, а також адаптувати стратегію до змін у галузі. Стратегія використовує інноваційні методи оцінювання, враховуючи швидкий темп розвитку технологій. Оцінювання також враховує думки зацікавлених сторін, включаючи студентів, викладачів, роботодавців та випускників. Це забезпечує різноманітність перспектив та враховує потреби всіх учасників освітнього процесу. Звіти та рекомендації, що формуються на основі результатів оцінювання, стають основою для подальшого вдосконалення стратегії. Адаптація до змін в технологічному середовищі, постійне покращення програм

навчання та спрощення взаємодії із сферою бізнесу — це ключові аспекти, на яких спрямована стратегія.

Враховуючи ці особливості, можна стверджувати, що розроблена стратегія оцінювання підготовки кадрів у сфері кібербезпеки є ефективною та відповідає вимогам сучасного мінливого світу кібербезпеки та інформаційних технологій.

ВИСНОВКИ

Протягом виконання дипломної роботи була пророблена велика та ґрунтовна робота, що враховувала складність та багатоетапність процесів організації кібербезпеки та захисту інформації під час професійного консалтингового супроводу. Були сформовані пропозиції щодо підвищення ефективності підготовки кадрів у сфері кібербезпеки. Варто зазначити, що виконання роботи здійснювалось чітко відповідно до етапів формування стратегії. Першим важливим кроком стало вивчення теоретичного змісту консалтингу, що дозволило визначити нормативно-правове поле діяльності консультанта в подібних проєктах, надати основні визначення понять «стратегія», «ринок кібербезпеки», «аналітичний консалтинг», що дозволило в подальшому ефективно оперувати ними в ході реалізації проєкту. Також, були досліджені особливості ринку консалтингових послуг в Україні. Розраховано динаміку доходів окремих видів консалтингових послуг за використанням класифікації видів економічної діяльності. Визначено особливості кращих вітчизняних консалтингових компаній та вагомий вклад у розвиток ринку консалтингових послуг, який здійснюють міжнародні найкращі профільні компанії.

Визначення сутності та особливості сфери кібербезпеки в Україні дозволило сформувати важливість ефективного забезпечення кібербезпеки для економіки країни, національної безпеки та захисту особистих даних громадян. Було чітко сформовано та визначено поняття «ринок кібербезпеки», досліджено окремі його складові. На даних окремих ключових складових, таких як «підготовка кадрів» та «роботодавці» було продовжене подальше більш ґрунтовне дослідження роботи.

Важливим кроком стало дослідження ролі консалтингу у забезпеченні господарської діяльності. Була сформована основна місія діяльності консультанта, важливі професійні та гнучкі навички, якими має володіти компетентний та

кваліфікований фахівець. Це дозволило зрозуміти особливості їх роботи та в чому є їх перевага та важливість на ринку праці.

Визначення необхідного ресурсного забезпечення дозволило розпочати реалізацію консалтингового проєкту. Була проведена робота по збору, аналізу, обробки та представлення даних. У рамках підготовки даних для проведення аналізу для збору інформації щодо пропозиції спеціалістів з кібербезпеки були використані відкриті та закриті дані з Єдиної державної електронної бази з питань освіти (ЄДЕБО) (наприклад, такі як кількість вступників, кількість здобувачів, кількість випускників, тощо) та дані, отримані за рахунок проведення опитування ЗВО щодо спеціальності 125 «Кібербезпека та захист інформації».

Для отримання даних від ЗВО, були розроблені та затверджені відповідні шаблони. Дані шаблони у вигляді форм розсилалися вибраним ЗВО для заповнення ними необхідними даними. Заповнила форми та надіслала відповіді переважна більшість ЗВО. За рахунок проведення опитування ЗВО були отримані дані, що стосуються детальної організації освітнього процесу та підготовки спеціалістів, такі як, наприклад, кількість здобувачів, що беруть участь в CTF змаганнях, інформація про здобувачів та випускників, які працюють за спеціальністю, інформація про кількість професійних сертифікацій у здобувачів та особливості співпраці з компаніям-партнерами У результаті проведення опитувальника було отримано дані від 42 ЗВО, питома вага яких серед загальної кількості здобувачів, які навчаються на 125 спеціальності за 2022-2023 навчальний рік (станом на 01.07.2023) склала 81.4%.

Для аналізу попиту на ринку кібербезпеки були використані закриті дані. Після надсилання запиту до Джерела 1, Джерела 2, Джерела 3, отримані дані були ґрунтовно проаналізовано, визначено актуальність та відповідність отриманих даних до потреб проєкту. Отримані дані автоматизовано оброблялись в таких

програмних продуктах як Excel, Power BI. Був розроблений вичерпний перелік показників та користувацьких інтерфейсів, інформаційні панелі, які відображають індикатори, індекси та показують тенденції на ринку праці в сфері кібербезпеки. На основі цього переліку були розроблені графічні моделі в середовищі Power BI. Кожен показник було детально описано та обґрунтовано актуальність його визначення та представлення. На кожному кроці виконання проєкту були проведені погодження щодо виконаних етапів із замовником проєкту та затверджені наступні кроки. Комунікація відбувалася регулярно, щотижня. Всі отримані зауваження, коментарі та побажання враховувалися.

У результаті створення автоматизованого інструменту кінцевий користувач отримав актуальний та детальний аналіз попиту та пропозиції ринку спеціалістів з кібербезпеки за 2018-2022 роки з можливістю проведення аналогічного дослідження у майбутньому та автоматизованому оновленні даних. Створений інструмент буде зручним та зрозумілим у користуванні як і тим, хто має мінімальний досвід користування Power BI, так і просунутим користувачам.

Проаналізувавши ситуацію на ринку підготовки спеціалістів з кібербезпеки, можна зробити наступні висновки. Дослідження ринку попиту кібербезпеки показало стрибок кількості відкритих вакансій на 80.8% у 2021 році. Таким чином, бізнес реагував на стрімкий розвиток інформаційних технологій та тенденцію до діджиталізації України. Важливу роль в цьому зіграли і обмеження під час ковіду, коли різноманітні установи зіштовхнулись з проблемою дистанційного способу ведення справ. Керівники компаній почали впроваджувати стратегії по забезпеченню кібербезпеки своїх потреб. Відповідно, це призвело до збільшення попиту та потреби до залучення великої кількості нових кадрів.

На такий попит у фахівцях з кібербезпеки реагували і ЗВО, які відповідальні за задоволення потреб ринку шляхом корегування пропозиції для

абітурієнтів та вступників та підготовки нових кадрів. Вже з 2016 року ЗВО активно збільшували ліцензовані обсяги на спеціальність 125 «Кібербезпека». Як наслідок, зростала і кількість вступників, які, починаючи з 2020 року, стали потужною базою для забезпечення потреб ринку у фахівцях. Проте ринок попиту зіштовхнувся з проблемою недостатньої кваліфікації нових фахівців. Про це говорить статистика 2018-2022 року щодо низької кількості здобувачів, що мають професійні сертифікації у порівнянні з вакансіями, що вимагають наявність таких сертифікацій. В середньому лише менше 10% від усієї кількості здобувачів мали необхідні професійні сертифікації.

Також, під час проведення аналізу розглядалися показники, пов’язані з організацією освітнього процесу у ЗВО. Погіршення забезпечення та надання освітнього процесу могло спричинити і збільшення навантаження на викладачів профільних кафедр. Особливі стрибки навантаження спостерігаються в 2019 році (на 34% або до 19 студентів на одну ставку) та 2021 році (на 17% або до 22 здобувачів на одну ставку). Це пов’язано з тим, що кількість здобувачів в 2019 зросла на 25%, а кількість викладацьких ставок профільних кафедр навпаки впала на 6%. Щодо 2021 року, то кількість здобувачів зросла на 18%, а кількість викладацьких ставок зросла лише на 0.9%. Варто зауважити, що ЗВО реагують на збільшення кількості здобувачів, шляхом збільшення кількості викладацьких ставок, але із запізненням в один рік.

Однак варто виокремити позитивні тенденції щодо спроб підвищення якості підготовки здобувачів. Починаючи з 2020 року відбувається збільшення кількості ЗВО, здобувачі яких брали участь в CTF-змаганнях на 58% в 2021 році, та на 150% у 2022 році та збільшення кількості ЗВО, що мали доступ до платформ «кіберполігонів» в середньому на 90% щорічно, починаючи з 2020 року.

Особливо важливим етапом покращення якості підготовки здобувачів стало впровадження дуальної форми навчання в ЗВО. У результаті цього запровадження спостерігалось збільшення відсотку ЗВО, що мають дуальну форму навчання, у співвідношення до загальної кількості ЗВО в 2020 та 2021 році на 200% та 64% відповідно. Дана позитивна тенденція пояснюється інформацією, яка надається Міністерством освіти та науки України щодо запровадження пілотного проєкту дуальної освіти в Україні в 2015 році та активний його розвиток, починаючи з 2019 року. Рушієм розвитку дуальної освіти в ЗВО став зріст зацікавленості реального сектору економіки у співпраці з закладами освіти та підготовки спеціалістів, які отримують практичні знання. Такі здобувачі після закінчення навчання є більш конкурентними та краще підготовленими до роботи на реальному ринку.

Підсумовуючи дані з отриманого дослідження можна стверджувати, що реальний ринок в сфері інформаційної та кібербезпеки дійсно активно розвивається. Попри спади попиту в 2022 році на 30% у зв’язку з воєнною ситуацією в країні, спостерігається тенденції до зросту цього ринку. На зріст попиту активно відреагували ЗВО, шляхом відкриття спеціальності 125 «Кібербезпека та захист інформації» у своїх навчальних підрозділах. Кількість ЗВО, що готує здобувачів за ступенем Бакалавра, у 2022 році зросла на 10%, попри воєнну ситуацію в країні, що говорить про збереження попиту на дану спеціальність, навіть попри воєнну ситуацію в країні. Активно збільшується щорічний абсолютний приріст вступників. Ефективним є залучення міжнародних фондів в освітній процес, що відображається на реальному прирості кількості проведених CTF-змагань та розширення доступу здобувачів до кіберполігонів. Все це сприяє розвитку та отриманню більш практичних та фахових навичок у здобувачів ЗВО. Проте найбільшою проблемою залишається низька кількість професійних сертифікацій, яку мають здобувачі ЗВО. Саме цей показник є

ключовим при відборі нових співробітників компаніями з реального ринку кібербезпеки.

Були надані пропозиції щодо підвищення ефективності підготовки кадрів. Вони були сформовані на основі трьох найбільш ефективних та дієвих способах здобуття практичних навичок та набуття цінності на ринку праці здобувачами освіти, а саме: активна взаємодія, співпраця та стажування з профільними компаніями в галузі кібербезпеки, розвиток професійних та гнучких навичок за рахунок участі в спеціалізованих змагань з кібербезпеки, підтвердження здобутих знань за рахунок професійних сертифікацій із заохоченням до цього з боку закладів вищої освіти. Окремо досліджувалось питання доцільності до ефективності розвитку дуальної освіти. Було проаналізовано ключові дослідження цієї теми, останні звіти профільних департаментів Міністерства освіти та науки України, матеріали конференцій присвячених даній тематиці, та апробовано частину матеріалів даної роботи на одній з таких конференцій. Було встановлено, що в умовах сучасних реалій вищої освіти це є найбільш дієвий, ефективний, ба більше, найбільш швидкий спосіб підняття якості та ефективності підготовки кадрів в сфері кібербезпеки.

Окремо варто зазначити важливість отриманих аналітичних даних для формування стратегії підготовки кадрів в сфері кібербезпеки. Вони стали першим та найважливішим етапом формування усієї стратегії, джерелом формулювання аналітичних висновків, рекомендацій та шляхів до покращення ефективності її формування. Щоб розуміти чи є стратегія ефективною, чи вдалось досягти результатів треба розуміти з якими показниками ефективності варто працювати в першу чергу. Для цього була розроблена комплексна система ключових показників ефективності. Також було розраховано відповідні вагові коефіцієнти до кожного показника, щоб компетентний фахівець міг оцінити ефективність впровадження стратегії, знаючи вагове значення кожного показника. Такий підхід дозволить не

лише розробити теоретичні аспекти стратегії а і надати реальні практичні важелі для її оцінки, щоб за можливості можна було вчасно її або відкоригувати, або навіть і змінити напрямок та сутність стратегії за необхідності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Державна служба спеціального зв'язку та захисту інформації України. Офіційний веб-сайт. URL: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit (дата звернення 15.06.2023)

2. Податковий кодекс України від 2 грудня 2010 року. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text (дата звернення 19.06.2023)

3. Марченко О. С. Бізнес-консалтинг : навч. посібник – Харків : Право, 2019. – 204 с.

4. Державна служба статистики. Класифікація видів економічної діяльності. URL: https://kved.ukrstat.gov.ua/KVED2010/kv10_i.html (дата звернення 19.06.2023)

5. Державна служба статистики. Обсяг реалізованих послуг за регіонами за видами економічної діяльності. URL: https://ukrstat.gov.ua/operativ/operativ2018/posl/arh_dpsp_19.html (дата звернення 15.10.2023)

6. Еволюція українського консалтингу. URL: http://anatoleach.livejournal.com/8931.html (дата звернення: 01.07.2023)

7. Business support 2023: провідні українські консалтингові компанії . URL: https://delo.ua/business/business-support-2023-pyat-providnix-ukrayinskix-konsaltingovix-kompanii-424308/ (дата звернення 19.06.2023)

8. Десятко А.М. Кібергігієна. Безпека держави: Матеріали наукових семінарів. – Київ: КНТЕУ, 2020. - 101с.

9. Краус Н., Краус К. Цифровізація в умовах інституційної трансформації економіки: базові складові та інструменти цифрових технологій. Інтелект XXI століття, 2018. – 280с.

10. Бойко О.В., Пушак Я.Я., Трушкіна Н.В. Формування сучасної парадигми інформаційної безпеки національної економіки: теоретичні засади. Вісник післядипломної освіти. Сер.: Соціальні та поведінкові науки. 2022. Вип. 22 (51). С. 139-160.

11. Орловська Ю.В., Кахович О.О. Необхідність публічного управління розвитком інформаційно-комунікаційних технологій в умовах формування світової цифрової економіки. Державне управління: удосконалення та розвиток. 2020. № 11. URL: http://www.dy.nayka.com.ua/pdf/11_2020/3.pdf (дата звернення: 20.06.2023).

12. Ткачук Г.О. Цифрові трансформації: взаємозв'язок із системою економічної безпеки підприємства. Економіка харчової промисловості. 2019. Т. 11. Вип. 4. С.42

13. Л. С. Шевченко, Стратегічний бізнес-консалтинг. Харків: Національний юридичний університет імені Ярослава Мудрого, 2019.

14. М. Ф. Безкровний та М. Ф. Кропивко, "Управлінський консалтинг", Підручник. Київ, Україна: Ліра-К, 2015.

15. М. Л. Гончарова, "Управлінське консультування в Україні: основні проблеми, тенденції та напрями розвитку", Економіка та управління національним господарством, № 2(164), С. 136 -141, 2015.

16. С. М. Ілляшенко, "Ключові чинники успіху управлінського консультування". URL: http://www.economy.nayka.com.ua/?op=1&z=969 (дата звернення: 15.07.2023)

17. Що заважає розвиватися цифровій економіці України? [Електронний ресурс]. URL: http://forbes.net.ua/ua/business/1363657 (дата звернення: 15.07.2023)

18. В. В. Стадник, Стратегічне управління інноваційним розвитком підприємства. Хмельницький, Україна: ХНУ, 2011.

19. Е. І. Цибульська, Управління потенціалом підприємства, Харків, Україна. НУА: -2011, 382 с.

20. К. Величко, Е. Цибульська. Трансформація бізнес-моделей компаній: сучасні виклики та перспективи у цифровій економіці. Економіка та суспільство, 2023, В.52. URL: https://doi.org/10.32782/ (дата звернення: 20.07.2023)

21. І. З. Должанський, Т. О. Загорна, О.О, Удалих. Управління потенціалом підприємства: навч посібник К.: Центр навч. л-ри, 2008. - 367 с.

22. Прохорова В. В., Проценко В. М., Чобіток В. І. Формування конкурентної стратегії підприємств на засадах інноваційно-спрямованого інвестування: монографія. Харків: Українська інженерно-педагогічна академія, 2015. 291 с.

23. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. URL: https://zakon.rada.gov.ua/ (дата звернення 22.07.2023)

24. Закон України Про інформацію. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 22.07.2023)

25. Закон України Про доступ до публічної інформації. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 22.07.2023)

26. Єдина державна електронна база з питань освіти. URL: https://info.edbo.gov.ua/ (дата звернення 22.07.2023)

27. Дрозд І., Маковець О. Кібербезпека як фактор фінансової безпеки підприємства. Економіка. Фінанси. Право. 2020. В. 5/3, С.31–35

28. Панченко, Марина. Цифрова трансформація як напрям післявоєнного відновлення та реалізації інноваційно-інвестиційного потенціалу України. Економіка та суспільство, 2023, В. 51.

29. Закон України Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 22.07.2023)

30. Вітер С., Світлишин І. Захист облікової інформації та кібербезпека підприємства. Економіка і суспільство. 2017. Вип.11, С.497–502

31. Жора В. Кібербезпека потребує кадрів: чому держава та бізнес повинні співпрацювати. Економічна правда. 2023. URL: https://www.epravda.com.ua/columns/2023/ (дата звернення 02.10.2023)

32. Бисторва Б. Особливості формування системи професійної підгтовки майбутніх бакалаврів з кібербезпеки у ВНЗ США. Вісник Черкаського університету. 2017. Серія: Педагогічні науки, 6, 15-19.

33. Бурячок В. Л. Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «Інформаційні технології». Сучасний захист інформації. 2016. № 2. С. 4-9

34. Мельник С. Оптимізація фахової підготовки майбутніх фахівців з кібербезпеки на основі інноваційної педагогіки та інтегрованого підходу в системі реалізації ключових компетенцій безпеки в інформаційному суспільстві. Витоки педагогічної майстерності. Серія : Педагогічні науки. 2018. Вип. 21. С. 125-129.

35. «Влада без стратегії не може бути конструктивною» // Дзеркало тижня. Анатолій Гальчинський / 28.10.2018.

36. Лібералізм: уроки для України: наук.-попул. есе / Анатолій Гальчинський. - К. :Либідь, 2011. - 288 с.

37. Політична економіка Лівану, 1948–2002: Межі принципу невтручання / Туфік Гаспар. - Лейден: Brill, 2004. – 311с.

38. Міністерство освіти. Дуальна освіта. URL: mon.gov.ua (дата звернення 08.10.2023)

39. Арсенович, Л. Удосконалення механізмів формування системи підготовки кадрів у сфері кібербезпеки в умовах державно-приватної взаємодії. Науковий вісник: Державне управління, 2022. В. 1, С. 6–27.

40. Мельник С. Концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки. Педагогічні науки: теорія, історія, інноваційні технології. 2016. № 10. С. 79-88.

41. Марков В. В. Особливості впровадження зарубіжного досвіду боротьби з кіберзлочинністю в навчальний процес. Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. 2014. Вип. 12(1). С. 105-107.

42. Gartner Research. Market Share Analysis: Consulting Services, Worldwide, 2022. URL: https://www.gartner.com/en/documents/4465399 (дата звернення 15.06.2023)

43. G. Verlander. The Practice of Professional Consulting. - San Francisco: Pfeiffer, 2012. - 320 p.

44. Lester Evans. What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners. – Bravex, 2019. – 230 p.

45. Raef Meeuwisse. Cybersecurity for Beginners. Lulu Publishing Services, 2015. - 190p.

46. Thomas J. Smedinghoff . Cybersecurity: A Practical Guide to the Law of Cyber Risk. UNKNO, 2015. - 562p.

47. Power BI. URL: https://uk.wikipedia.org/wiki/Power_BI (дата звернення 22.09.2023)

48. MS Excel. URL: https://uk.wikipedia.org/wiki/Microsoft_Excel (дата звернення 22.09.2023)

49. MS Word. URL: https://uk.wikipedia.org/wiki/Microsoft_Word (дата звернення 22.09.2023)

50. KoboToolbox. URL: https://www.kobotoolbox.org/features/ (дата звернення 22.09.2023)

51. Marc Goodman. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. Anchor, 2016. - 608 p.

52. Impact Rankings 2023: quality education. URL: www.timeshighereducation.com. (дата звернення 02.10.2023)

ДОДАТКИ

№	Назва ЗВО	Вага, 2022
15	Харківський національний університет імені В.Н. Каразіна	1.82%
16	Національний університет 'Запорізька політехніка'	1.67%
17	Національний університет 'Чернігівська політехніка'	1.62%
18	Національний технічний університет 'Харківський політехнічний інститут'	1.61%
19	Тернопільський національний технічний університет імені Івана Пулюя	1.60%
20	Хмельницький національний університет	1.54%
21	Харківський національний економічний університет імені Семена Кузнеця	1.48%
22	Національний аерокосмічний університет ім. М. Є. Жуковського 'Харківський авіаційний інститут'	1.34%
23	Чернівецький національний університет імені Юрія Федьковича	1.31%
24	Центральноукраїнський національний технічний університет	1.30%
25	Київський університет інтелектуальної власності та права Національного університету 'Одеська юридична академія'	1.29%
26	Національний університет 'Одеська юридична академія'	1.29%
27	Львівський державний університет безпеки життєдіяльності	1.26%
28	Національний університет біоресурсів і природокористування України	1.19%
29	Київський національний університет будівництва і архітектури	1.07%
30	Державний вищий навчальний заклад 'Ужгородський національний університет'	1.05%
31	КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА	1.03%
32	Черкаський державний технологічний університет	0.92%
33	Львівський національний університет імені Івана Франка	0.90%
34	Університет митної справи та фінансів	0.90%
35	Луцький національний технічний університет	0.88%
36	Український державний університет науки і технологій	0.76%
37	Національний університет кораблебудування імені адмірала Макарова	0.71%

38	Державний біотехнологічний університет	0.70%