

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ"
Факультет соціальних наук і соціальних технологій
Кафедра соціології

ДОСЛІДНИЦЬКА РОБОТА

ДОСТУП ЖІНОК ДО СФЕРИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

виконана в межах курсу “Вступ до гендерних студій” (зима-весна 2025 року)

Координаторка дослідження:

Тамара Марценюк, кандидатка соціологічних наук, доцентка кафедри соціології НаУКМА;

Координатор(к)и дослідницьких груп:

Софія Хессін, Володимир Гривцов, Ростислав Сидоров, Іуліанія Семерникова, Софія Квят, Діана Бойко; за участі Катерини Заремби

Авторський колектив:

Слухачі та слухачки курсу “Вступ до гендерних студій” (зима-весна 2025) – деталізовано по підрозділах

Текст за загальної редакції Тамари Марценюк

Консультант(к)и:

Трохим Бабич, керівник бакалаврської програми з кібербезпеки НаУКМА, консультант дослідження

Анна Прохорова, старша викладачка кафедри соціології НаУКМА, консультантка з питань якісних методів

Анастасія Островська, співзасновниця та CEO WLSIF, власниця агенції Ostrovska Consulting, консультантка з питань стратегічних комунікацій, жіночого лідерства та розвитку професійних спільнот у сфері кібербезпеки

Технічне рецензування:

Софія Колісник, студентка кафедри філології НаУКМА

Літературна редакція:

Софія Колісник, студентка кафедри філології НаУКМА

Виконано у співпраці з ГО “Фундація жіночого лідерства та стратегічних ініціатив”

Зміст

Вступ	4
Розділ 1. Доступ жінок до сфери кібербезпеки у світі	6
1.1. Міжнародний досвід залучення жінок до кібербезпеки: освіта і ринок праці	6
1.1.1. Жінки у кіберсфері: історична перспектива	6
1.1.2. Освіта жінок в кібербезпеці: ключові аспекти	9
1.1.3. Ринок кібербезпеки: цивільна та військова сфери	10
1.2. Виклики та успіхи залучення жінок у сферу кібербезпеки	14
1.3. Досвід подолання бар'єрів. Протидія дискримінації та гендерним стереотипам у кібербезпеці	17
Розділ 2. Залучення жінок до кібербезпеки в Україні	24
2.1. Статистична інформація про жінок у кібербезпеці: освіта та ринок праці.	24
2.1.1. Жінки у закладах вищої освіти на спеціальності кібербезпека в Україні.	24
2.1.2. Жінки у сфері кібербезпеки в світі	27
2.1.3. Жінки в освіті за спеціальністю кібербезпека в Україні.	31
2.2. Ситуація в Україні та щодо регулювання гендерних відносин у кібербезпеці	34
2.2.1. Законодавча база щодо кібербезпеки України	34
2.2.2. Державні ініціативи та програми гендерної інклюзії в кібербезпеці	37
2.2.3. Війна як фактор актуалізації гендерного виміру в безпековому секторі	40
2.2.4. Ініціативи бізнесу та приватного сектора щодо забезпечення гендерної рівності в кібербезпеці	41
2.2.5. Вплив повномасштабної війни на гендерні аспекти кібербезпеки України	45
Розділ 3. Жінки в українській кібербезпеці: голоси тих, які подолали перешкоди.	48
3.1. Результати глибинних інтерв'ю із жінками у кібербезпеці про їхній успішний і проблемний досвід перебування у цій сфері.	48
3.1.1. Методологія дослідження доступу жінок до сфери кібербезпеки в Україні	48
3.1.2. Суспільне сприйняття жінок в кібербезпеці	50
3.1.3. Перешкоди в роботі в сфері кібербезпеки у жінок	54
3.1.4. Персональні досягнення жінок в сфері кібербезпеки	57
3.1.5. Позитивні зрушення у практиках залучення та підтримки жінок в сфері кібербезпеки в Україні	58
3.2. Результати експертних інтерв'ю щодо успіхів і викликів залучення жінок у сферу кібербезпеки в часи російсько-української війни.	60
3.2.1. Методологічні основи опитування щодо успіхів і викликів доступу жінок до сфери кібербезпеки в Україні	60
3.2.2. Виклики у доступі жінок до сфери кібербезпеки в Україні: гендерні стереотипи і упередження	64
3.2.3. Виклики у доступі жінок до сфери кібербезпеки в Україні: горизонтальна гендерна сегрегація	65

3.2.4. Виклики у доступі жінок до сфери кібербезпеки в Україні: вертикальна гендерна сегрегація	68
3.2.5. Виклики у доступі жінок до сфери кібербезпеки в Україні: сексуальні домагання і насильство	70
3.2.6. Успіхи у доступі жінок до сфери в Україні: подолання горизонтальної гендерної сегрегації	71
3.2.7. Успіхи у доступі жінок до сфери в Україні: подолання вертикальної гендерної сегрегації	74
3.3. Українські медіа про жінок у кібербезпеці	75
3.3.1. Методологія аналізу медійних повідомлень	75
3.3.2. Жінки в ІТ та кібербезпеці на ринку праці: залучення та гендерна (не)рівність	77
3.3.3. Освітні програми для жінок у сфері кібербезпеки	79
3.3.4. Жінки у військовій кібербезпеці та обороні	83
3.3.5 Жінки як експертки з кібербезпеки	86
Висновки	88
Рекомендації	93
Рекомендації щодо покращення становища жінок у кібербезпеці	93
Рекомендації щодо доступу жінок до сфери кібербезпеки в Україні: освітні чинники	96
Рекомендації щодо доступу жінок до сфери кібербезпеки в Україні: обізнаність про сферу та можливості жінок	97
Рекомендації щодо доступу жінок до сфери кібербезпеки в Україні: спільнота та підтримка жінок	98
Список використаних джерел	100
Додатки	110
Додаток А. Гайд для проведення напівструктурованого інтерв'ю у дослідженні “Жінки в українській кібербезпеці: голоси тих, які подолали перешкоди”	110
Додаток Б. Гайд для проведення напівструктурованого експертного інтерв'ю у дослідженні “Доступу жінок до сфери кібербезпеки в Україні”	112
Додаток В. Перелік одиниць аналізу	114

Вступ

В умовах глобальної цифровізації кібербезпека постає ключовим елементом міжнародної стабільності та національної безпеки. Її стратегічне значення зростає, особливо у період війни: гібридних загроз, інформаційних тисків та цифрових атак. Проте, попри нагальну потребу у кваліфікованих кадрах, сфера кібербезпеки досі демонструє гендерний дисбаланс: жінки значно менше представлені серед фахівців, ніж чоловіки. Цей розрив зумовлений не лише технічними бар'єрами, а й глибоко вкоріненими соціокультурними установками, стереотипами, які призвели до освітньої сегрегації та браку інституційної підтримки. На зараз міжнародна увага до гендерної нерівності у цій галузі зростає, адже залучення жінок до кібербезпеки набуває особливої актуальності, з огляду на ефективне використання загального людського потенціалу для протидії сучасним кіберзагрозам.

На глобальному рівні дедалі більше уваги приділяється ініціативам, спрямованим на розширення участі жінок у галузі кібербезпеки. Впроваджуються освітні програми, професійні спільноти та державні політики, що націлені на подолання бар'єрів серед жінок у цій сфері. Усвідомлення значущості кадрового різноманіття базується не лише на принципах рівності, а й на доказах того, що гендерно збалансовані команди в кібербезпеці є більш гнучкими, інноваційними та здатними до ефективного адаптування у кризових умовах.

Отже, дослідження міжнародного досвіду залучення жінок до сфери кібербезпеки є важливим, оскільки дозволяє виявити бар'єри та чинники успішної інтеграції жінок у цифрову сферу. За допомогою цього, жінки можуть показати інші сторони проблеми та знайти додаткові рішення для їх розв'язання.

При цьому важливо враховувати, що нерівне представництво жінок у кіберсфері має глибше коріння. Ще на етапі освіти дівчата стикаються зі стереотипами щодо "нежіночності" технічних спеціальностей, що впливає на їхню самовпевненість, вибір професії та подальше професійне зростання.

Приклади з різних країн можуть слугувати орієнтиром для України у впровадженні більш інклюзивної кіберполітики та у подоланні гендерної нерівності. Їхній досвід переконливо свідчить, що подолання гендерного дисбалансу у кіберсфері потребує багаторівневої стратегії: залучення дівчат з раннього віку до STEM-освіти; створення організацій, що спрямовані на розвиток саме жінок у сфері кібербезпеки; впровадження гендерно чутливого законодавства; підтримка системної боротьби зі стереотипами. За допомогою вивчення результативних міжнародних практик і підходів можна розробити ефективні рекомендації для формування стійкого та гендерно збалансованого середовища. Успішні приклади таких реформ вже демонструють свої результати, наприклад, у формі менторських програм (CyberFirst, WiCyS), корпоративних та державних ініціатив (стипендії, квоти).

Отже, на тлі світових тенденцій та міжнародних практик актуалізується потреба у дослідженні національного контексту. Україна, яка перебуває у стані тривалої війни, розвиває свою діджиталізацію, хоч і наражається на унікальні випробування.

У таких умовах кібербезпека України набуває виняткової стратегічної ваги, що підкреслює питання ефективного залучення всього національного потенціалу, включно з гендерним виміром цієї критичної сфери. Вторгнення росії спричинило значні зміни в країні, так як вагома частина чоловіків зазнали мобілізації, що призвело до відчутного кадрового дефіциту. У цій ситуації жінки почали активніше залучатися до кіберсфери, заповнюючи професійні ніші та демонструючи свою майстерність. Таким чином, сама війна сформувала складну динаміку нових “вікон можливостей” для жінок у цій традиційно мускулінній галузі.

Водночас жінки, потрапляючи в цю сферу, стикаються з численними бар’єрами, зокрема з кібернасильством, що негативно впливає на їх емоційний стан та професійний розвиток. Чимало чинників створюють перешкоди для жінок у кіберсфері, наприклад, несвідомі, так і відкриті прояви дискримінації на роботі, упередження щодо компетентності та нерівна оплата праці. Проте, програми, які цілеспрямовані на підтримку жінок, демонструють позитивні результати у збільшенні їхньої присутності на робочому місці та міжнародному ринку праці.

Дане дослідження має на меті здійснити комплексний аналіз сучасного стану гендерних відносин у сфері кібербезпеки України, з акцентом на зміни, що відбуваються внаслідок повномасштабної війни. У роботі послідовно розглядаються аспекти державної політики та законодавства, ініціативи бізнес-середовища, а також безпосередній вплив воєнного часу на професійні траєкторії жінок, наявні перешкоди та перспективи для досягнення реальної гендерної рівності й посилення кіберстійкості країни.

Розділ 1. Доступ жінок до сфери кібербезпеки у світі

Хессін Софія, Денисова Грета, Кукурік Марія, Ларькова Юлія, Решетнік Анастасія

1.1. Міжнародний досвід залучення жінок до кібербезпеки: освіта і ринок праці

1.1.1. Жінки у кіберсфері: історична перспектива

Станом на 2024 рік, жінки складають 36% кадрів у сфері ІТ, однак у сфері кібербезпеки їхня частка менша – лише 24%¹. Очікується, що до 2025 року цей показник зросте до 30%². Кібербезпека, як сучасна технологічна спеціалізація, базується на міждисциплінарних знаннях і навичках, які формуються в межах STEM-освіти (Science, Technology, Engineering, Mathematics). Саме ці напрями забезпечують розвиток критичного мислення, аналітичних навичок і компетентностей, необхідних для участі у технологічно складних сферах майбутнього, таких як інформаційні технології, штучний інтелект та цифрова безпека³. Однак яким чином жінки потрапили до сфери комп'ютерних наук, коли зараз ця сфера вважається специфічно “чоловічою”?

Активне залучення жінок до роботи з комп'ютерами розпочалося ще у 1940-х роках⁴. Досвід роботи жінок у комп'ютерній сфері, пов'язаний з механізмами для розрахунків, почав формуватися ще в довоєнний період. До інших технічних та промислових професій жінки були залучені вже під час Другої світової війни.

До початку 1940-х жінки займалися розрахунками, бухгалтерською роботою та виконували обов'язки канцеляристок, завдяки чому могли проявляти себе як ефективні працівниці, яких було легко навчати⁵. У Британії з розвитком машинної справи саме жінки ставали операторками даних механізмів, оскільки їх було більше, ніж чоловіків, а також через **гендерні стереотипи**: чоловіки виконували складнішу роботу та вважалися “годувальниками” родини. Водночас економічна ситуація країни сприяла тому, що жінки займалися не тільки неоплачуваною репродуктивною працею, але й погоджувались на низькооплачувану роботу, пов'язану з машинами. Однією з причин низької оплати праці жінок був стереотип про них, як про тимчасових та допоміжних робітниць, які рано чи пізно покинуть роботу задля репродуктивної праці вдома. На початку ХХ століття машинна робота почала вважатися неprestижною та індустріальною, проте саме на її результати спиралася

¹ Global Cybersecurity Forum & Boston Consulting Group. (2024). *2024 cybersecurity workforce report: Bridging the workforce shortage and skills gap*. p. 15.

² Osborne, C. (2023, 27 березня). Women to hold 30 percent of cybersecurity jobs globally by 2025. *Cybercrime Magazine*.

³ Танська, В., Майданюк, І., Овчаренко, О., Денисенко, А., & Стрілецька, Н. (2024). STEM, як інноваційна стратегія інтегрованої освіти: світовий досвід та перспективи. *Перспективи та інновації науки*. с. 596-597.

⁴ Hicks, M. (2017). *Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing*. MIT press. p. 1.

⁵ Там само, p. 21.

інтелектуальна праця офісних робітників та бюрократичної системи. Незважаючи на це, машинна робота жінок стала незамінною для підтримки життєздатності уряду та інституцій Великої Британії⁶.

Дефіцит чоловічої робочої сили під час Другої світової війни стимулював жінок до освоєння нових професій, попередньо “чоловіча” сфера комп’ютерних технологій не стала виключенням⁷. Британія почала формувати списки жінок, які могли б займати місця чоловіків у найважливіших галузях промисловості, тоді для них відкрилися можливості кар’єрного зросту, які були значно обмежені у довоєнний період. Основною сферою, куди направляли жінок, була інформаційна обробка (військова інформація, логістика та аналіз даних). Поки чоловіки були зайняті в армії, жінки становили основу британської інформаційної сфери, посідали більшість керівних посад, деякі навіть ставали частиною армії та флоту, завдяки чому доводили, що жінок можна вважати рівними чоловікам⁸. Варто зазначити, що навіть у воєнний період у Великій Британії продовжували існувати стереотипи, що жінки це перш за все – матері та дружини, а потім військові та машиністки.

Після запуску у США першого цифрового комп’ютера: the Electronic Numerical Integrator and Computer (ENIAC), чоловікам доручили престижну та складну розробку апаратного забезпечення, тоді ж як робота кодувальниць та програмісток, що займались технічним програмуванням машин, тобто “легшою” роботою – залишалась невидимою. Поки військове міністерство США заохочувало роботу жінок у військовій та цивільних сферах, загалом позитивно описувало їх внесок в медіа, у новинах про такий важливий проєкт, як ENIAC, основну славу отримували чоловіки, а про роботу жінок, які відігравали ключову роль у його програмуванні, не згадували взагалі⁹.

Протягом 1950-60-их років відбулося перетворення комп’ютерів з громіздких машин на більш універсальні апарати, які стали доступними не лише уряду, але й іншим підприємствам. Тоді як за чоловіками були зарезервовані більш кваліфіковані сфери, жінки здобували досвід та розвивались у канцелярській справі – програмуванні. Репутація комп’ютерного програмування як “жіночої” роботи створила можливості для їхнього розвитку у цій сфері: успіхи жінок підкріплювалися їхньою репутацією як швидких та здібних до навчання робітниць.

Жінок у сфері програмування стало так багато, що у квітні 1967 року Лоїс Мандель у статті журналу *Cosmopolitan* “The Computer Girls” (Комп’ютерні дівчата) зазначала, що комп’ютерне програмування вимагає терплячості, та уваги до деталей, чим саме наділені жінки, а не чоловіки. “Жінки є природженими для комп’ютерного програмування”, – а тому мають перевагу у цій сфері¹⁰. Це була майже єдина розумова робота, де жінки змогли заробляти непогані гроші – близько 20 000 доларів на рік на той час. Попри те, що комп’ютерне програмування початково було технічно складною професією, яка вимагала високого рівня навичок друку та

⁶ Там само, р. 25.

⁷ Там само, р. 26.

⁸ Там само, pp. 26-27.

⁹ Light, J. S. (1999). When Computers Were Women. *Technology and Culture*. p. 473.

¹⁰ Mandel, L. (1967, квітень). The computer girls. *Cosmopolitan*. p. 52.

швидкості аналізу, нижча вартість праці жінок негативно впливала на їхній статус: їх вважали менш цінними працівниками, які не могли виконувати роботу вищого рівня, як чоловіки. Коли чоловіки не змогли повністю замінити жінок, як операторів машин, то наслідком стала **фемінізація** програмування – робочі місця операторок машин довелося розбити на дрібніші завдання, щоб вони відповідали “фемінізованим” категорії, хоча саме жінки переважно виконували роботу з машинами раніше¹¹.

З середини 1960-х років почалося масове витіснення жінок зі сфери програмування, яка набула виразно **маскулінного** вигляду – почала сприйматися як престижна, більш технічно складна і “чоловіча” професія. Розвиток технологій призвів до ускладнення процесів галузі – аналізу, кодування, планування тощо, що вимагало культивування унікальних навичок, які розвивали чоловіки через більший доступ до ремісничих практик. Програмування почало сприйматись як явище, незрозуміле для більшості населення, у якому робиалася лише обмежена група спеціалістів¹². Загалом, коли гендерний склад галузі змінюється, що стало з комп’ютерним програмуванням у 1960-х, то змінюється й зміст роботи галузі: коли домінують чоловіки, робота вважається престижною та складною, а коли жінки – простою та менш вимогливою до специфічних навичок. “Маскулінне” програмування активно підвищувало статусність професії через професійні асоціації, що не включали жінок: формальні програми з інформатики, професійні журнали й товариства тощо¹³.

У результаті до 1970-х років сфера програмування стала відверто сексистською. У професійних журналах існували принизливі жарти про жінок, їхні навички та емоційність, що сприяло поширенню ідей “*програмування, як маскуліної сфери*”, де емоції заважають, а потрібна розсудливість та адаптивність¹⁴. Наприклад, у 1970 році в США жінки становили вже 38% усієї робочої сили, однак лише 8% серед працівників STEM¹⁵. Жіночий рух у 1970-х був спрямований на усунення бар’єрів, що заважали жінкам стати кваліфікованими спеціалістами різних галузей. Результатом стало те, що образ жінки в комп’ютерній сфері змінювався на більш позитивний. Успіхи фемінізму призвели до того, що три великі комп’ютерні фірми – IBM, Control Data та Burroughs Corporation сприяли практикам гендерного різноманіття на робочому місці¹⁶.

1980-ті роки не змогли продовжити успіх феміністичного руху: фінансова дерегуляція економіки США, що настала у 70-х, сприяла скороченню кількості робітників багатьох компаній, збільшення міжнародної конкуренції та неолібералізм зменшили інвестиційні потенціали більшості американських компаній у навчання

¹¹ Hicks M. (2017). *Programmed Inequality How Britain Discarded Women Technologists and Lost Its Edge in Computing*. pp. 75-77.

¹² Kim, H. H. (2020, 14 вересня). *Computing’s gender divide: Why tech is stuck in the 1980s*. Welcome to the Jungle.

¹³ Ensmenger, N. (2010). Making Programming Masculine. In *Gender Codes: Why women are leaving computing*, T.J. Misa (Ed.). p. 121.

¹⁴ Kim, H. H. (2020, 14 вересня). *Computing’s gender divide: Why tech is stuck in the 1980s*.

¹⁵ Gwinn, M. (2022, 11 лютого). *Why representation matters for girls and women in STEM*. US EPA.

¹⁶ Kim, H. H. (2020, 14 вересня). *Computing’s gender divide: Why tech is stuck in the 1980s*.

працівників, а тому скорочення переважно стосувалися жінок. Багато компаній фактично скасували внутрішні зміни, спрямовані на підтримку гендерної рівності, започатковані жіночим рухом у 1970-х¹⁷. Додатково випуск домашніх комп'ютерів також став однією з причин малої кількості жінок в програмуванні 1980 та 90-х – у той час, коли чоловіки очолювали професійну комп'ютерну сферу, медіа просували образ комп'ютера, як “іграшки для хлопців”, таким чином сприяючи гендерній стереотипізації роботи з комп'ютерами, як “чоловічої праці”¹⁸.

1.1.2. Освіта жінок в кібербезпеці: ключові аспекти

Варто зазначити, що гендерна сегрегація бере початок ще у шкільному віці, коли дівчат менше заохочують до вивчення технічних предметів. Тож заклади вищої освіти (ЗВО), де є спеціальності, пов'язані з інформаційною безпекою, нерідко мають вкрай малу кількість саме студенток – більшу частину абітурієнтів займають хлопці. Це показує, що освіта відіграє важливу роль у формуванні гендерно збалансованого цифрового майбутнього¹⁹.

Згідно з даними NCWIT (National Center for Women & Information Technology), у 2022 році жінки становили лише 23% випускників бакалаврату у сфері комп'ютерних і інформаційних наук у США²⁰. Це вказує на недостатню представленість жінок ще на етапі освіти, зокрема у кібербезпеці. Низка ініціатив намагається змінити цю ситуацію. Наприклад, у США діє програма CyberCorps: Scholarship for Service, яка фінансується Національним науковим фондом (NSF) і адмініструється урядом США²¹. Програма наголошує на залученні представників недостатньо репрезентованих груп, включаючи жінок, до національного сектору кібербезпеки, надаючи стипендії студентам бакалаврату, магістратури та аспірантури в обмін на обов'язкове працевлаштування в державних структурах після завершення навчання²². У США активно діє і міжнародна організація Women in CyberSecurity (WiCyS), що була створена у 2013 році також за підтримки Національного наукового фонду (NSF). Вона об'єднує студенток, викладачок та фахівчинь галузі, надаючи менторство, кар'єрну підтримку та можливості нетворкінгу. Зокрема, університет Джорджа Вашингтона має офіційне студентське представництво WiCyS, що проводить тренінги, воркшопи та кар'єрні події, орієнтовані на лідерство жінок у цифровій безпеці²³.

Водночас деякі глобальні компанії розробляють власні практики підтримки жінок, зокрема після перерви в кар'єрі. Яскравим прикладом є ініціатива IBM Tech “Re-Entry Program”. Ця програма орієнтована на технічних фахівчинь, які мали

¹⁷ Там само.

¹⁸ Devlin H. & Hern A. (2017). Why are there so few women in tech? The truth behind the Google memo. *The Guardian*.

¹⁹ Blackburn, H. (2017). The status of women in STEM in higher education: A review of the literature 2007–2017. *Science & Technology Libraries*. pp. 244-246.

²⁰ National Center for Women & Information Technology. (2024). *By the numbers*.

²¹ U.S. Office of Personnel Management. (2025). *CyberCorps: Scholarship for Service (SFS)*.

²² National Science Foundation (NSF). (2023). *CyberCorps: Scholarship for Service (SFS). Program Solicitation*.

²³ Women in CyberSecurity (WiCyS). (2025a). *Training Programs*.

вимушену паузу в роботі (наприклад, через декретну відпустку), і прагнуть повернутися в ІТ-сферу (аналітика, програмування, кібербезпека тощо). Учасниці проходять оплачуване стажування, беруть участь у практичних проєктах, відвідують адаптаційні тренінги та отримують менторську підтримку. Після завершення програми більшість жінок отримують постійні контракти в ІВМ або інші пропозиції на ринку праці. Програма активно реалізується в США, Канаді, Великобританії, Німеччині, Індії та Австралії, і за словами організаторів, сприяє не лише подоланню кар'єрних розривів, але й формуванню більш інклюзивного корпоративного середовища²⁴.

Сучасна кібербезпека є прикладом галузі з вираженою вертикальною і горизонтальною **гендерною сегрегацією**²³. Жінки не лише менше представлені серед технічного персоналу, але й рідко обіймають керівні посади. Теорія **скляної стелі** (glass ceiling), розроблена в межах феміністичної соціології, пояснює, що жінкам можуть дозволяти обіймати посади до певного рівня, однак їхнє подальше кар'єрне зростання часто обмежене²⁵. Чоловіки на керівних позиціях схильні допускати жінок до управління нижчого та середнього рівня, але не до найвищих щаблів ієрархії. Ці бар'єри мають як структурний характер (закріплені у внутрішніх політиках організацій), так і поведінковий (пов'язаний із гендерними нормами, стереотипами та очікуваннями щодо "належної" ролі жінки²⁶). Це підтверджують також результати опитування Women in CyberSecurity (WiCyS) у 2023 році, згідно з якими 83% жінок повідомили про принаймні один випадок незалучення на робочому місці²⁷. Основними джерелами таких інцидентів були: керівництво (68%), безпосередні менеджери (61%) та колеги (52%)²⁸.

Попри ці бар'єри, деякі ініціативи демонструють позитивну динаміку. Наприклад, у Великобританії програма The CyberFirst Girls Competition, організована Національним центром кібербезпеки (NCSC), щороку залучає школярок віком 12-13 років до участі в інтерактивних змаганнях з кібербезпеки. У 2023 році понад 8700 дівчат долучилися до конкурсу, що на 24% перевищує кількість 2022 року, і з початку ініціативи у 2017 році загальна кількість учасниць сягає 65 000²⁹.

1.1.3. Ринок кібербезпеки: цивільна та військова сфери

Попри глобальні ініціативи, жінки у сфері кібербезпеки залишаються **меншістю**. За даними ISC2 (The International Information System Security Certification Consortium) на березень 2025 року, середня частка жінок у командах з кібербезпеки

²⁴ IBM. (2025). *Return to the workforce with the IBM Tech Re-Entry Program*.

²⁵ Baxter & Wright як цит. у Приймак, К. (2021). *Бар'єри кар'єрного зростання, з якими зіштовхуються жінки під час служби в Збройних Силах України* (дипломна робота). с. 8.

²⁶ Там само, с. 8.

²⁷ Shein, E. (2023, 31 березня). *Study: Women in cybersecurity feel excluded, disrespected*. TechRepublic.

²⁸ Women in CyberSecurity. (2025c). *Lack of respect, career opportunities lead to exclusion for women in cybersecurity*.

²⁹ National Cyber Security Centre. (2025a). *Schoolgirls across UK prepare to vie for crown of cyber security champion*.

загалом становить лише 22%³⁰. Аналітика LinkedIn (див. *Рис. 1.1.3.1*) у липні 2024 року дає ще більш деталізовану картину: найбільший відсоток жінок спостерігається в Італії та Сінгапурі – по 26,7%, у Канаді – 21,2%, Індії – 20,9%, США – 18,3%, Великобританії – 17,9%, а найменший показник у Німеччині – 14,6%³¹.

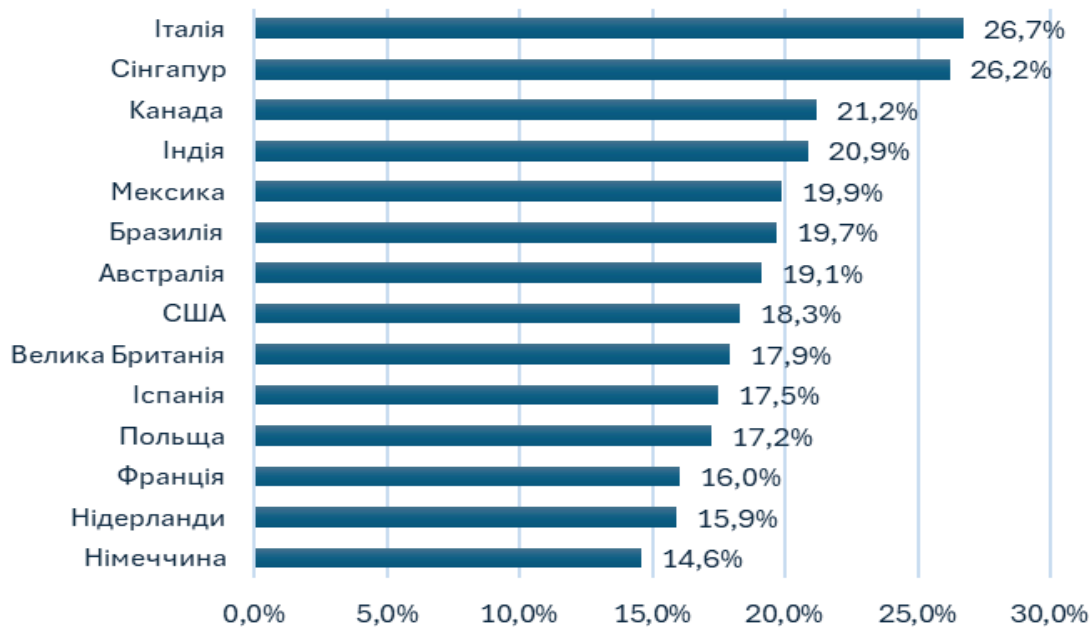


Рис. 1.1.3.1. Частка жінок серед працівників кібербезпеки у 2024, % за країнами
Джерело: LinkedIn Economic Graph. (2024). p. 8

Особливо складна ситуація в країнах Південно-Східної Азії, де жінки становлять 5-25% фахівців галузі. Саме суспільні очікування, гендерні стереотипи та обмежені лідерські можливості частіше виступають основними бар'єрами до їхнього розвитку³². На протипагу цьому було створено програму Ready4Cybersecurity, яка до 2025 року планує надати 100 000 жінкам в Азії освіту та навички у сфері кібербезпеки³³.

У 2024 році жінки становили значну частку кібербезпекових команд у тих галузях, де вони представлені: у сфері хмарних сервісів та будівництва відзначали найбільшу частку жінок у таких командах – 27%, у сфері нерухомості це 26%, а у галузі розробки програмного/апаратного забезпечення та роздрібної торгівлі – 25%³⁴.

³⁰ ISC2. (2024b). *Women in cybersecurity: Inclusion, advancement and pay equity are keys to attracting and retaining more women.*

³¹ LinkedIn Economic graph. (2024). *Global Demand for Cybersecurity Talent Continues to Cool.* p. 8.

³² Bouher, K. (2024, 3 вересня). *Unlocking potential: How women can shape Southeast Asia's digital... PGI.*

³³ Там само.

³⁴ ISC2. (2025, 6 березня). *Survey: Women comprise 22% of the cybersecurity workforce.* Cybersecurity Certifications and Continuing Education.

За ними йдуть освіта, здоров'я, некомерційні організації, виробництво та фінансові послуги – 20%. Найменшими частки жінок в командах кібербезпеки юридичної та військової галузей – 19% та 18% відповідно. Разом з цим, жінки обіймають багато керівних або вищих посад у кібербезпеці – 55%, проте до посад вищого керівництва (директор з інформаційної безпеки, з інженерії або технічний директор) належать лише 7%. Варто зазначити, що жінки на вищих та керівних посадах мають сильну освітню базу – 38% мають диплом бакалавра, переважно з STEM-спеціальностей (51% – комп'ютерні науки/кібербезпека, 12% в інженерії), 48% жінок – ступінь магістра або спеціаліста (58% у комп'ютерних науках/кібербезпеці та 12% в інженерії), також 9% мають докторський ступінь³⁵.

Окрім гендерних стереотипів, на досвід роботи у кібербезпеці впливають й скорочення штату. Дослідження ISC2 у 2024 році виявило, що загалом 32% жінок зазначали про скорочення з місць роботи у кібербезпеці, проти 23% чоловіків³⁶. Разом з цим, прямі (зі штату кібербезпеки організації) та непрямі (звільнення з іншої частини організації) негативно впливають на рівень задоволення роботою: у 2022, 82% жінок та 73% чоловіків були задоволені роботою у кібербезпеці, тоді як у 2025 – показник опустився до 67% та 66% відповідно. Станом на 2024 рік (див. *Рис. 1.1.3.2*) жінки частіше стикалися зі скороченнями на роботі, ніж чоловіки, через урізання бюджету для роботи штату кібербезпеки (40% проти 36%), затримками при наймі на роботу (42% проти 37%) та затримками у підвищенні зарплати та посади на роботі – 36% та 31%.

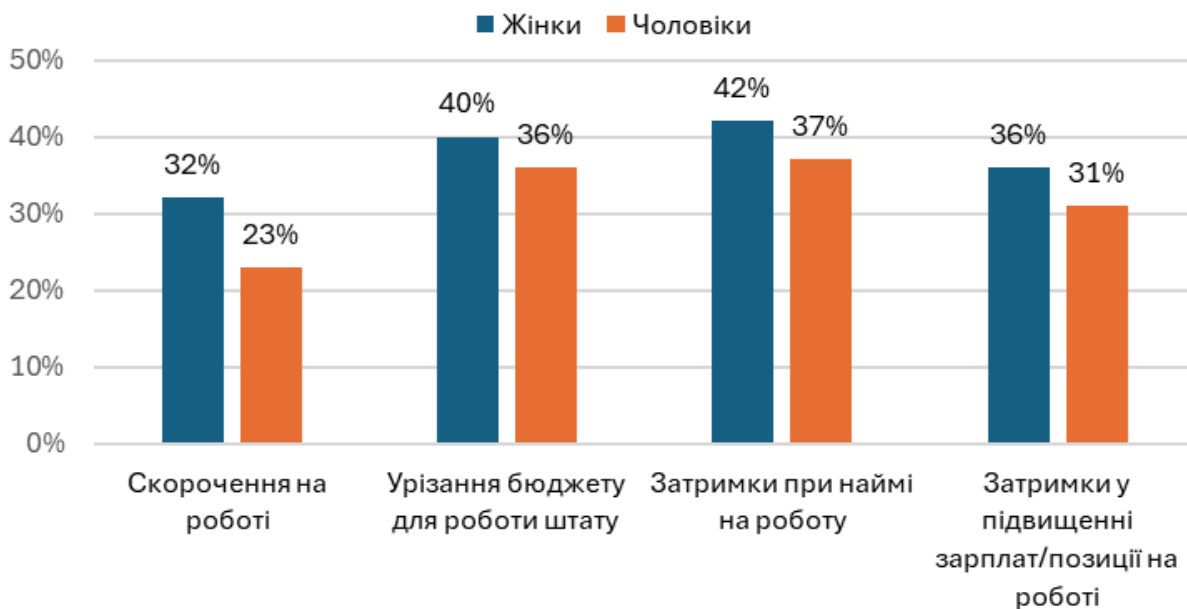


Рис. 1.1.3.2. Результати опитування ISC2 про види скорочень у кібербезпеці в 2024, %

³⁵ Там само.

³⁶ ISC2. (2025, 6 березня). *Survey: Women comprise 22% of the cybersecurity workforce.*

Джерело: ISC2. (2025, 6 березня). *Survey: Women comprise 22% of the cybersecurity workforce.* Cybersecurity Certifications and Continuing Education.
<https://www.isc2.org/insights/2025/03/women-comprise-22-percent-of-the-cybersecurity-workforce?queryID=58116337420fa48c15de4b734b253b2d>

Серед глобальних галузей, які найчастіше стикалися зі скороченнями витрат компанії на її цифрову безпеку, найбільшого впливу зазнали хмарні сервіси (48%), телекомунікації (44%) та аерокосмічна галузь – 43%. На відміну від цього, юридичний сектор (19%), некомерційні організації (24%) та військова галузь (26%) найменше постраждали від обмежень фінансування кібербезпеки³⁷.

Згадані вище скорочення персоналу впливають не тільки на життя окремих людей, але й на можливості низки індустрій: на розробку програмного/апаратного забезпечення (38%), на хмарні сервіси (34%) та будівництво (34%), у той час, як найменшого впливу скорочень персоналу зазнали юридичний сектор (14%), неприбуткові організації та військова галузь – по 13%³⁸. Скорочення кваліфікованих кадрів не тільки значно вплинули на можливість наявних працівників забезпечувати цифрову безпеку організацій, але й продовжують наражати їх на значний ризик. Global Cybersecurity Outlook у 2025 році виявив, що лише 14% кібербезпекових компаній впевнені, що мають достатньо кадрів з потрібними навичками. Разом з цим, **глобальний гендерний розрив на ринку кібербезпеки з 20% у 2024 році збільшився до 28% у 2025**³⁹.

Згідно з дослідженням Allied Market Research, **світовий ринок військової кібербезпеки** у 2023 оцінювався в 15,7 млрд доларів США, а до 2033 року, за прогнозами, досягне 68,5 млрд доларів США⁴⁰. Водночас витрати на якісне технічне, програмне/апаратне забезпечення та послуги у сфері кібербезпеки у США, Франції, Великій Британії та Китаї постійно зростають, а тому постає питання нових кадрів, що можуть їх ефективно використовувати й надавати. Особливої актуальності набуває розгляд гендерного розриву в армії та військовій кібербезпеці. У дослідженні “2023 Demographics Profile of the Military Community”, що розглядає Міністерство оборони Сполучених Штатів, було виявлено, що серед загального складу Міністерства оборони, жінки складають лише 19,3% осіб, тоді як чоловіки – 80,7%⁴¹. Серед них у 2023 році службу проходили 17,7% жінок, у 2022 – 17,5%. У порівнянні з 2005 роком, частка жінок, що у 2023 долучились до активної служби, зросла на 3,1%, тоді як для чоловіків відповідно зменшилась (див. *Рис. 1.1.3.3*)⁴². Щодо Європи, то у 2023 році, загальна частка жінок у Збройних силах становила 13%, де найвищий показник у Швеції (22%), а найнижчий в Ірландії (7%)⁴³. Порівняно з 2020 – 12,24%, середня частка жінок у Збройних силах НАТО зросла до 12,73% у 2022

³⁷ ISC2. (2024a). *Key findings.* 2024 ISC2 Cybersecurity Workforce Study.

³⁸ Там само.

³⁹ World Economic Forum. (2025). *Global cybersecurity outlook 2025.* p. 7.

⁴⁰ Allied Market Research. (2024). *Military cybersecurity market size, share | forecast - 2033.*

⁴¹ Military OneSource. (2024). *2023 demographics profile.* p. 6.

⁴² Там само, p. 21.

⁴³ European Organisation of Military Associations and Trade Unions. (2023). *EUROMIL survey – gender equality/women in the armed forces.* p. 5.

році⁴⁴. Таким чином, жінки все частіше починають працювати у традиційно "маскулінних" сферах, таких як кібербезпека та військова галузь, де здобувають особливі навички та обіймають вищі посади.

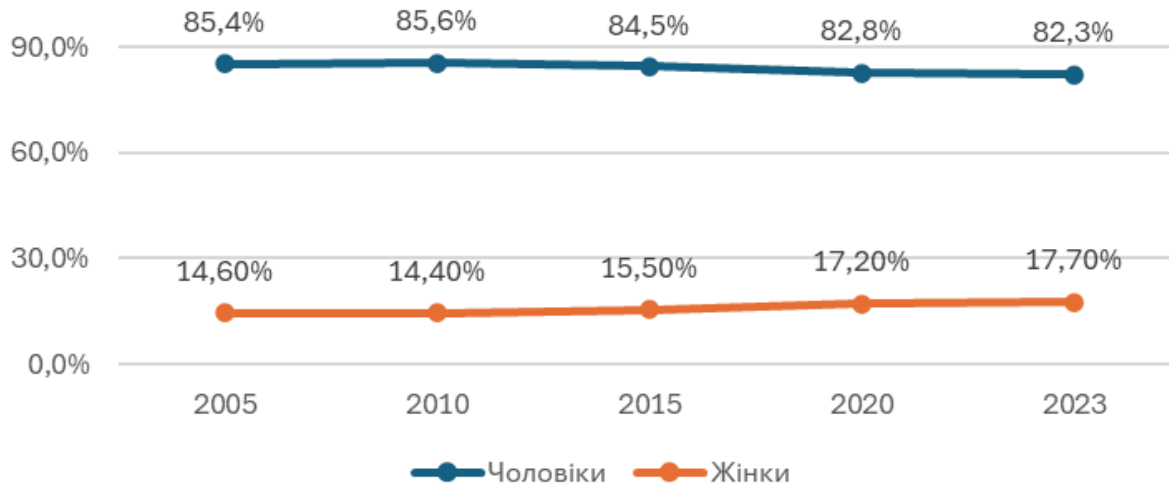


Рис. 1.1.3.3. Відсоток активних військослужбовців(-виць) в Міноборони США, 2005-2023, %

Джерело: Military OneSource. (2024). *2023 demographics profile*. p. 21.

Даних про кількість жінок у сфері військової кібербезпеки у відкритому доступі не знайдено. Однак відомо, що жінки-офіцерки складають 20,1% від загальної кількості (18,4%) офіцерів строкової служби США (2023)⁴⁵. Тоді як для військовослужбовиць НАТО у 2022 – 2,84% для молодших офіцерок, 1,41% серед середніх ("польових") офіцерок та лише 0,01% серед старших офіцерів або генералів⁴⁶. Варто зазначити, що багато строкових військовослужбовиць США отримують досвід роботи з технічним забезпеченням та кібербезпекою навіть без спеціальної освіти. Завдяки тому, що в армії існують освітні програми з підготовки спеціалістів, такі жінки, як Джулія Давіла – солдатка, співзасновниця та головна директорка кібербезпекової компанії ZibaSec – мають змогу розвиватися й після закінчення служби⁴⁷. Однією з ключових програм для розвитку жінок у сфері кібербезпеки після завершення служби є гілка Women in CyberSecurity (WiCyS) – Military Affiliate, яка пропонує не тільки менторські програми, але й нетворкінг, допомогу у пошуку та розвитку їхньої кар'єри у такій унікальній галузі⁴⁸.

⁴⁴ The NATO Committee on Gender Perspectives (NCGP). (2023). *2022 summary of the national reports of NATO members and partner nations*. p. 13.

⁴⁵ Military OneSource. (2024). *2023 demographics profile*. p. 19.

⁴⁶ The NATO Committee on Gender Perspectives (NCGP). (2023). *2022 summary of the national reports of NATO members and partner nations*. p. 13.

⁴⁷ Cupper, C. (2021). *Military women use skills to excel in cybersecurity*. Military Families.

⁴⁸ Women in CyberSecurity (WiCyS). (2025b). *WiCyS military*.

1.2. Виклики та успіхи залучення жінок у сферу кібербезпеки

Кібербезпека є одним з напрямків ІТ, що досі залишається переважно чоловічою галуззю з низьким представництвом жінок. Численні дослідження та практичний досвід свідчать про те, що різноманіття в командах є важливим фактором для досягнення високих економічних результатів і новаторських рішень, проте у сфері кібербезпеки воно все ще суттєво обмежене. Станом на 2025 рік галузь кібербезпеки в усьому світі переживає **хронічний кадровий дефіцит**, саме тому залучення й підтримки жінок може мати позитивні наслідки для цієї сфери⁴⁹.

Відомо, що залучення жінок до STEM було складним і затяжним процесом. Для опису тривалої траєкторії, яка веде до залучення жінок у STEM-сферу, було запроваджено термін **STEM pipeline** (“STEM-трубопровід”). Надалі у відповідь на цей термін в науковій літературі з’явилася метафора *leaky pipeline* (дослівно — “трубопровід з протіканням”), згідно з якою жінки частіше залишають STEM-сферу на всіх етапах — починаючи з початкового зацікавлення в школі, під час здобуття вищої освіти та навіть працюючи викладачками. Це пояснюється численною кількістю викликів, що супроводжують жінок на всіх етапах шляху в STEM⁵⁰.

Основи гендерного дисбалансу в кібербезпеці закладаються ще на етапі освіти та соціалізації жінок у STEM-напрямах. Дослідження показують, що дівчата з раннього віку стикаються зі стереотипами щодо “нежіночності” технічних і природничих спеціальностей, що підриває їхню впевненість у власних здібностях⁵¹. Стереотипи та упередження, вкорінені в суспільстві й освітніх інститутах, часто формують уявлення, ніби науки про комп’ютери, ІТ та кібербезпека – це “чоловічі” сфери, де жінкам буде некомфортно⁵². Зокрема, культура STEM-напрямів нерідко описується як “чоловіча”: комп’ютерні науки стереотипно асоціюються з соціальною ізоляцією, технократичністю та вродженим “талантом до технологій”, якого потребують успішні фахівці. Такі уявлення несумісні з гендерними ролями, традиційно приписуваними жінкам, тому дівчата можуть несвідомо уникати цих сфер через відчуття, що не відповідають образу “типового” ІТ-фахівця⁵³. Дослідження шляхів залучення жінок у кібербезпеку в Норвегії виявило, що панівні маскуліні образи ІТ-галузі – “чоловіки-геймери в худі, які змалку програмують” – відлякують багатьох потенційних кандидаток. Жінки не ототожнюють себе з такими образами й часто не вірять, що зможуть вписатися в ІТ-середовище. Як наслідок,

⁴⁹ Bongiovanni, I., & Gale, M. (2023). *Women in Cyber: Exploring the Barriers, Redesigning the Profession*. The University of Queensland. p. 6.

⁵⁰ Blackburn, H. (2017). The status of women in STEM in higher education: A review of the literature 2007–2017. p. 239.

⁵¹ Там само, p. 245.

⁵² Cheryan, S., Master, A., & Meltzoff, A. N. (2015). Cultural stereotypes as gatekeepers: Increasing girls’ interest in computer science and engineering by diversifying stereotypes. *Frontiers in psychology*, 6. p. 49.

⁵³ Там само, p. 49.

брак обізнаності про реальний спектр ролей у кібербезпеці та звужені уявлення про цю сферу стають бар'єрами для залучення жінок⁵⁴.

Окрім стереотипів, трапляються й **упередження** при наймі та оцінці кандидаток. Менеджери можуть віддавати перевагу кандидатам-чоловікам на технічні посади, сумніваючись у технічних навичках жінок через гендерні упередження⁵⁵. Дослідження підтверджують, що роботодавці іноді сприймають жінок як менш компетентних у питаннях кібербезпеки лише на основі стереотипів, а не реальних навичок⁵⁶. Гендерні стереотипи проявляються вже на етапі входження в професію, ускладнюючи для жінок отримання першого робочого місця або гідної посади в кібербезпеці. На робочому місці ці тенденції продовжуються у формі як несвідомої, так і відкритої дискримінації. Жінки в галузі часто відзначають нестачу підтримки та наставництва. Багато хто зіштовхується з чоловічими "мережами", до яких важко долучитися, та браком менторів-жінок у керівництві⁵⁷. Наприклад, культура 24/7 у кібербезпеці – тобто очікування цілодобової готовності до роботи – є суттєвим бар'єром для фахівчинь, особливо тих, хто має сімейні обов'язки⁵⁸. Зрештою, сукупність цих соціально-інституційних бар'єрів призводить до того, що жінкам значно важче не лише увійти у галузь кібербезпеки, але й закріпитися та просуватися по ній.

Окремим викликом є поширення **гендерно орієнтованих форм кібернасильства**, що негативно позначаються на професійному розвитку жінок у технологічних галузях. До таких явищ належать, зокрема, онлайн-сталкінг (кіберсталкінг), сексуальний та психологічний онлайн-харасмент, доксинг (публікація приватної інформації) та інші види агресії у цифровому просторі. Варто наголосити, що кібернасильство проти жінок і дівчат визнано однією з найбільш стрімко зростаючих форм гендерно зумовленого насильства у Європейському Союзі⁵⁹.

Згідно з дослідженням *Cybersecurity Workforce Study 2021*, 87% жінок у сфері стикалися з несвідомою дискримінацією на робочому місці, а 19% пережили випадки відкритої дискримінації за ознакою статі. Несвідомі упередження можуть проявлятися у дрібницях – від того, кому надають слово на нарадах, до припущень керівників щодо професійних здібностей співробітниць. Накопичуючись, такі мікронерівності створюють для жінок невидимі перешкоди у кар'єрному розвитку. Одним із наслідків є гендерний розрив в оплаті праці та посадовому зростанні. Жінки

⁵⁴ Corneliussen, H. G. (2020, листопад). What brings women to cybersecurity? A qualitative study of women's pathways to cybersecurity in Norway. *Proceedings of the 2020 European Interdisciplinary Cybersecurity Conference*. pp. 1-2.

⁵⁵ Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT professional*, 12(1), p. 48.

⁵⁶ Cheryan, S., Master, A., & Meltzoff, A. N. (2015). Cultural stereotypes as gatekeepers: Increasing girls' interest in computer science and engineering by diversifying stereotypes. p. 49.

⁵⁷ Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. p. 47.

⁵⁸ Там само, p. 47.

⁵⁹ European Institute for Gender Equality. (2022). *Combating cyber violence against women and girls*. Publications Office of the European Union. p. 10.

також повідомляли про незрозумілі затримки в кар'єрному просуванні (53%) і перебільшену реакцію на помилки (29%)⁶⁰.

Попри окреслені вище бар'єри, у сфері кібербезпеки протягом останнього десятиліття спостерігаються низка позитивних зрушень. Дослідження свідчать, що цілеспрямовані програми здатні суттєво змінити гендерний профіль кібербезпеки. Зокрема, британська програма "CyberFirst" у 2023 році забезпечила жінкам 39% місць у стипендіальній схемі й залучила понад 12 500 дівчат до змагання "Girls' Competition", піднявши частку студенток до рекордних 43% за всю історію проєкту⁶¹. У Латинській Америці державні стипендіальні програми підвищили частку жінок-випускниць кіберкурсів до 30–35%, порівняно з менш ніж 20% у 2018 році⁶².

1.3. Досвід подолання бар'єрів. Протидія дискримінації та гендерним стереотипам у кібербезпеці

Розвиток залучення жінок до сфери кібербезпеки вимагає комплексного підходу, що охоплює освітню та кар'єрну підтримку, політику рівності, протидію дискримінації та гендерним стереотипам. Одним із ключових рішень є синергія ініціатив на мікро-, мезо- та макрорівнях, структурованих за коротко-, середньо- та довгостроковими рішеннями (див. *таблицю 1.3.1*)⁶³.

Таблиця 1.3.1 Чинники подолання бар'єрів для жінок у сфері кібербезпеки.

РІВЕНЬ		
МІКРО Індивідуальний	МЕЗО Інституційні та організаційні	МАКРО Системні та державні
Саморозвиток	Кадрова політика	Освітні та інформаційні
<ul style="list-style-type: none"> - Самоосвіта (курси, сертифікації) та підвищення кваліфікації; - Участь у навчальних програмах, тренінгах, воркшопах та конференціях з кібербезпеки; - Підвищення впевненості у власних компетенціях. 	<ul style="list-style-type: none"> - Позитивна дискримінація при наймі; - Тренінги з протидії гендерним упередженням та дискримінації; - Прозорі практики найму та просування по службі. 	<ul style="list-style-type: none"> - Національні STEM-олімпіади та конкурси для дівчат; - Проінформованість про кібербезпеку; - Фінансування досліджень та публікацій з питань гендерної рівності у сфері кібербезпеки; - Популяризація жіночих рольових моделей в медіа;
Професійна підтримка	Розвиток кар'єри	
<ul style="list-style-type: none"> - Взаємопідтримка жінок в професійному середовищі; 	<ul style="list-style-type: none"> - Сприяння у відвідуванні професійних заходів, 	

⁶⁰ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, M. A. M., & AlShalan, M. B. H. (2022, 7 вересня). *Empowering women to work in cybersecurity: Is a win-win*. Boston Consulting Group. p. 3.

⁶¹ National Cyber Security Centre. (2024). *CyberFirst annual highlight report 2023–2024*. p. 3

⁶² OECD (2023), *Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico*. OECD Skills Studies. OECD Publishing, Paris. p. 46.

⁶³ Bongiovanni, I., & Gale, M. (2023). *Women in Cyber: Exploring the Barriers, Redesigning the Profession*. pp. 33-40.

<ul style="list-style-type: none"> - Нетворкінг жінок в індустрії та їхнє залучення до професійних спільнот; - Залучення чоловіків до програм підтримки гендерної рівності. 	<ul style="list-style-type: none"> конференцій та відряджень; - Програми стажування та навчання для жінок; - Менторські програми, наставництво; - Програми повернення до роботи після декретної відпустки. 	<ul style="list-style-type: none"> - Кампанії проти гендерних стереотипів у кібербезпеці.
<p align="center">Сімейна підтримка</p>	<p align="center">Організаційна культура/умови праці</p>	<p align="center">Економічні та політичні</p>
<ul style="list-style-type: none"> - Заохочення та підтримка з боку сім'ї та партнерів; - Спільні домашні обов'язки (зменшення подвійного навантаження на жінок). 	<ul style="list-style-type: none"> - Гнучкий графік роботи; - Дистанційний/змішаний формат роботи; - Догляд за дитиною на робочому місці або субсидії по догляду за дитиною; - Підтримка балансу "робота-життя". 	<ul style="list-style-type: none"> - Державні гранти/стипендії для жінок у кібербезпеці; - Податкові пільги для компаній, що підтримують жінок у кібербезпеці; - Фінансування освітніх STEM-програм для дівчат; - Закони про боротьбу з дискримінацією та рівну оплату праці; - Законодавче регулювання гнучких форматів роботи та декретних відпусток; - Забезпечення гендерно чутливого середовища на державному рівні.

Джерела: Проєкт USAID (2023), Women4Cyber Montenegro (2023), OECD (2023), Bongiovanni & Gale (2023), ISC2 (2024), Global Cybersecurity Forum & Boston Consulting Group (2024), National Cyber Security Centre (2024), Women in CyberSecurity (WiCyS) (2025c), Bachschmidt & Cohignac (2025).

На індивідуальному (мікро) рівні передбачається врахування низки чинників, які сприяють професійній реалізації та розвитку жінок у сфері кібербезпеки. Зокрема, одним із ключових аспектів є саморозвиток, що включає здобуття освіти та підвищення кваліфікації через участь у спеціалізованих курсах, сертифікаційних програмах, тренінгах і конференціях⁶⁴. Такий безперервний процес навчання не лише забезпечує необхідні технічні знання, а й допомагає формувати впевненість у власних компетенціях, що є важливим для подолання стереотипів і упереджень, які часто супроводжують жінок у цій галузі. Важливим елементом є також професійна

⁶⁴ ISC2. (2024a). *Key findings*. 2024 ISC2 Cybersecurity Workforce Study.

підтримка, яка реалізується через активну взаємодію в межах професійних спільнот і нетворкінг. Вони створюють сприятливі умови для обміну досвідом, розвитку навичок і підвищення впевненості, а також допомагають подолати професійну ізоляцію, що часто відчувають жінки у технічних сферах⁶⁵. Крім того, залучення чоловіків до програм підтримки гендерної рівності та співпраця з ними сприяють формуванню більш інклюзивного середовища в галузі кібербезпеки, що є важливим для подолання стереотипів щодо ролі жінок у технічних сферах⁶⁶. Не менш важливим є чинник сімейної підтримки, що включає емоційну підтримку з боку близьких і партнерів, яка сприяє подоланню професійних викликів і стресів. Рівномірний розподіл домашніх обов'язків і зменшення побутового навантаження на жінок створюють умови для кращого балансу між професійним і особистим життям, що, своєю чергою, дозволяє їм приділяти більше уваги професійному розвитку та кар'єрному зростанню⁶⁷. Таким чином, на мікрорівні подолання бар'єрів для жінок у кібербезпеці базується на розвитку особистих компетенцій, створенні професійних мереж підтримки між жінками та забезпеченні сприятливого сімейного середовища, що разом формує підґрунтя для успішної кар'єри та активної участі жінок.

Організаційний (мезо)рівень охоплює інституційні трансформації у сфері освіти, професійної підготовки та розвитку кар'єрних можливостей для жінок у кібербезпеці. Однією з ключових стратегій є поширення STEM-освіти, що реалізується через мотиваційні ініціативи, інформаційні кампанії, спеціалізовані курси, тренінги й менторські програми для підготовки кваліфікованих фахівчинь з кібербезпеки⁶⁸. Провідні університети, такі як Оксфорд (1 місце в рейтингу вишів) та Массачусетський технологічний інститут (2 місце)⁶⁹ пропонують низку програм, спрямованих на залучення жінок у сферу кібербезпеки. Вони включають як університетські курси з основ кібербезпеки, криптографії та мережевої безпеки, так і студентські та позакласні ініціативи. Наприклад, Массачусетський технологічний інститут пропонує безкоштовні відкриті онлайн-курси доступні різними мовами⁷⁰ та організовує літню академічну Жіночу Технологічну Програму (Women's Technology Program) для американських старшокласниць, які продемонстрували сильні здібності в математиці та природничих науках⁷¹. Діяльність студентської організації Стенфордські Жінки в Комп'ютерних Науках (Stanford Women in Computer Science, WiCS) спрямована на підтримку жінок у технологічній сфері через організацію воркшопів та зустрічей з галузевими експертами, забезпечення менторства та нетворкінгу для підтримки жінок у технологічній сфері⁷². Такий підхід розширює

⁶⁵ Проект USAID "Кібербезпека критично важливої інфраструктури України". (2023). *Рекомендації для подолання перешкод у професійній реалізації жінок у сфері кібербезпеки на рівні освіти*.

⁶⁶ Bongiovanni, I., & Gale, M. (2023). *Women in Cyber: Exploring the Barriers, Redesigning the Profession*. p. 34.

⁶⁷ Там само. p. 34.

⁶⁸ ISC2. (2024b). *Women in cybersecurity: Inclusion, advancement and pay equity are keys to attracting and retaining more women*.

⁶⁹ Times Higher Education. (2025). *World University Rankings*.

⁷⁰ Massachusetts Institute of Technology. (2025a). *Free Online Course Materials*. MIT OpenCourseWare.

⁷¹ Massachusetts Institute of Technology. (2025b). *MIT Women's Technology Program*.

⁷² Stanford Women in Computer Science (WiCS). (2025). *Events*.

доступ до якісної STEM-освіти та дозволяє розвивати базові та поглиблені навички в технічній галузі, зокрема у кібербезпеці.

Попри це, на етапі отримання освіти існує проблема “витоку кадрів”, коли рівень зацікавленості дівчат у кібербезпеці зменшується з переходом до вищих освітніх рівнів. Однією з запроваджених ініціатив для розв’язання цієї проблеми є підхід “Cybersecurity for All”, який спрямований на популяризацію кар’єри у кібербезпеці та створення гендерно-нейтрального середовища⁷³. Обов’язковим аспектом при навчанні та роботі є врахування політики гендерного балансу серед керівництва та педагогічного складу⁷⁴.

Яскравим прикладом є кампанія #NoBiasInCyber від Orange Cyberdefense⁷⁵, яка спрямована на подолання стереотипів, що стримують жінок від входу у сферу. У співпраці з організацією Women4Cyber вона пропонує спеціалізовані програми навчання й наставництва для підтримки гендерної та соціальної різноманітності в кібербезпеці.

Впровадження ініціатив з підтримки жінок у кібербезпеці також здійснюється як через діяльність неурядових та громадських організацій, а також корпоративних програм провідних компаній (Google, Microsoft, IBM)⁷⁶. Вони створюють додаткові можливості для професійного розвитку та просування жінок у галузі. Низка програм, таких як: CyberFirst⁷⁷, Women4Cyber⁷⁸, Cyberdefense – надають практичне навчання та стажування, а опісля допомагають жінкам з працевлаштуванням у кібербезпеці. Приклад організацій (ініціатив) та напрями їхньої діяльності представлено у таблиці 1.3.2.

Таблиця 1.3.2. Приклад організацій (ініціатив) та напрями їхньої діяльності для подолання бар’єрів у кібербезпеці.

Назва програми/ініціативи		Країна	Напрями діяльності
CyberFirst Girls Competition		Велика Британія	Державна програма для школярів 11–17 років, що включає конкурси, літні школи, стипендії та менторство.
Women4Cyber (неурядова організація)	Women4Cyber Academy	ЄС	Інноваційна онлайн-платформа, доступ до професійного навчання: спеціалізованих тренінгів, курсів, сертифікацій.

⁷³ Liu, X.M., & Murphy, D.R. (2016). Engaging females in cybersecurity: K through Gray. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. p. 256.

⁷⁴ Проект USAID "Кібербезпека критично важливої інфраструктури України". (2023). *Рекомендації для подолання перешкод у професійній реалізації жінок у сфері кібербезпеки на рівні освіти*.

⁷⁵ Orange Cyberdefense. (2023, 7 березня). *For a safer digital society: Breaking down gender barriers in cybersecurity*.

⁷⁶ ISC2. (2024b). *Women in cybersecurity: Inclusion, advancement and pay equity are keys to attracting and retaining more women*.

⁷⁷ National Cyber Security Centre. (2025a). *CyberFirst Girls Competition*.

⁷⁸ Women 4 Cyber Montenegro. (2025a). *Projects*.

	Менторські програми		Допомога жінкам у здобутті професійних знань, розширенні зв'язків, підвищенні впевненості.
	Women4Cyber Expert Registry		Реєстр експерток у кібербезпеці сприяє видимості жінок та їхніх досягнень, залученню до публічних заходів, створює можливості для співпраці.
	Women4Cyber STARTup		Підтримка жіночого підприємництва/стартапів (засновниці або принаймні 50% жінок у складі команди), сприяння жіночому лідерству.
	Видання книг		Підвищення обізнаності та популяризація справжніх рольових моделей жінок у кібербезпеці (наприклад, книга "Руйнуючи гендерні бар'єри: Найкращі кібер-жінки Європи" ("Hacking gender barriers: Europe's top cyber women")).
WiCyS (Women in CyberSecurity) (некомерційна організація)		США	Комплексний підхід: від освіти до професійної підтримки. -щорічна конференція, присвячена жінкам у кібербезпеці, для обміну досвідом та налагодження професійних контактів; -менторські програми (WiCyS Mentorship Program), тренінги; -стипендії та гранти; -партнерство з університетами та корпораціями (можливості для стажувань, працевлаштування).
Google Women Techmakers (WTM) глобальна ініціатива компанії Google	Women Techmakers Story	Світ (охоплює понад 75 країн)	Поширення видимості та натхнення, руйнування стереотипів через історії успіху технологінь з різних частин світу.
	Black Women in Tech		Збільшення представленості темношкірих жінок у технічній сфері через доступність до платформ навчання.
	She Builds AI		Розширює можливості через навчання в галузі штучного інтелекту, менторство, підтримку спільноти, участь у воркшопах та виконання проєктних завдань.

Джерела: National Cyber Security Centre (2025), Women 4 Cyber Montenegro (2025), Women in CyberSecurity (WiCyS) (2025), Google for Developers (2025).

Завдяки впровадженню цих програм спостерігається зростання кількості жінок, які долучаються до освітніх та професійних ініціатив у кібербезпеці. У 2024 році для участі в конкурсі CyberFirst Girls Competition, організованому Національним центром

кібербезпеки Великої Британії (NCSC), зареєструвалась рекордна кількість – 15 тисяч дівчат, що свідчить про зростання залученості жінок до кібербезпеки⁷⁹; у програмі менторства від Women4Cyber у 2023 році взяло участь 600 учасниць⁸⁰; понад 1900 жінок з США щороку беруть участь у конференціях WiCyS, а ще більше – у менторських і освітніх програмах⁸¹, зокрема Girls Who Code залучила понад 670 тисяч учасниць за період своєї діяльності з 2012 року⁸².

Таким чином, організаційний рівень ініціатив сприяє подоланню бар'єрів для жінок у кібербезпеці через розвиток навичок, формування професійних мереж і підвищення їхньої видимості у галузі.

Попри освітні ініціативи, жінки в кібербезпеці стикаються з кар'єрними бар'єрами та гендерними упередженнями вже на робочому місці. В ЄС жінки отримують в середньому на 13% менше, ніж чоловіки, що відповідає приблизно півтора місяцям неоплачуваної роботи на рік на тій самій посаді. Цей гендерний розрив в оплаті праці є однією з головних перешкод для рівної участі жінок у професійній сфері, в тому числі у сфері кібербезпеки⁸³. Згідно з останніми дослідженнями, жінки становлять лише близько 22-25% світової робочої сили в галузі кібербезпеки, а серед керівних посад ці показники ще нижчі⁸⁴. Не зважаючи на докладені зусилля, за наявних темпів прогресу, згідно з даними Всесвітнього економічного форуму, досягнення повної гендерної рівності буде можливе не раніше 2158 року, тобто знадобиться ще понад п'ять поколінь (понад 130 років)⁸⁵.

Відповідно до цього, необхідно пришвидшити подолання системних бар'єрів та упереджень на **макрорівні** (в індустрії, уряді та суспільстві) через впровадження політики гендерної рівності, яка сприятиме інклюзії, усуненню дискримінації та створенню гендерно чутливого робочого середовища. З цією метою, як інструмент позитивної дискримінації, передбачено встановлення обов'язкових квот для жінок у конкурсах на посади⁸⁶. Так, наприклад, у Франції встановлено квоти для жінок у радах директорів великих компаній (“Women on Boards”), що сприяє збільшенню їхньої присутності на керівних посадах⁸⁷.

Окрему увагу у подоланні бар'єрів приділено протидії дискримінації та гендерним стереотипам у кібербезпеці. Для цього запропоновано здійснення реформи освітніх програм, які підвищуватимуть обізнаність про важливість гендерної рівності, зокрема у сфері кібербезпеки, та сприяють ранньому залученню дівчат до STEM-дисциплін через руйнування гендерних стереотипів. Європейська Комісія заохочує жіноче підприємництво та розвиток освіти через свої програми

⁷⁹ National Cyber Security Centre. (2025b). *This is a cyberfirst world*. Annual highlight report 2024-2025, p. 20.

⁸⁰ Women4Cyber Montenegro. (2025b). *W4C 2023 Annual Report*. p. 14.

⁸¹ Women in Cybersecurity (WiCyS). (2024). *WiCyS 2024 Conference Evaluation Report*. p. 5.

⁸² Girls Who Code. (2025) *Research*.

⁸³ Bachschmidt, J., & Cohignac, M. (2025). Technological and security issues: 2025, a pivotal year for women. *Fondation Robert Schuman*, (782), p. 2.

⁸⁴ Global Cybersecurity Forum & Boston Consulting Group. (2024). *2024 cybersecurity workforce report: Bridging the workforce shortage and skills gap*. p. 15.

⁸⁵ The Gurus. (2025). *Advancing Gender Equality in 2025 and Beyond*. IT Security Guru.

⁸⁶ Bongiovanni, I., & Gale, M. (2023). *Women in Cyber: Exploring the Barriers, Redesigning the Profession*. pp. 36-37.

⁸⁷ Bachschmidt, J., & Cohignac, M. (2025). Technological and security issues: 2025, a pivotal year for women. p. 2.

DIGITALEUROPE та Horizon Europe, головною умовою яких є забезпечення гендерної рівності⁸⁸.

Наступний крок – розробка державних політик щодо реінтеграції жінок на робочі місця після декретної відпустки: фінансова підтримка, гнучкий графік, можливості перекваліфікації тощо⁸⁹. Загалом, подальший розвиток кібербезпеки потребує системного підходу для формування гендерно чутливої політики та подоланню гендерного дисбалансу у кібербезпеці.

У цьому контексті вагомим чинником є роль лідерок, які вже досягли успіху у кібербезпеці та активно популяризують цю сферу. Зокрема, Кеті Мусуріс – експертка з кібербезпеки та засновниця Luta Security, одна з новаторок впровадження програм “Bug bounty” – ініціативи, які стимулюють виявлення вразливостей у програмному забезпеченні. Вона була однією з перших, хто впровадив такі програми у Microsoft, а також виступила співініціаторкою проєкту Міністерства оборони США “Hack the Pentagon”⁹⁰, що стало революційним кроком у державній кібербезпеці. Іншим яскравим прикладом успішних жінок у сфері кібербезпеки є американська інженерка і технологиня Меган Сміт, яка працювала головною технічною директоркою США, а до цього – віцепрезиденткою Google. Там вона була співзасновницею ініціативи “Women Techmakers”, яка спрямована на підтримку участі жінок у STEM-галузях⁹¹. Її діяльність сприяє не лише підвищенню видимості жінок у технічних сферах, а й формуванню структурних шляхів для їхнього професійного розвитку. Значний внесок у подолання бар’єрів робить і Джессіка Гулік, засновниця Katzcy, компанії, що спеціалізується на маркетингу та стратегіях кібербезпеки, а також під її керівництвом реалізуються програми менторства та навчання, які допомагають жінкам розвивати професійні навички та долучитися до нетворкінгу⁹². Також вона бере участь у конференціях і форумах, присвячених гендерній рівності у технологіях, де виступає з доповідями та організовує панельні дискусії. Через діяльність таких жіночих рольових моделей формується позитивний імідж жінок у кібербезпеці, що є важливим чинником подолання стереотипів і стимулює молоде покоління дівчат обирати кар’єру у галузі кібербезпеки.

⁸⁸ Там само. р. 4.

⁸⁹ Bongiovanni, I., & Gale, M. (2023). *Women in Cyber: Exploring the Barriers, Redesigning the Profession*. p. 36.

⁹⁰ Luta Security. (2025). *Founder & CEO*.

⁹¹ The White House. (2025). *Megan Smith*.

⁹² Katzcy. (2025). *About Us*.

Розділ 2. Залучення жінок до кібербезпеки в Україні

2.1. Статистична інформація про жінок у кібербезпеці: освіта та ринок праці.

Гривцов Володимир, Смоленська Юлія, Оніщенко Артур

2.1.1. Жінки у закладах вищої освіти на спеціальності кібербезпека в Україні.

Задля визначення особливостей гендерного розподілу в українських закладах вищої освіти (ЗВО) було відібрано 7 передових закладів за цим напрямом в країні. Це було зроблено за власноруч створеним індексом університетської затребуваності для освітньої програми (скорочено – ІУЗдОП). Побудова цього показника зумовлена відсутністю релевантних аналогів. Хоча спроби створити топ ЗВО вже існують, вони приділяють основну увагу лише одному критерію, наприклад, середньому балу вступників⁹³. Така метода не враховує інші важливі показники, на кшталт кількості студентів, що навчаються на обраній освітній програмі, що може бути джерелом систематичних похибок. Інші схожі індекси намагаються вирахувати якість наданої освіти, проте не відображають популярності закладу серед вступників⁹⁴).

Своєю чергою, запропонована в цьому дослідженні методика базується на трьох основних показниках: **загальній кількості зарахованих студентів, середнього бала ЗНО зарахованих та конкурсу на одне бюджетне місце**. Ці показники об'єднують у собі репрезентативність та простоту збору даних. Як показано в *Таблиці 2.1.1.1*, між цими змінними не виявлено сильної кореляції, що свідчить про їхню незалежність. Крім того, тест Бартлетта на сферичність не показав статистичної значущості ($p = 0.233$), що вказує на відсутність підстав для зведення змінних до єдиного латентного чинника. Таким чином, кожна змінна відображає окремий аспект оцінювання університету. Щоб урівноважити масштаб показників і забезпечити їхню співмірність в інтегрованому індексі, було проведено мін-макс нормалізацію з приведенням значень до інтервалу $[0;1]$.

Таблиця 2.1.1.1. Кореляційна матриця для складників ІУЗдОП вступу 2024 року⁹⁵

		Середній бал	Кількість зарахованих	Конкурс
Кореляція	Середній бал	1,000	-0,072	-0,414

⁹³ Яблоновська, 2020

⁹⁴ Іпполітова, 2023

⁹⁵ Тест проводився на базі результатів вступу на спеціальність “Кібербезпека” 2024 року до 25 українських ВНЗ за даними сайту “Вступ.ОСВІТА.УА”

	Кількість зарахованих	-0,072	1,000	0,025
	х			
	Конкурс	-0,414	0,025	1,000

В результаті формула індексу ІУЗдОП виглядає таким чином:

$$ІУЗдОП_n = \frac{x_n - 100}{100} + \frac{y_n}{y_{max}} + \frac{z_n - 96}{z_{max}}$$

(де x_n - середній бал абітурієнтів конкретного університету, y_n - кількість зарахованих, z_n - конкурс, x_{max} , y_{max} , z_{max} - відповідно найбільші значення серед усіх ЗВО.). Індекс є лінійною змінною та набуває значень від 0 до 3.

Кількість зарахованих студентів відображає реальні обсяги навчання за спеціальністю “Кібербезпека” в ЗВО. Конкурс на одне місце є показником попиту абітурієнтів і привабливості для них закладу та спеціальності в ньому. Середній бал зарахованих демонструє академічний рівень студентів і суворість відбору.

В межах цього дослідження ІУЗдОП було вираховано за результатами вступної кампанії 2024 року за спеціальністю “Кібербезпека”. Дані було відібрано вручну із сайту Вступ.Освіта.УА (б. д.).

В цьому випадку $x_{max} = 168.78$, $y_{max} = 327$, $z_{max} = 18,75$. В результаті було визначено список із 15 передових ЗВО (див. *Таблицю 2.1.1.2*) на основі даних з вебресурсу Освіта.уа⁹⁷, підв'язаному до інформації з державного реєстру Єдиної державної бази з питань освіти (ЄДБО). Перше місце по середньому рейтинговому балу зайняв Київський національний університет Тараса Шевченка; за кількістю зарахованих Національний університет “Львівська політехніка”; а по конкурсу на одне бюджетне місце — Національний університет “Києво-Могилянська академія”. В топ три університети увійшли Національні університети “Львівська політехніка”, “Києво-Могилянська академія” та “Київський політехнічний інститут імені Ігоря Сікорського”.

Таблиця 2.1.1.2. Топ 15 освітніх програм закладів вищої освіти за індексом ІУЗдОП за 2024 рік

Університет	Середній рейтинговий бал всіх зарахованих х	Кількість зарахованих	Конкурс на одне бюджетне місце	Сумарний бал ІУЗдОП
Національний університет "Львівська політехніка"	159,88	327	4,56	1,84

⁹⁶ Формула 2.1. Розрахунок індексу ІУЗдОП.

⁹⁷ Вступ.Освіта.УА. Пошуковий запит: Кібербезпека та захист інформації; бакалавр.

Національний університет "Києво-Могилянська академія"	162,03	36	18,75	1,73
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"	165,97	205	4,81	1,54
Державний університет інформаційно-комунікаційних технологій	138,9	53	15,67	1,39
Державний торговельно-економічний університет	141,46	113	10,5	1,32
Київський національний університет імені Тараса Шевченка	168,78	96	5,29	1,26
Львівський національний університет імені Івана Франка	167,41	47	7,47	1,22
Державний університет інформаційно-комунікаційних технологій (управління)	147,42	108	5,21	1,08
Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут"	163,74	16	7,13	1,07
Національний університет біоресурсів і природокористування України	140,65	58	8	1,01
Сумський державний університет	161,21	32	5,4	1,00
Харківський національний університет імені В.Н. Каразіна	163,07	49	3,56	0,97
Київський столичний університет імені Бориса Грінченка	145,54	65	5,87	0,97
Національний університет "Одеська політехніка"	160,15	61	3,33	0,97
Харківський національний університет радіоелектроніки	164,48	42	3,4	0,95

Після цього був зроблений пошук даних результатів балів ЗНО⁹⁸ зарахованих вступників на бакалаврський ступінь в університети, а також даних за зимову сесію студентів 1-4 курсу з відкритих джерел на офіційних сайтах університетів. У

⁹⁸ Зовнішнє незалежне оцінювання (ЗНО) — це оцінювання результатів навчання, здобутих особою на певному освітньому рівні, яке здійснюється спеціально уповноваженою державою установою (організацією) (Закон України про вищу освіту, 2014).

результаті були знайдені дані про результати ЗНО для двох найвищих за рейтингом університетів: Національного університету "Львівська політехніка" і "Києво-Могилянська академія". Ці заклади відрізняються за регіоном та розміром, що робить їх доцільним для порівняння. Під час аналізу вступників, були вилучені ті, хто вступали за квотою через закодованість їх ПІБ та неможливість ідентифікації їх статі. Водночас для аналізу гендерного розподілу студентів в університетах, було проаналізовано результати зимових сесій 1-4 курсів Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" та Державного університету інформаційно-комунікаційних технологій. Додавання атрибутивної характеристики статі для осіб було зроблено через мовний штучний інтелект Chat GPT, та опісля редагування вручну. Кодування, аналіз та візуалізація була зроблена через програмне забезпечення Excel.

Даних щодо жінок у роботі у сфері кібербезпеки в Україні бракує. Були зроблені усні запити у Головне управління розвідки Міністерства оборони України, Службу безпеки України та Державну службу спеціального зв'язку та захисту інформації України, проте відмовлено через конфіденційність даних.

2.1.2. Жінки у сфері кібербезпеки в світі

У сфері кібербезпеки у світі простежується **горизонтальна гендерна сегрегація**, хоч відсоток фахівчинь з кібербезпеки буде коливатися залежно від країни. За оцінкою Світового форуму з кібербезпеки (Global Cybersecurity Forum), в цій галузі працює приблизно 24% фахівчинь (*Рисунок 2.1.2.1*). За регіонами, найбільший відсоток має Азійсько-Тихоокеанський регіон (майже 25%). Це можна пояснити нещодавнім прискоренням у розвитку STEM-наук у цьому регіоні. Як наслідок, більшість працівників та працівниць здобули відповідну освіту вже в умовах зменшеної сегрегації за статтю. Своєю чергою, найменшу частку має Африка — 13.5%. В Європі при цьому налічується 22.4% працівниць кібербезпеки. Як видно з *Рисунка 2.1.2.2*, в усіх країнах світу станом на 2022 рік також існує гендерний розрив щодо представленості жінок та чоловіків у сфері кібербезпеки. Лише в двох країнах понад третина працівників виявились жінками, а саме в Нігерії та Мексиці. Оскільки Африка є регіоном з найменшою часткою жінок у кібербезпеці, Нігерія може виступати як винятком, так і похибкою в розрахунках дослідників. На протилежному кінці списку знаходяться Японія, Німеччина та Сполучені Штати зі значеннями від 10 до 13%. Також на графіку видно, що серед п'ятірки країн з найменшим гендерним розривом майже всі не належать до переліку найбагатших держав, коли найбільший гендерний розрив присутній суто в заможних країнах. Це може вказувати на меншу горизонтальну гендерну сегрегацію серед країн з менш забезпеченим населенням.

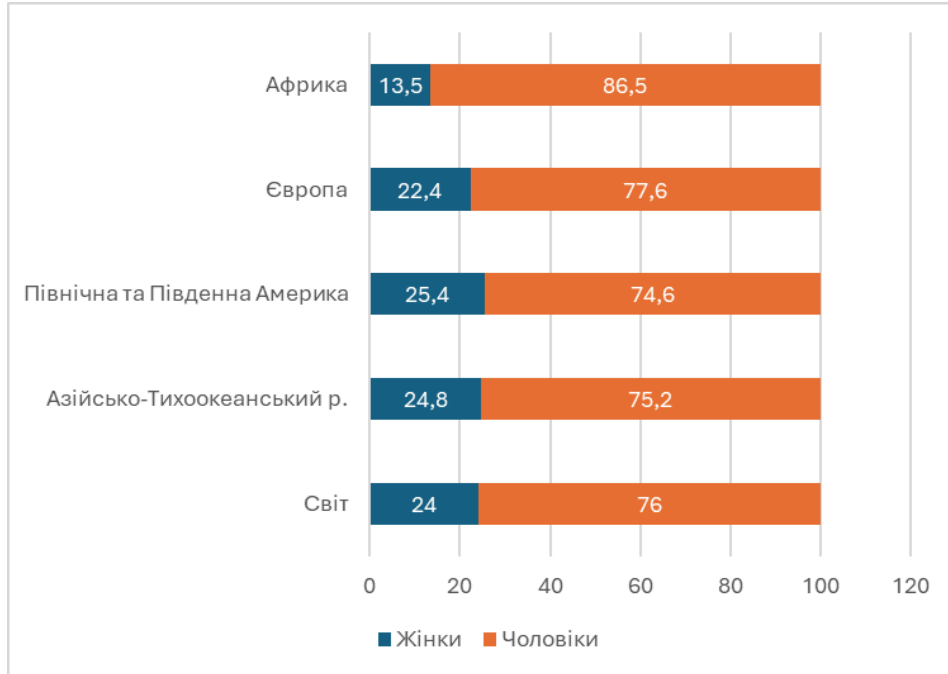


Рисунок 2.1.2.1. Гендерний розподіл у сфері кібербезпеки за регіонами у 2024 році (%)⁹⁹

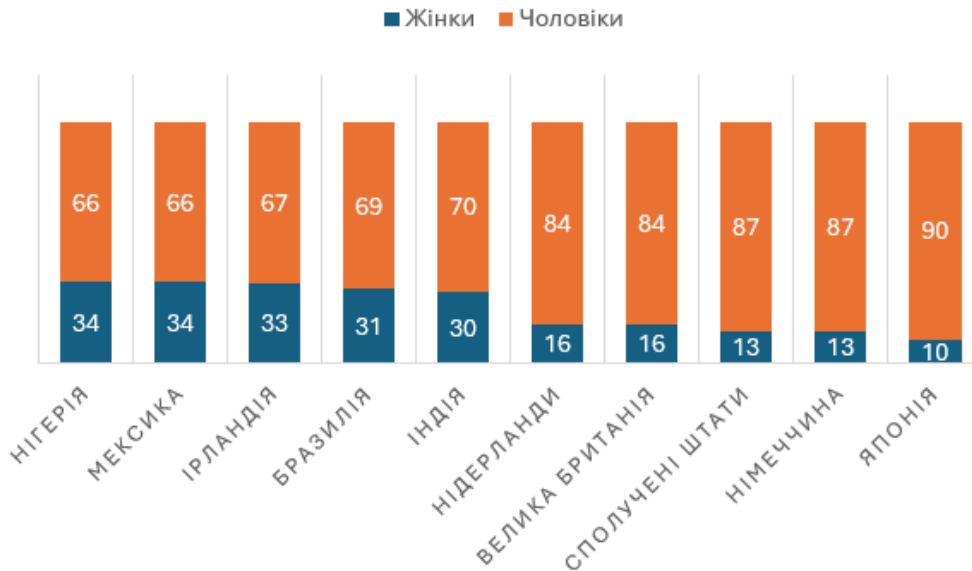


Рисунок 2.1.2.2. Гендерний розподіл у сфері кібербезпеки: 5 країн з найбільшою та найменшою часткою жінок у 2022 році (%)¹⁰⁰

Втім, існують опосередковані докази зменшення горизонтальної сегрегації з часом. Такі висновки можемо зробити із статистики щодо розподілу працівників і працівниць в цій сфері за гендером та віком, як це демонструє *Рисунок 2.1.2.3.*

⁹⁹ Global Security Forum, 2024, с. 15.

¹⁰⁰ ISC2, 2022, с. 41.

Найбільший відсоток жінок (24%) знаходиться у віковій категорії до 30 років, коли зі збільшенням віку їх частка зменшується. У категорії 30-38 років жінок вже 20%, коли в усіх старших категоріях вона знаходиться приблизно на рівні 15%.

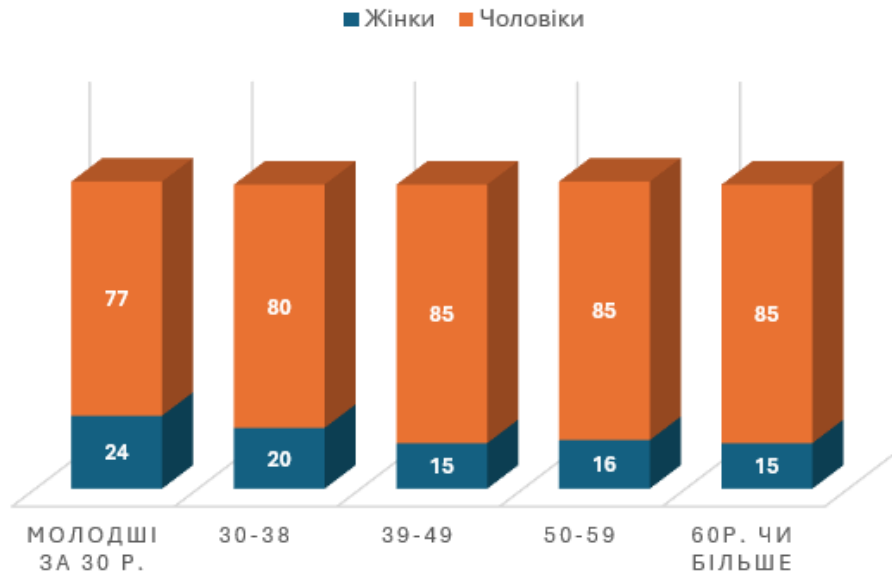


Рисунок 2.1.2.3. Гендерно-віковий розподіл у сфері кібербезпеки у світі у квітні-травні 2023 року (%)¹⁰¹.

Дані також демонструють **явище вертикальної сегрегації** в цій сфері, адже у 2024 році “лише 16% від усіх CISO (начальників/начальниць відділу інформаційної безпеки) — це жінки”¹⁰². Таким чином, скляну стелю (невидимий бар’єр в досягненні керівних позицій) в цьому випадку все-таки складно вважати непрохідною, адже наявний показник лише на третину менший за згадану загальну частку жінок у сфері кібербезпеки, що становить 24%.

Окрім сегрегації, у світі існує **гендерний розрив в оплаті праці**. Як видно з графіка на *Рисунку 2.1.2.4*, жінки у сфері кібербезпеки в середньому за рік заробляють 109.61 тис. доларів США, що на 4.9% менше за чоловіків.

¹⁰¹ ISC2, 2023, с. 39.

¹⁰² Cybersecurity workforce report, 2024, с. 15.

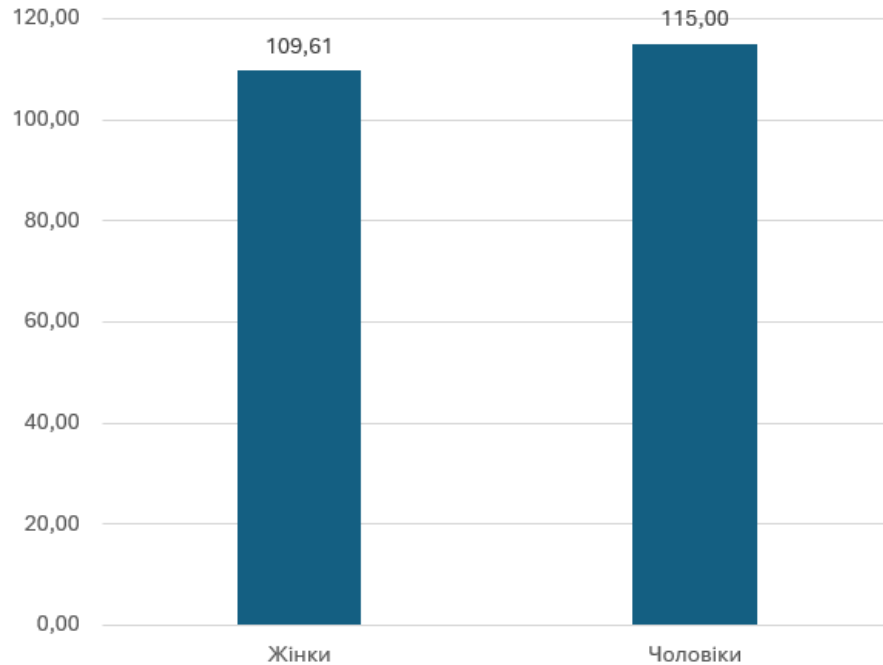


Рисунок 2.1.2.4. Гендерний розрив в оплаті праці у сфері кібербезпеки у світі у квітні-травні 2023 року (тис. \$ США на рік).¹⁰³

Щодо освіти, у світі також було встановлено, що в середньому спеціалістки з кібербезпеки мають вищий освітній рівень, ніж їхні колеги-чоловіки. Як продемонстровано на *Рисунку 2.1.2.5*, жінки схильні радше отримувати магістерський ступінь чи вище. Натомість, у чоловіків трохи більший шанс працювати у сфері кібербезпеки із загальною, спеціальною чи неповною вищою освітою.

¹⁰³ Borgeaud, 2024.

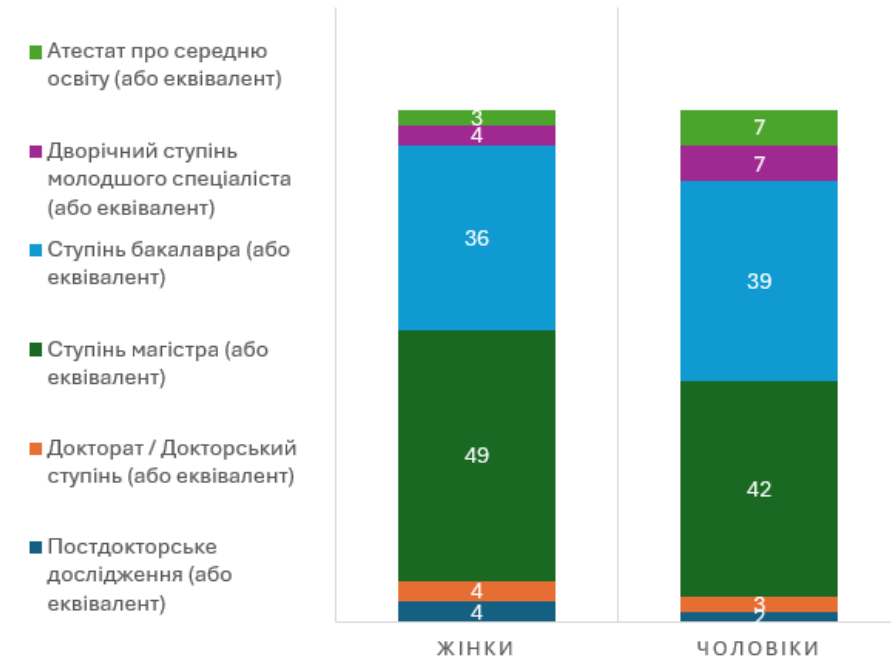


Рисунок 2.1.2.5. Відмінності у рівні освіти за гендером у сфері кібербезпеки у світі у 2022 році (%).¹⁰⁴

2.1.3. Жінки в освіті за спеціальністю кібербезпека в Україні.

Гендерна сегрегація проявляється з раннього віку людини і є помітною під час вибору спеціальності у закладах вищої освіти. У двох найпопулярніших серед абітурієнтів освітніх програмах за спеціальністю 125 “Кібербезпека” у 2024 році (див. Таблицю 2.1.3.1), частка жінок серед зарахованих в університет на цю спеціальність становить у середньому 27,4%, водночас розрив між середніми конкурсними балами чоловіків і жінок незначний (менше за 4%), з невеликою перевагою жінок в одному університеті та чоловіків — в іншому.

Таблиця 2.1.3.1. Порівняльна таблиця гендерної сегрегації серед зарахованих студентів на топ 2 освітні програми за спеціальністю 125 у 2024 році.

Стать	Львівська політехніка		Києво-Могилянська академія	
	чоловіки	жінки	чоловіки	жінки
кількість осіб*	236	82	25	10
% від усіх зарахованих	74,20%	25,8%	71%	29%
середній рейтинговий бал	159,3	160,9	163,5	159,2

¹⁰⁴ ISCT, 2022, с. 52

дані взяті з сайтів національного університету “Києво-могилянська академія”¹⁰⁵ та “Львівська політехніка”¹⁰⁶

*квотні місця були не взяті до аналізу

Результати зимових сесій 1-4 курсів за спеціальністю 125 “Кібербезпека” в Державному університеті інформаційно-комунікаційних технологій та Національному технічному університеті України “Київський політехнічний інститут імені Ігоря Сікорського” вказують на горизонтальну гендерну сегрегацію у сфері освіти кібербезпеки: середня частка жінок складає 26%. Водночас можна простежити загальну тенденцію зростання кількості студенток у кібербезпеці з роками: на 4 курсі, студенти якого вступали у 2021 році, середня частка жінок складала 22%, коли на 1 курсі, вступ до якого відбувся у 2024 році, середня частка складає вже 29% (див. *Рисунок 2.1.3.2 та Рисунок 2.1.3.3*).

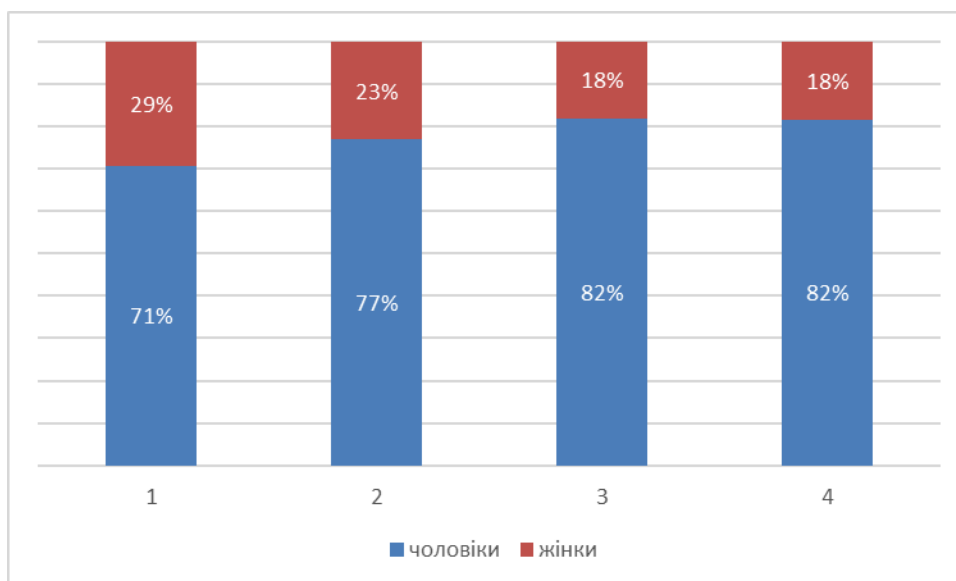


Рисунок. 2.1.3.2. Гендерний розподіл серед студентів 1-4 курсу навчання в Державному університеті інформаційно-комунікаційних технологій в 2024/2025 н.р.¹⁰⁷

¹⁰⁵ Рейтинговий список вступників за освітньо-професійною програмою підготовки бакалавра, на спеціальність 125 у 2024 році. Кібербезпека та захист інформації. Вступ до НаУКМА.

¹⁰⁶ Рейтинговий список вступників на перший курс денної форми навчання за освітньо-професійною програмою підготовки бакалавр за спеціальністю 125. Кібербезпека та захист інформації до Національного університету “Львівська політехніка”. Вступ 2024.

¹⁰⁷ Рейтинговий список студентів ННІ кібербезпеки та захисту інформації(за осінній семестр 2024-2025 н.р.). Державний університет інформаційно-комунікаційних технологій.

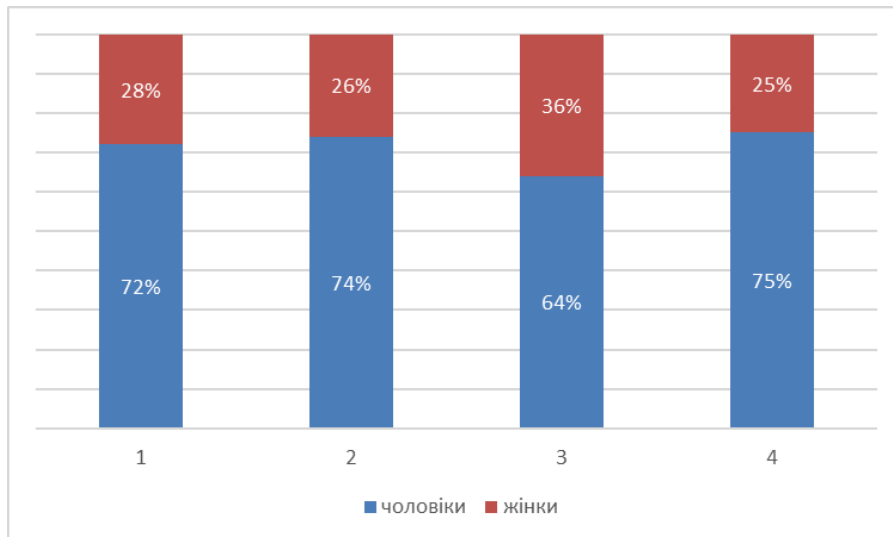


Рисунок. 2.1.3.3. Гендерний розподіл серед студентів 1-4 курсу навчання в Національному технічному університеті України “Київський політехнічний інститут імені Ігоря Сікорського” у 2024/2025 н.р.¹⁰⁸

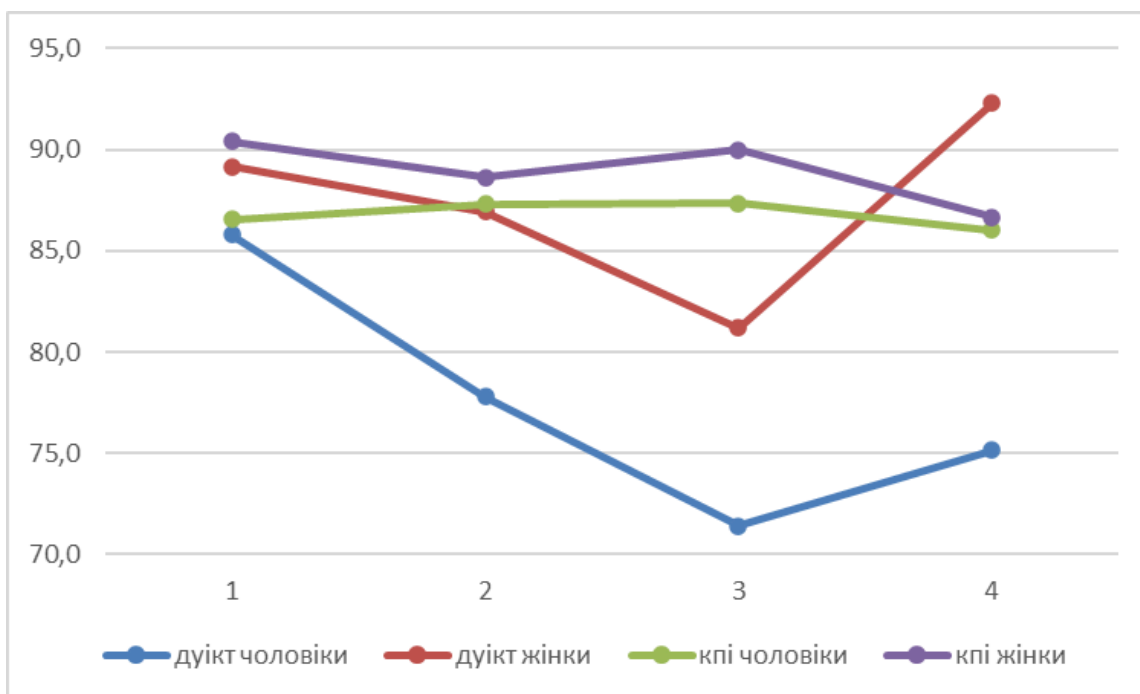


Рисунок. 2.1.3.4. Середній рейтинговий бал чоловіків і жінок у результаті зимової сесії 2024/2025 н.р. 1-4 курсу в ДУІКТ та Національному технічному

¹⁰⁸ Рейтинг успішності студентів Фізико-технічного інституту (ФТІ) за результатами зимового семестрового контролю 2024/2025 н.р. Департамент навчально-виховної роботи КПІ ім. Ігоря Сікорського.

університеті України “Київський політехнічний інститут імені Ігоря Сікорського”(КПІ).

Цей тренд може бути зумовлений початком повномасштабного вторгнення в Україну у 2022 році та підвищенням попиту на спеціалістів з кібербезпеки. Однак він може бути пояснений іншими факторами, такими як систематичне відрахування жінок на останніх курсах. Щодо успішності в навчанні, жінки всюди переважають чоловіків за рейтинговим балом з розривом від 1% до 23% (див. *Рисунок 2.1.3.4*).

2.2. Ситуація в Україні та щодо регулювання гендерних відносин у кібербезпеці

Сидоров Ростислав, Чорна Вікторія, Василенко Поліна, Кучабська Катерина

2.2.1. Законодавча база щодо кібербезпеки України

Європейські країни, зокрема в рамках ЄС, розвивають правові механізми для боротьби з такими явищами. Наприклад, **Директива Європейського парламенту 2011/93/ЄС** щодо боротьби з сексуальною експлуатацією дітей охоплює й онлайн-злочини, що містять гендерний вимір.¹⁰⁹ Крім того, у грудні 2022 року Європейська комісія ініціювала розробку окремої директиви щодо боротьби з **гендерно обумовленим насильством в інтернеті**¹¹⁰, яка пропонує криміналізувати: цифрове переслідування, розповсюдження інтимних зображень без згоди та онлайн-дискредитацію.

Для осмислення специфіки формування гендерних відносин в українській кібербезпеці, варто розпочати дослідження з ретельного аналізу чинної державної політики та законодавчих актів, оскільки саме вони встановлюють нормативні рамки та відображають рівень інституційної підтримки **гендерної рівності** у цій стратегічно важливій для України сфері.

Нормативно-правове регулювання кібербезпеки в Україні базується переважно на технократичному підході, орієнтованому на захист інформаційних систем, критичної інфраструктури та запобігання кіберзагрозам на рівні держави й приватного сектору. Водночас у чинних політиках майже не враховується вплив цифрових загроз на різні соціальні групи, зокрема — за ознакою статі. У результаті специфічні ризики, з якими стикаються жінки в онлайн-середовищі (зокрема **кібернасильство**, переслідування, сексторшен), залишаються поза увагою профільних стратегій. На відміну від деяких міжнародних практик, у яких враховується вразливість жінок до певних форм цифрових загроз, українські політики кібербезпеки поки що залишають ці аспекти поза увагою.

Центральним нормативним актом у сфері **кібербезпеки** є **Закон України "Про основні засади забезпечення кібербезпеки України"** від 5 жовтня 2017 року №

¹⁰⁹Directive 2011/93/EU of the European Parliament and of the Council.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0093>

¹¹⁰ EU Commission. (2022). Proposal for a Directive on combating violence against women and domestic violence.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0105&utm>

2163-VIII¹¹¹. Документ регламентує діяльність органів державної влади, правоохоронних структур, операторів критичної інфраструктури та суб'єктів господарювання у сфері кіберзахисту. Однак у тексті відсутні будь-які згадки про гендерну рівність, протидію дискримінації чи заходи підтримки представниць жіночої статі в секторі кібербезпеки. Натомість, закон містить загальні положення, які можна інтерпретувати як потенційне підґрунтя для гендерно чутливого тлумачення. Лише загальна згадка про **принцип недискримінації** (стаття 2, пункт 6) може бути інтерпретована як потенційна можливість гендерно чутливого тлумачення, згідно з яким “рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до відмінностей у правах та обов'язках осіб у подібних ситуаціях, якщо така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу”.¹¹² Хоча ця норма може застосовуватись у ширшому контексті забезпечення рівності, вона не передбачає жодного акценту на гендерну специфіку кіберзагроз і не пропонує механізмів реалізації рівного доступу жінок до сфери кіберзахисту.

Таким чином, Закон “Про кібербезпеку” є гендерно нейтральним, але не гендерно чутливим, що суперечить сучасним європейським практикам безпеки, де цифрові права, зокрема захист від гендерно обумовленого онлайн-насильства, інтегруються у загальну безпекову стратегію. Наприклад, **Директива ЄС 2024/1385** передбачає криміналізацію таких форм **кібернасильства**, як несанкціоноване поширення інтимних зображень, **deepfakes**, кіберпереслідування, **доксинг** і **кіберфлешинг**, а також зобов'язує держави-члени забезпечити спеціалізовану допомогу постраждалим і механізми запобігання. У фокусі цієї політики — визнання цифрових загроз, як чинника системної нерівності, що обмежує громадську участь жінок, зокрема в медіа, політиці та сфері безпеки.

На рівні аналітичних установ, таких як **Європейський інститут з питань гендерної рівності (EIGE, 2024)**, також підкреслюється потреба в окремих вимірювальних і політичних інструментах для реагування на кібернасильство, яке непропорційно зачіпає жінок. Відсутність подібних положень в українському законодавстві не лише обмежує можливості для захисту вразливих груп, а й свідчить про необхідність переосмислення підходів до цифрової безпеки, як багатовимірного явища, що вимагає урахування соціальних, правових і гендерних факторів.

В українському законодавстві не передбачено спеціальних положень щодо гендерної специфіки кіберзагроз, хоча дослідження свідчать про те, що жінки є непропорційно вразливою групою у цифровому середовищі. Згідно з даними Європейського інституту з питань гендерної рівності (EIGE, 2017), кожна десята жінка в ЄС стикалася з проявами кібернасильства з 15 років, включно з кіберсталкінгом, сексторшеном, розповсюдженням інтимного контенту без згоди, шантажем або погрозами у соціальних мережах. Ці форми насильства часто поєднуються з

¹¹¹ Закон України “Про основні засади забезпечення кібербезпеки України” № 2163-VIII
<https://zakon.rada.gov.ua/laws/show/2163-19>

¹¹²Верховна Рада України. (2017)

фізичним або сексуальним насильством у реальному житті: 77% жінок, які зазнали кіберцькування, також пережили насильство з боку партнера¹¹³.

У цьому контексті відсутність подібних норм в українській системі права вказує на необхідність актуалізації політики кібербезпеки з урахуванням гендерної специфіки ризиків. Це особливо критично у воєнний період, коли зростає рівень агресивних комунікацій у цифровому просторі щодо жінок — військовослужбовиць, активісток, журналісток.

Українська нормативна база в цій площині залишається фрагментарною. Попри мовчання спеціалізованого закону про кібербезпеку, деякі суміжні нормативно-правові акти створюють підґрунтя для імплементації гендерної складової в цифрову політику. Зокрема, **Закон України “Про забезпечення рівних прав та можливостей жінок і чоловіків”**¹¹⁴ закріплює обов’язок державних органів впроваджувати **гендерну рівність** у всіх сферах державного управління, включно з інформаційною політикою. Важливо, що закон надає інструмент гендерно-правової експертизи — дієвий механізм оцінки нормативно-правових актів на предмет гендерної дискримінації, який цілком може (і повинен) застосовуватись до актів, що регулюють сферу кібербезпеки.

Аналогічно, **Закон України “Про запобігання та протидію дискримінації”**¹¹⁵ формалізує можливість юридичного оскарження дискримінаційних практик. У контексті цифрової сфери це означає, що бар’єри для жінок у доступі до професій у сфері ІТ та кібербезпеки, зокрема у формі **структурної дискримінації** чи прихованих **гендерних упереджень**, можуть бути предметом правового аналізу та виправлення. Втім, на практиці механізми реалізації цих норм залишаються малоефективними через відсутність чітких адміністративних процедур, відповідального органу та моніторингових інструментів.

Значущим документом у сфері цифрової безпеки є **План реалізації Стратегії кібербезпеки України**, схвалений РНБО 30 грудня 2021 року та введений у дію Указом Президента № 37/2022.¹¹⁶ Цей план розрахований на п’ятирічний період, тож у найближчій перспективі очікується оновлення як самої Стратегії, так і Плану її реалізації. Це створює підґрунтя для актуалізації підходів до цифрової безпеки з урахуванням гендерних чинників та включення гендерної складової в державну кіберполітику.

У документі окреслено низку цілей і заходів, спрямованих на посилення спроможностей держави щодо кібероборони, реагування на кіберінциденти, розвитку критичної інформаційної інфраструктури та гармонізації з міжнародними

¹¹³ European Institute for Gender Equality. (2017)

file:///C:/Users/user/Downloads/cyber_violence_against_women_and_girls.pdf

¹¹⁴ Закон України “Про забезпечення рівних прав та можливостей жінок і чоловіків” № 2866-IV від 08.09.2005.

<https://zakon.rada.gov.ua/laws/show/2866-15>

¹¹⁵ Закон України “Про засади запобігання та протидії дискримінації в Україні” № 5207-VI від 06.09.2012.

<https://zakon.rada.gov.ua/laws/show/5207-17>

¹¹⁶ Про План реалізації Стратегії кібербезпеки України

<https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>

стандартами. Зокрема, передбачається створення кібервійськ, систем управління інцидентами, національного плану реагування на кризи в кіберпросторі, запровадження обов'язкових аудитів інформаційної безпеки, а також розвиток кіберосвіти та науки в Україні.

Однак аналіз змісту документа свідчить про відсутність системного гендерного підходу: у Плані повністю ігнорується питання гендерної нерівності або гендерно обумовлених кіберзагроз. Жоден із пріоритетів, включно з розвитком людського капіталу у сфері кібербезпеки, не містить посилань на необхідність урахування потреб жінок або інших соціально вразливих груп. Це вказує на домінування **технократичного дискурсу** в українській кіберстратегії, у межах якого питання інклюзії, різноманіття та соціальної справедливості залишаються поза полем уваги.

У результаті, навіть маючи потенціал для трансформації державної кіберполітики в інноваційну та стійку, Стратегія реалізується без інтеграції гендерної оптики, що суперечить сучасним підходам до цифрової безпеки, які визнають нерівномірний вплив кіберзагроз на різні соціальні групи.

2.2.2. Державні ініціативи та програми гендерної інклюзії в кібербезпеці

Незважаючи на виявлену в попередньому аналізі обмежену гендерну чутливість ключових законодавчих актів та стратегічних документів, упродовж останніх років в Україні спостерігається поступове формування нормативно-політичної чутливості до потреб гендерної інклюзії у сфері кібербезпеки. Хоча спеціалізовані державні політики щодо інтеграції гендерного підходу в цифрову безпеку залишаються фрагментарними й декларативними, окремі **інституційні ініціативи** демонструють зрушення в напрямку визнання важливості участі жінок у національній кіберстійкості. Відбувається поетапне зміщення фокусу з технократичного підходу до більш інклюзивної парадигми цифрової безпеки, яка враховує соціальні чинники ризику, включно з **гендерною нерівністю**.

Показовим є активізація діяльності Національного координаційного центру кібербезпеки при РНБО України, зокрема в аспектах публічної підтримки жіночого лідерства у сфері кіберзахисту. У грудні 2024 року відбулося 32-ге засідання Національного кластера кібербезпеки, присвячене темі “Роль жінок у забезпеченні кіберстійкості України: виклики та перспективи”.¹¹⁷ Захід, організований НКЦК спільно з ГО «Фундація жіночого лідерства та стратегічних ініціатив», Фондом цивільних досліджень і розвитку США за підтримки Державного департаменту США, став першим у низці подій, які мають на меті інституціоналізувати гендерний вимір в політиці кібербезпеки України. Під час відкриття заходу заступник Секретаря РНБО України Сергій Демедюк наголосив: “Залучення жінок до сфери кібербезпеки значно підсилює нашу здатність протидіяти кіберзагрозам. Жінки мають унікальне мислення, яке доповнює підходи чоловіків, створюючи синергію, що дозволяє успішно вирішувати найскладніші завдання. Ми повинні сприяти тому, щоб більше

¹¹⁷ Рада національної безпеки і оборони України. (2024).

жінок та дівчат знаходили своє місце в кіберсфері, адже їхній потенціал здатний посилити нашу спроможність на всіх рівнях — від оперативних дій до стратегічного планування та ухвалення ключових рішень”¹¹⁸.

Керівниця служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, секретарка Наталія Ткачук підкреслила: *“Під час повномасштабного вторгнення РФ залучення жінок до сфери кібербезпеки — це не просто питання рівності чи дотримання міжнародних стандартів. Це життєва необхідність для зміцнення національної безпеки та забезпечення стійкості держави. Жінки завжди відігравали важливу роль у розвитку нашої країни, і сьогодні їхній внесок стає ще більш значущим. Ми маємо створювати можливості для професійного зростання та розвитку на всіх рівнях - від здобуття освіти до керівних посад, сприяючи залученню нових талантів у сферу кібербезпеки. Це не лише зміцнює нашу економіку та технологічний розвиток, але й сприяє спільній перемозі в боротьбі за майбутнє України”*.¹¹⁹ Важливою частиною заходу стали практичні сесії, під час яких учасники й учасниці розробляли пропозиції для національної ініціативи з підвищення **гендерної рівності** у сфері кібербезпеки. Ці напрацювання мають потенціал стати основою для майбутніх політик з розширення участі жінок у цифровому врядуванні, зокрема в контексті нормативної розробки та імплементації стандартів гендерно чутливої кіберстійкості.

Важливим інструментом реалізації таких прагнень та виконання міжнародних зобов'язань держави став Національний план дій з виконання резолюції **Ради Безпеки ООН 1325 "Жінки, мир, безпека"**. Уряд України за підтримки міжнародних партнерів інтегрував у Національний план дій за вищезазначеною резолюцією Ради Безпеки ООН серію заходів, які не лише відкрили жінкам доступ до вузькопрофільних курсів із кібербезпеки, а й закріпили за ними право на участь у формуванні національних стандартів захисту¹²⁰. Зі звіту Київської міської державної адміністрації за 2022 рік видно, що тепер у складі експертних груп та консультаційних рад з **кіберзахисту** обов'язково мають бути представниці жіночого кластера, де їхня думка реально впливає на політики оборони¹²¹. Паралельно структура UN Women координувала проведення воркшопів і грантових програм. Без такого мультисекторного підходу справжнє розкриття жіночого потенціалу в кібербезпеці й надалі залишатиметься декларацією на папері. Окрім державних ініціатив, реалізованих під егідою Національного координаційного центру кібербезпеки, в Україні активно впроваджуються міжсекторальні програми, що спрямовані на підтримку, навчання та залучення жінок до сфери цифрової безпеки. Вони мають різний формат — від громадських платформ до державних програм перекваліфікації — та виконують ключову роль у формуванні інклюзивного кадрового потенціалу для кіберсектору.

¹¹⁸ Рада національної безпеки і оборони України. (2024).

¹¹⁹ Рада національної безпеки і оборони України. (2024).

¹²⁰ Київська міська державна адміністрація. (2022). Звіт про виконання Національного плану дій з виконання резолюції Ради Безпеки ООН 1325 "Жінки, мир, безпека" на період до 2025 року.

¹²¹ КМДА. (2022). Звіт про виконання Національного плану дій 1325.

У лютому 2025 року в Києві відбувся спільний захід "Кіберінновації та стійкість: **Women4Cyber Talks**", що об'єднав понад 100 представників державного, приватного та академічного секторів.¹²² Його мета - формування національного дискурсу довкола ролі жінок у забезпеченні кіберстійкості України. Участь у заході взяли провідні експертки з цифрової безпеки, а також менторки для студенток, що засвідчує зростання горизонтальних зв'язків у професійній спільноті.

Проект "**Reskilling Ukraine**" є масштабною програмою перекваліфікації, орієнтованою на жінок, ветеранів та ветеранок, які втратили роботу внаслідок війни. Ініціатива реалізується шведською неприбутковою організацією Beredskapslyftet у партнерстві з Міністерством економіки України та за підтримки уряду Швеції, приватних шведських фондів і бізнесу.¹²³ Цей проєкт також активно співпрацює з органами державної влади, організаціями та бізнесом у контексті інклюзивності та соціальної відповідальності, сприяючи формуванню інклюзивного середовища та підтримці жіночого лідерства у сфері кібербезпеки.¹²⁴

Лідерська програма для жінок, залучених до цифровізації держпослуг, започаткована **Програмою розвитку ООН в Україні (UNDP)** у партнерстві з **CDTO Campus** за фінансової підтримки уряду Швеції, є показовим прикладом **міжнародно-державної ініціативи**, яка прямо сприяє **гендерній інклюзії** в цифровому державному управлінні.¹²⁵ Хоча програма не фокусується виключно на кібербезпеці, вона функціонує в полі ширшої цифрової трансформації, де питання кіберзахисту, цифрової грамотності та безпечного управління інформацією є інтегральними. У фокусі програми — підготовка жінок-лідерок до впровадження цифрових інструментів у державному секторі, зокрема в контексті послуг для населення. Навчальні модулі програми охоплюють як технічну складову цифрової трансформації (впровадження електронних сервісів, захисту даних, аналітики процесів), так і розвиток софт-скілів, які є критично важливими для просування жінок на керівні посади — публічні виступи, ведення переговорів, стратегічна комунікація тощо. Принципово важливо, що ця ініціатива орієнтована на практичну підтримку представниць органів влади, місцевого самоврядування та **цифрових інституцій**, які вже залучені до процесів **цифровізації** або прагнуть активніше включитися в цю сферу. У такий спосіб програма не лише збільшує представництво жінок у ключових процесах діджиталізації, а й підсилює їхній вплив на формування політик, у тому числі у сферах дотичних до безпеки, управління ризиками, захисту даних і кіберстійкості державних інституцій. Її приклад свідчить про поступовий перехід від декларативних закликів до **гендерної рівності** до структурної інтеграції жінок у цифрові стратегії держави. Такий підхід дозволяє не лише розширити можливості для жінок у сфері високотехнологічного державного управління, але й забезпечити

¹²²https://www.linkedin.com/posts/ncsc_the-role-of-women-in-strengthening-ukraines-activity-7295440315245592576-OcYw?utm

¹²³ <https://www.reskillingukraine.com/>

¹²⁴ Reskill Ukraine Women to Tech and IT Jobs Program - FutureCollars

¹²⁵ UNDP

<https://www.cdto-campus.com/ua/programs/undp-liderska-programa-dlya-zhinok-zalucheni-h-do-cifrovizaciyi-derzhpslug>

сталість та ефективність інституційної кіберстійкості шляхом залучення різноманітного управлінського потенціалу.

У цьому ж контексті варто згадати про ще одну важливу ініціативу — проєкт **USAID** “Кібербезпека критично важливої інфраструктури України”, який був менторською програмою для студенток спеціальності “Кібербезпека”, руйнував стереотипи про виключно “чоловічі” професії та підтримував жінок у галузі кібербезпеки. Програма проходила онлайн протягом серпня та вересня 2022 року.¹²⁶ До неї також відноситься вебінар “Побудова кар’єри жінок у сфері кібербезпеки: рекомендації та поради успішних професіоналок”, який відбувся в травні 2023 року. Вебінар був призначений для студентства і мав на меті розповісти три різні історії харизматичних кіберексперток та їх приклади кар’єрного зростання у кібербезпеці¹²⁷. А 31 жовтня 2023 року, проєкт **USAID** “Кібербезпека критично важливої інфраструктури України” у партнерстві з Аспен Інститутом Київ провели діалог на тему: “Гендерне різноманіття в кібербезпеці: реалії та можливості для жінок в Україні”. Метою діалогу було налагодження співпраці між представниками та представницями різних галузей для просування гендерної рівності в сфері кібербезпеки в Україні та опрацювання рекомендацій для подолання перешкод у професійній реалізації жінок.¹²⁸

У цьому ж напрямі діє й **ініціатива SheCyber Hub**, започаткована ГО “Фундація жіночого лідерства та стратегічних ініціатив” у співпраці з Національним університетом “Кієво-Могилянська академія”. Проєкт створює простір для розвитку студенток і молодих фахівчинь у сфері кібербезпеки, поєднуючи освітні заходи, зустрічі з лідерками галузі, менторство, практичні воркшопи та проєктну роботу. Особлива увага приділяється формуванню спільноти підтримки й створенню доступу до рольових моделей — жінок, які досягли успіху у сфері кібербезпеки та готові ділитися досвідом. SheCyber Hub сприяє залученню жінок до професійної спільноти, розвитку лідерського потенціалу та руйнуванню гендерних стереотипів у галузі.

Усі проаналізовані ініціативи демонструють потенціал для формування нової генерації жінок-експерток у сфері кібербезпеки та цифрового врядування. Водночас для забезпечення їхньої сталості необхідна цілеспрямована підтримка з боку держави — не лише у вигляді фінансування, а й через нормативне закріплення та інтеграцію результатів у публічну політику. За умови політичної волі такі програми можуть стати основою для структурного гендерного реформування ІТ-сектору та посилення інституційної кіберстійкості України.

¹²⁶ DOU. (2022). Менторська програма для студенток спеціальності “Кібербезпека”

¹²⁷ DOU. (2023). Вебінар “Побудова кар’єри жінок у сфері кібербезпеки: рекомендації та поради успішних професіоналок”

¹²⁸ Громадський Простір. (2023). “Гендерне різноманіття в кібербезпеці: реалії та можливості для жінок в Україні”: відбувся Діалог в межах програми “Діалог про кібербезпеку”

2.2.3. Війна як фактор актуалізації гендерного виміру в безпековому секторі

Розглянуті вище державні та міжсекторальні програми, що демонстрували певний прогрес у напрямку **гендерної інклюзії**, з лютого 2022 року функціонують в абсолютно нових реаліях. Повномасштабне вторгнення російської федерації у 2022 році суттєво трансформувало архітектуру національної безпеки України, включаючи кіберпростір як ключовий компонент гібридної війни. Водночас війна актуалізувала потребу в переосмисленні ролі жінок у безпековому секторі, зокрема в його цифровому сегменті. Як зазначає Шопіна, з 2014 року, а особливо з 2022 року, спостерігається зростання чисельності жінок у секторі оборони, зокрема в напрямках стратегічного планування та інформаційної безпеки¹²⁹. При цьому, авторка наголошує, що зростання кількості жінок у сфері не супроводжується відповідним підвищенням їхньої ролі у процесах прийняття рішень — жінки залишаються недостатньо представленими на управлінських і аналітичних рівнях, що свідчить про стійкість **горизонтальної сегрегації**.¹³⁰

Зміна характеру загроз, зокрема в цифровій площині, спричинила зростання форм насильства, специфічно орієнтованих на жінок. За результатами дослідження Л. Сороки, в умовах війни особливого поширення набули такі явища, як кіберсталкінг, сексторшен, масова публікація персональних даних без згоди, дискредитаційні кампанії та дезінформація, спрямована на жінок, які беруть активну участь у громадському житті — журналісток, військовослужбовиць, активісток¹³¹. Цифровий простір, таким чином, стає не лише каналом інформування, а й середовищем репресивного контролю, що ускладнює участь жінок у публічному просторі.

У статті І. Шопіної наголошується, що гендерна політика в умовах воєнного стану вимагає переходу від суто декларативного забезпечення прав до розробки функціональних механізмів залучення жінок до безпекового управління, зокрема в ІТ-секторі. Авторка підкреслює, що війна чинить подвійний вплив: з одного боку — посилює вразливість жінок, з іншого — відкриває можливості для їхнього професійного зростання у сферах, де раніше їхня присутність була маргіналізованою¹³². Крім того, реалізація Національного плану дій з виконання **Резолюції Ради Безпеки ООН 1325 “Жінки, мир, безпека”** сприяла формалізації підходів до залучення жінок у безпековий сектор, включно з цифровими напрямками. У рамках цього процесу започатковуються механізми участі жінок у консультаційних, аналітичних і експертних групах при органах державного управління, зокрема у

¹²⁹ Шопіна.І (2024). Гендерний баланс та гендерна рівність в секторі безпеки і оборони: проблеми і перспективи.<https://academy-vision.org/index.php/av/article/view/1548/1479>

¹³⁰ Шопіна.І (2024). Гендерний баланс та гендерна рівність в секторі безпеки і оборони: проблеми і перспективи.<https://academy-vision.org/index.php/av/article/view/1548/1479>

¹³¹ Сорока, Л. (2023). Цифрове насильство щодо жінок у період війни. У зб.: *Гендерна політика в умовах воєнного стану: правовий вимір*. Репозиторій БНАУ. https://rep.btsau.edu.ua/bitstream/BNAU/8785/1/Vplyv_viiny.pdf

¹³² Шопіна.І (2024). Гендерний баланс та гендерна рівність в секторі безпеки і оборони: проблеми і перспективи.<https://academy-vision.org/index.php/av/article/view/1548/1479>

сферах, що стосуються кіберзахисту. Така практика закладає основу для більш інклюзивного та гендерно збалансованого підходу до публічного адміністрування в секторі національної безпеки.

Таким чином, російсько-українська війна стала не лише викликом для безпеки держави, а й каталізатором зміни підходів до гендерної інклюзії в стратегічних секторах. У сфері кібербезпеки це проявляється як у зростанні жіночого представництва, так і в актуалізації потреби нормативного оформлення гендерно чутливої політики — через перегляд чинного законодавства, розширення освітніх ініціатив і посилення інституційної спроможності щодо реагування на цифрові загрози, зокрема з гендерним виміром. Водночас важливим фактором змін стало усвідомлення того, що кібербезпека, поряд із військовою та гуманітарною безпекою, є одним із критичних компонентів сучасного безпекового середовища. Розширення фронту **гібридної агресії**, зокрема через інформаційні атаки, втручання в критичну інфраструктуру та кампанії з дезінформації, зумовило необхідність залучення ширшого кола фахівців і фахівчинь до розробки та реалізації політики цифрового захисту. У цьому контексті **Національний план дій з виконання Резолюції ООН 1325**¹³³ виступає інструментом нормативної легітимації участі жінок у секторах, що раніше не розглядалися крізь призму гендерної інклюзії, зокрема в інформаційній та кібербезпеці. Передбачене в документі залучення жінок до процесів прийняття рішень у безпековій сфері створює підґрунтя для формування цілісної, **гендерно збалансованої кіберполітики**.

2.2.4. Ініціативи бізнесу та приватного сектора щодо забезпечення гендерної рівності в кібербезпеці

Важливим аспектом створення гендерно чутливого середовища в кібербезпеці України є ініціативи, що виходять з приватного сектору. Порівняно з урядом, який у більшості випадків встановлює загальні рамки, бізнес може гнучкіше реагувати на потреби ринку та застосовувати інновації в підходах до залучення та підтримки жінок. Тому в цьому розділі аналізується практика провідних ІТ-компаній разом з міжнародними організаціями, що працюють в Україні, щодо їхніх зусиль, спрямованих на заохочення гендерної рівності з метою подолання існуючих бар'єрів. Усі ці ініціативи здійснюються на тлі кількох системних викликів. Зокрема, незважаючи на гостру нестачу висококваліфікованих фахівців – теоретично, це мало б забезпечити більше місця для українських жінок у кібербезпеці – усталені стереотипи щодо “чоловічого” характеру цієї професії продовжують виступати дуже суттєвими перешкодами¹³⁴. Як наслідок, хоча після 2022 року частка жінок в ІТ-секторі загалом зросла¹³⁵, саме в кіберзахисті вони й далі складають меншість на критичних технічних і управлінських ролях¹³⁶.

¹³³ Cabinet of Ministers of Ukraine. (2022)https://uwf.org.ua/wp-content/uploads/2023/03/nap-1325_eng.pdf?utm

¹³⁴ Orange Cyberdefense. (n.d.). For a safer digital society: Breaking down gender barriers in cybersecurity.

¹³⁵ DOU. (2024). Жінки в українській ІТ-індустрії: як змінюється гендерний баланс та роль жінок.

¹³⁶ ISC2. (2023). Women in cybersecurity: Inclusion, advancement and pay equity.

Надзвичайно важливі зміни прийшли в освітній та професійний ландшафт кібербезпеки: нові складні кіберзагрози змусили фахівців постійно розробляти інноваційні методи захисту, а також модернізувати інструменти реагування. В додачу до цього спостерігається загальний дефіцит публічної інформації та досліджень, які б детально описували ситуацію та кар'єрні шляхи жінок в українському секторі кібербезпеки, особливо під час війни. Прогалини в навчальних програмах, що не враховують потреби жінок, недостатні для вирішення викликів нових викликів. Як повідомляє DOU, жінки становлять приблизно 24% від загальної кількості ІТ-працівників в Україні, але лише 19% обіймають технічні посади¹³⁷. Політика та системи навчання, які не реформовані належним чином, увічнюють існуючі системні прогалини, тим самим дозволяючи нерівну участь у просуванні по кар'єрних сходах та зайнятті стратегічних посад. Це можна змінити за допомогою конкретних втручань – спеціалізованих курсів, програм наставництва та прозорих критеріїв відбору на керівні посади.¹³⁸

Незважаючи на гостру нестачу персоналу, кіберпростір все ще домінує з боку чоловіків, оскільки вступ до стратегічних груп офіційного відбору блокується не через кваліфікацію, а радше через неформальні зв'язки, де обговорюються питання безпеки. Кандидатура жінок виступає під питанням щоразу, коли йдеться про державний захист, ця недовіра підсилює їхню ізоляцію. Ненавмисне заперечення формує середовище повільного відсторонення: навіть найсміливіші спеціалісти змушені виконувати складні завдання поза своєю основною сферою діяльності, хоча й готові брати на себе відповідальність. Подібний сценарій спостерігається в усьому ІТ-секторі України: гендерний дисбаланс залишається одним із найяскравіших маркерів несправедливості і¹³⁹.

Цей підрозділ має на меті виявити та описати конкретні бар'єри, з якими стикаються українські фахівчині з кібербезпеки в умовах безперервного конфлікту. Саме тому особливий інтерес має аналіз конкретних ініціатив, що реалізуються різними компаніями, як українськими, так і міжнародними, які працюють в Україні. Порівняння їхніх підходів до залучення, підтримки та професійного розвитку жінок у кібербезпеці дасть змогу виявити найефективніші моделі та найкращі практики, які можуть бути масштабовані для подолання наявного **гендерного дисбалансу**. Для порівняльного аналізу ролі бізнесу в забезпеченні **гендерної рівності** у сфері кібербезпеки розглянемо діяльність декількох компаній, що надають послуги в ІТ-галузі, серед яких українська компанія ELEKS, а також Sigma Software та Apriorit, котрі мають значний досвід у розробці рішень, зокрема й у галузі кібербезпеки.

¹³⁷ DOU. (2024). Жінки в українській ІТ-індустрії: як змінюється гендерний баланс та роль жінок.

¹³⁸ DOU. (2022). Менторська програма для студенток спеціальності "Кібербезпека".

¹³⁹ UN Women Ukraine. (2024, September). Скорочення гендерного розриву в оплаті праці з 186 до 136 та старт національної кампанії "Звісно зможеш": Як Україна рухається до економічного уповноваження жінок у часи великої війни.

ELEKS входить до 100 найкращих світових аутсорсингових компаній, яка понад 30 років надає експертні послуги з розробки програмного забезпечення та консультації.¹⁴⁰ ELEKS демонструє публічну прихильність до гендерної рівності та інклюзивності. Компанія позиціонує себе як роботодавця рівних можливостей та включає різноманітність, справедливість та інклюзивність до своїх ключових напрямків корпоративної соціальної відповідальності. Вона прагне створювати інклюзивні та різноманітні IT-спільноти з рівними можливостями не лише в Україні, а й для низки інших країн.¹⁴¹

У 2021 році компанія отримала звання кращої компанії, дружньої до сім'ї, серед IT-компаній. Ці кроки свідчать про визнання більш глобальних соціальних факторів, що впливають на кар'єру жінок. ELEKS підкреслює важливість добробуту співробітників та створення престижного робочого місця, де панують повага, довіра та підтримка, що сприяють особистому зростанню та забезпечують конкурентну заробітну плату. За даними компанії, 34% її спеціалістів складають жінки. ELEKS також бере участь у зустрічах "Women In Tech".¹⁴²

Sigma Software демонструє рішучий та активний підхід до гендерної рівності, бажаючи усунути перепони, що ґрунтуються на упередженнях, сприяє розмаїттю та мультикультурності.¹⁴³ Компанія підкреслює, що її стратегія завжди була зорієнтована на людей, їх потреби, професійне зростання та реалізацію потенціалу незалежно від гендеру. Sigma Software активно просуває гендерну рівність з моменту свого заснування, а з 2022 року виділила це питання в окремий проєкт. Компанія прагне відповідати міжнародним стандартам та вимогам соціально відповідальних партнерів щодо **DEI (diversity, equity, and inclusion)** та гендерного балансу. Sigma Software наголошує на потребі залучення більшої кількості жінок до технічної сфери для розширення кадрового резерву та боротьби зі стереотипами в суспільстві.¹⁴⁴

Частка жінок, які працюють у Sigma Software становить 35%, що перевищує середній показник у галузі — 25%. Близько 50% жінок займають керівні посади. У технічних та інженерних підрозділах їхня частка становить 19%. Компанія прагне усунути розбіжності в оплаті праці, невинно відслідковує ринок та пропонує належну заробітну плату в залежності від професійного рівня та досвіду працівника, незважаючи на гендер чи інші характеристики. Вона гарантує гендерну рівність у питаннях умов праці та можливостей (компенсація, робочий час, баланс між роботою та особистим життям, страхування, відпустки, декретні відпустки, механізми захисту від булінгу та домагань)¹⁴⁵.

Компанія Apriorit прагне забезпечити гендерну рівність, що стосується представництва жінок та їхнього кар'єрного зростання в межах організації. Apriorit визначає ключові аспекти забезпечення гендерної рівності, включаючи нейтральний підхід до відбору кандидатів, гендерно збалансоване лідерство при розподілі ролей,

¹⁴⁰ <http://eleks.com/news/eleks-2021-global-overview/>

¹⁴¹ <https://eleks.com/about-eleks/corporate-social-responsibility/>

¹⁴² <https://careers.eleks.com/about/>

¹⁴³ <https://cdn.sigma.software/wp-content/uploads/2024/12/SigmaSoftware-Gender-Equality.pdf>

¹⁴⁴ <https://cdn.sigma.software/wp-content/uploads/2024/11/DEI-manifesto.pdf>

¹⁴⁵ <https://sigma.software/about/csr>

доступні кар'єрні шляхи незалежно від гендеру, а також безпечне та комфортне робоче середовище.¹⁴⁶ Посаду генерального директора Apriorit обіймає жінка — Клавдія Заїка, що може свідчити про підтримку гендерної рівності на рівні керівництва. Крім того, компанія підкреслює важливість інклюзивного дизайну в розробці програмного забезпечення, спрямованого на забезпечення доступності продуктів для користувачів з різним походженням та можливостями¹⁴⁷.

Отже, всі три компанії є важливими учасниками ІТ-галузі України. Вони забезпечують робочі місця для тисяч українських ІТ-фахівців, сприяють розбудові технологічної експертизи в країні та роблять чималий внесок в економіку України через експорт ІТ-послуг. Їхня діяльність в Україні охоплює увесь спектр розробки програмного забезпечення та супровідних послуг для міжнародних клієнтів. Якщо Sigma Software є явно вираженою структурою політики DEI, значною кількістю жінок на керівних посадах та детальним аналізом гендерної рівності, то ELEKS зосереджує увагу на глобальній діяльності та благополуччю своїх співробітників. Apriorit, зі свого ж боку, робить акцент на внутрішній рівності процесів.

Окрім ініціатив окремих українських компаній, важливу роль у залученні жінок до цифрової економіки та кібербезпеки, відіграють міжнародні організації та їхні проєкти, які часто реалізовані у відповідь на виклики, спричинені війною.

Відділ процвітання ЮНІТАР запуслав свою навчальну програму “Підвищення рівня життя: Цифрова перекваліфікація для українських жінок-евакуйованих у Польщі” 16 жовтня 2023 року на заході у Варшаві. Серед гостей були представники уряду, партнерів програми, академічних установ, неурядових організацій та учасниці нового тренінгу. Навчальна програма тривала з жовтня 2023 року по березень 2024 року. Близько 1000 українських жінок, евакуйованих у Польщі, подали заявки на участь у програмі¹⁴⁸. Такі програми перекваліфікації є критично важливими для жінок, чиї кар'єри були перервані війною, надаючи їм можливість увійти до перспективних технологічних секторів дотичними до кібербезпеки.

Також, всесвітньо відома корпорація Microsoft співпрацює на національному та місцевому рівнях, щоб збільшити кількість жінок у галузі кібербезпеки, працюючи з такими організаціями, як Інститут Костюшка в Польщі, реалізуючи програми навчання та стажування для жінок, у тому числі українських біженок, та співпрацює з понад 20 іншими неприбутковими організаціями, які так само зосереджені на підготовці жінок до можливостей працевлаштування¹⁴⁹. Партнерство великих технологічних корпорацій з локальними НУО та освітніми установами є ефективним механізмом для масштабування навчальних програм та їх адаптації до потреб конкретних груп жінок, зокрема тих, що постраждали від війни.

Підсумовуючи аналіз ролі бізнесу та приватних ініціатив, можна констатувати їхній зростаючий внесок у просування гендерної рівності в українській ІТ-сфері та дотичних до неї галузях, таких як кібербезпека. Компанії все частіше впроваджують

¹⁴⁶ <https://openapi.com/gender-equality-policy>

¹⁴⁷ <https://www.apriorit.com/dev-blog/design-accessibility-in-ui-ux>

¹⁴⁸ Digital Reskilling for Ukrainian Women Evacuees in Poland Programme Launched at Warsaw Ceremony. (2023)

¹⁴⁹ The world needs cybersecurity experts – Microsoft expands skilling effort with a focus on women - Microsoft On the Issues. (2023)

політики DEI, прагнуть забезпечити рівні можливості та усунути розрив в оплаті праці. Міжнародні організації та корпорації також запускають цільові програми перекваліфікації та навчання, особливо для жінок, які постраждали від війни. Однак, попри ці позитивні зрушення, залишаються виклики, пов'язані з **горизонтальною сегрегацією** (нижче представництво жінок у суто технічних ролях кібербезпеки), подоланням глибоко вкорінених стереотипів та забезпеченням реального просування жінок на вищі технічні та керівні позиції саме у сфері кіберзахисту. Ефективність цих ініціатив значною мірою залежатиме від їхньої системності, довгостроковості та здатності адаптуватися до специфічних потреб жінок в умовах війни та повоєнного відновлення.

2.2.5. Вплив повномасштабної війни на гендерні аспекти кібербезпеки України

Повномасштабне вторгнення росії спричинило значні трансформації на ринку праці в українській кібербезпеці. Мобілізація значної частини чоловіків-спеціалістів та різке зростання попиту на фахівців сформували унікальне “вікно можливостей” для жінок¹⁵⁰. Вони почали активніше залучатися до сфери, заповнюючи кадрові прогалини, демонструючи високий професіоналізм та впроваджуючи нові підходи, що сприяло певній трансформації уявлень про їхню суб'єктність та роль у кіберспільноті¹⁵¹. Кіберпростір став помітним майданчиком для професійної самореалізації жінок. Однак цей процес відбувається на тлі парадоксального виклику: мілітаризація публічного дискурсу та сприйняття кіберзахисту як частини військових дій потенційно могли посилити традиційні гендерні стереотипи щодо “чоловічої” природи безпекового сектору¹⁵², створюючи додатковий тиск на жінок, що входять у цю традиційно маскулінізовану сферу.

У багатьох професійних середовищах України оборона й безпека все ще сприймаються як суто чоловічі сфери, а жінку швидше уявляють біля плити чи поруч із колискою дитини. Подібні уявлення не оминають і технологічний сектор: часто доводиться чути, що роботою з алгоритмами чи мережевим аналізом повинні займатися люди з “характером воїна”, натякаючи на “чоловічий” тип мислення. Навіть найсміливіші спроби жінок вступити до пентест-к о м а н д и зустрічають скепсис через недостатню “стриманості” чи “холодний розрахунок”¹⁵³. Архетип хакера-ін д и від у а л і с т а лише зміцнює бар'єр, підкреслюючи, що до “великої цифрової війни” мають допускатися ті, хто відповідає уявленню про міцного чоловіка¹⁵⁴. В цьому контексті, війна росії проти України могла посилити деякі гендерні стереотипи: під мілітарною парадигмою кіберзахист постає як продовження бойових мистецтв і все більше укріплює уявлення про цю сферу як традиційно “чоловічу”. Водночас гострий дефіцит кваліфікованих кадрів змушує відмовитися від

¹⁵⁰ United24Media. (n.d.). On how Ukrainian women are reshaping the workforce amid war.

¹⁵¹ European Cyber Security Organization. (2023). Women in Cybersecurity: Global and Ukrainian perspectives.

¹⁵² Gender and cybersecurity: Legal frameworks and policy implications.

¹⁵³ Lack of respect, career opportunities lead to exclusion for women in cybersecurity.

¹⁵⁴ Women in cybersecurity: Challenges and opportunities in the digital age [Conference paper]. Chornomorskyi National University.

забобонів і відкриває двері талановитим жінкам. Проте, існують свідчення, що децентралізовані російськомовні кібергрупи час від часу висловлюють сумніви в адекватності “хакерок”, адже архетип агресивної маскулінності залишається домінантним¹⁵⁵. Коли військові завдання мігрують у цифрову площину, жінки переважно опиняються на периферійних позиціях, виконуючи другорядні ролі захисту.

Щодо кар’єрного зростання, жінки в технологічному секторі зіштовхуються зі **структурними бар’єрами**, що обмежують їхнє просування. На глобальному рівні для них спостерігається ефект **“скляної стелі”**¹⁵⁶ на шляху до топ-менеджерських позицій, але в кібербезпеці ці складнощі набувають особливої гостроти: справжні можливості очолити стратегічні проекти нівелюються, а наставницькі ініціативи часто відтворюють патерни **горизонтальної та вертикальної гендерної сегрегації**¹⁵⁷. Хоча формально декларується рівний доступ до участі в експертних чи робочих групах, на практиці впливові неформальні мережі та центри ухвалення рішень часто залишаються замкненими для жінок¹⁵⁸, обмежуючи їхнє представництво вузьким колом. Хоча після 2022 року частка жінок в ІТ-секторі зросла на 4%, саме в кіберзахисті вони й далі складають меншість на критичних технічних і управлінських ролях¹⁵⁹. Ці фактори можуть призводити до так званого **“ефекту липкої підлоги”**, коли жінкам важко піднятися з початкових або середніх позицій, особливо у висококонкурентних та стресових умовах воєнного часу.

Наявний гендерний розрив в оплаті праці, характерний як для світового сектору кібербезпеки (де глобальний гендерний розрив у зарплатах становить близько 20 %¹⁶⁰), так і для економіки України загалом (де розбіжність до 2021 року трималася на позначці близько 18,6 %), а в рамках національної кампанії має скоротитися до 13,6 % до 2030 року¹⁶¹, не демонструє виражених тенденцій до скорочення. В умовах економічного спаду та підвищеної вразливості жінок на ринку праці існує ризик його подальшого поглиблення¹⁶². Навіть серед висококваліфікованих ІТ-фахівців, де частка українок уже сягає двозначних відсотків, **“зарплатні паузи”** на користь чоловіків зберігаються, демонструючи інерцію усталених уявлень про роль і винагороду в професії¹⁶³. Це означає, що на шляху до реальної гендерної рівності бракує не лише навичок і знань, а й чітких, прозорих механізмів коригування внутрішньої політики оплати праці. За даними DOU

¹⁵⁵ Sentsova, A., Lychak, M., O’Connor, S., & Thomas, W. (2024, November 18). Women in Russian-speaking cybercrime: Mythical creatures or significant members of underground? SANS Institute.

¹⁵⁶ ISC2. (2023). Women in cybersecurity: Inclusion, advancement and pay equity.

¹⁵⁷ WiCyS. (2023). 2023 State of Inclusion Benchmark in Cybersecurity Report.

¹⁵⁸ WiCyS. (n.d.). Lack of respect, career opportunities lead to exclusion for women in cybersecurity.

¹⁵⁹ DOU. (2024). Жінки в українській ІТ-індустрії: як змінюється гендерний баланс та роль жінок.

¹⁶⁰ ISC2. (2023). Women in cybersecurity: Inclusion, advancement and pay equity.

¹⁶¹ UN Women Ukraine. (2024, September). *Скорочення гендерного розриву в оплаті праці з 18,6 % до 13,6 % та старт національної кампанії “Звісно зможеш”*.

¹⁶² UN Women. (2025). *Three years of full-scale war in Ukraine roll back decades of progress for women’s rights, safety and economic opportunities*.

¹⁶³ DOU. (2022, October 18). *Портрет ІТ-спеціаліста 2022*.

(2024), жінки становлять близько 24 % усіх ІТ професіоналів в Україні, але лише 19 % із них працюють у технічних ролях¹⁶⁴. У результаті це сприяє існуванню непрямой дискримінації, що ускладнює її статистичне виявлення, проте негативно впливає на кар'єрне просування жінок.

Незважаючи на складність викликів, період воєнного стану також стимулював активізацію ініціатив, спрямованих на розвиток технічних компетенцій та підтримку жіночого лідерства. Це включає дискусії в рамках **Національного кластера кібербезпеки** та зростання видимості жінок у неформальних кіберволонтерських рухах та діяльність хактивісток. Ця активність, поряд з іншими зусиллями, ілюструє потенціал для подолання існуючих бар'єрів за умови забезпечення прозорих механізмів відбору. Проте в екстремальних умовах, де швидкість і гнучкість вирішують усе, відчайдушний пошук спеціалістів хоч і руйнує фрагменти деяких бар'єрів, та без системних ініціатив, спрямованих на трансформацію гендерних норм та уявлень про професійну роль жінок, такі "проблиски" інтеграції ризикують залишитися випадковими спалахами, а не фундаментом для сталих змін. Для досягнення довгострокового ефекту необхідне впровадження чітких дорожніх карт кар'єрного зростання, забезпечення рівного доступу до вузькопрофільних навчальних треків, створення спеціалізованих курсів та програм наставництва, орієнтованих на жінок, та прозорі механізми відбору на лідерські позиції, що враховують гендерну специфіку. Важливо також наголосити на загальному дефіциті публічної гендерно-дезагрегованої статистики та досліджень, які б детально висвітлювали специфіку становища та кар'єрних шляхів жінок, саме в українському секторі кіберзахисту в умовах війни, що суттєво ускладнює розробку та моніторинг ефективності відповідних політик та програм.

¹⁶⁴ DOU. (2024, March 7). *Як змінювалася кількість і роль жінок в українському ІТ за останнє десятиліття.*

Розділ 3. Жінки в українській кібербезпеці: голоси тих, які подолали перешкоди.

3.1. Результати глибинних інтерв'ю із жінками у кібербезпеці про їхній успішний і проблемний досвід перебування у цій сфері.

Семерникова Іуліанія, Сіманська Зоя, Коробкова Марія, Дудка Ольга, Краснопольська Тетяна, Гунда Дана, Глазкова Вікторія, Наталія Дітчук, Погоріла Єлізавета, Колісник Софія.

“Якщо ти боїшся чогось, то це не означає, що це не твоє. Це якраз таки означає, що це твоє. І що ти хочеш це робити. І хочеш робити це добре. Тому зневіра і страх – це нормально. І не треба боятися страху”
(Респондентка 3)

3.1.1. Методологія дослідження доступу жінок до сфери кібербезпеки в Україні

Дослідження доступу жінок до сфери кібербезпеки в Україні базується на інтерпретативній парадигмі, яка передбачає, що соціальна реальність є сконструйованою та багатогранною. Інтерпретативний підхід дозволяє дослідити суб'єктивний досвід жінок, які працюють у сфері кібербезпеки, розкрити їхні історії подолання перешкод та краще зрозуміти соціальні механізми включення та виключення в цій професійній сфері. Інтерпретативна парадигма надасть голос самим жінкам, дозволяючи дослідити їхні власні переживання та сприйняття. Дослідження базується на первинних даних, зібраних за допомогою напівструктурованих глибинних інтерв'ю з жінками, що працюють у сфері кібербезпеки в Україні. Напівструктурований формат передбачає гнучкість: респондентки можуть розширювати відповіді та надавати несподівані інсайти, що є цінним для розкриття соціального контексту їхніх кар'єрних шляхів.¹⁶⁵

Дослідження відповідає етичним принципам якісної соціології: нами була розроблена інформована згода, і перед інтерв'ю респондентки були ознайомлені з детальною інформацією про дослідження. Імена й інші персональні дані учасниць, за якими їх можна ідентифікувати, було анонімізовано: для позначення кожної респондентки в тексті використовується умовне позначення у вигляді номера (наприклад, Респондентка 1, Респондентка 2 тощо). Респондентки могли перервати інтерв'ю в будь-який момент, або відмовитися відповідати на певні питання; отримані дані використовувалися виключно в наукових цілях.

Вибірку було сформовано методом “снігової кулі”. Цей метод працює за принципом рекомендацій: жінки, які вже пройшли інтерв'ю, пропонують знайомих колег зі своєї професійної спільноти, які також можуть поділитися своїм досвідом. Метод “снігової кулі” є корисним для дослідження закритих або недостатньо

¹⁶⁵ Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data*. Sage.

вивчених сфер, де знайти респонденток на пряму складно.¹⁶⁶ Снігова куля почалась із заходу “SheCyber Hub”, який відбувався всередині лютого. На заході вдалось познайомились із жінками, що працюють у сфері кібербезпеки, та запросили їх долучитись до участі в інтерв’ю. У кінці інтерв’ю учасниць просили порекомендувати їхніх знайомих жінок зі сфери кібербезпеки, аби запросити їх взяти участь у дослідженні. Також підтримувався зв’язок з заступником декану Факультету Інформатики в НаУКМА Трохимом Бабичем, що надавав контакти знайомих йому жінок у сфері кібербезпеки. Аби забезпечити широкий спектр думок та можливість виявити закономірності у викликах та можливостях жінок у цій сфері, кількість учасниць становить 11 осіб. Основними ознаками потрапляння у вибірку був досвід роботи у галузі кібербезпеки, жіноча стать. Зведену інформацію про респонденток наведено у *Таблиці 3.1.1.1.*

Таблиця 3.1.1.1. Респондентки дослідження становища жінок у кібербезпеці.

Респондентка	Компанія/сфера	Посада	Досвід
Респондентка №1	ІТ-компанія	СОК-аналітиkinя	Пів року
Респондентка №2	Консалтингова компанія	Security Analytic	Більше року
Респондентка №3	Банк	Адміністративна (конфіденційно)	1 рік
Респондентка №4	ІТ-компанія	-	3 роки
Респондентка №5	Державна установа	Аналітиkinя	5 років
Респондентка №6	ІТ-компанія	Lead security engineer, director	5 років
Респондентка №7	Компанія у сфері кібербезпеки	Infrastructure security, devsecops, менторка в vona tech community	Близько року
Респондентка №8	Консалтингова компанія	Спеціаліст з GRC (Governance, Risk, and Compliance)	Більше року
Респондентка №9	Банк	Провідний	Пів року

¹⁶⁶ Жерьобкіна, Т., Кабанець, Ю., Куделя, М., Ломоносова, Н., Назаренко, Ю., Слободян, О., & Філіпчук, Л. (2021). *Досвід Cedos: соціальні дослідження для суспільних трансформацій*, сс. 76-77. Київ: Аналітичний центр Cedos.

		інженер відділу реагування на кіберінциденти	
Респондентка №10	Компанія у сфері кібербезпеки	Security engineer	5 років
Респондентка №11	IT-компанія	PR-менеджер з хорошим знанням галузі кібербезпеки	3 роки

Польовий етап тривав з середини лютого до початку травня 2025 року. Було надіслано 20 запитів з запрошенням щодо участі. Розмір вибірки зумовлений чутливістю теми та високим рівнем навантаженості потенційних респонденток, що вплинуло на кількість осіб, які погодились взяти участь.

В основі дослідження лежать наступні питання, які визначають його фокус:

1. Яких викликів зазнають жінки у сфері кібербезпеки та як вони справляються з ними?
2. Як жінки оцінюють свій професійний досвід та сприйняття з боку колег і суспільства?
3. Які умови, на думку респонденток, сприяють або перешкоджають їхньому професійному розвитку?

Гайд інтерв'ю, наявний у Додатку А, має напівструктурований формат, що дає респонденткам змогу вільно висловлюватися. Він складається з 5 блоків. Вступний блок містить пояснення мети дослідження, інформовану згоду та знайомство з форматом розмови. Перший блок охоплює кар'єрний шлях: освіту, початковий досвід та підтримку. Другий блок стосується робочого досвіду, включаючи умови праці, рівність у компанії та професійні спільноти. Третій блок фокусується на перешкодах: гендерні упередження, дискримінації та їхньому впливі на кар'єру. Четвертий досліджує суспільне сприйняття жінок у технічних сферах та стереотипи. У фінальному блоці респондентки діляться спостереженнями, дають поради та пропонують зміни в галузі, а також можуть додати власні думки. Загалом кожен блок допомагає розкрити основне питання блоку — тобто його тему.

Аналіз даних проведений у програмі Word та базується на тематичному аналізі. Було обрано саме тематичний аналіз, адже цей метод є більш гнучким та підходить під нашу теоретичну парадигму. Також цей метод аналізу краще передає думки й позиції респонденток без упереджень нас як дослідників. Обрання цього методу також зумовлено величиною дослідницької групи — кодування не доречно використовувати, адже воно зазнало б впливу нашої позиційності як дослідниць. Аналіз даних відбувався методом дедукції — шлях від найбільшого до найменшого. Після транскрибування інтерв'ю тексти проходять першу стадію — виділяються основні теми, що об'єднують усі транскрипти. Ми виділили декілька основних тематик: перешкоди, успіхи, ставлення (оточуючих, близьких, колег, в галузі), рекомендації для покращення становища жінок в сфері кібербезпеки. Далі були

виділені окремі значущі фрагменти тексту та позначені відповідними кольорами та мітками, відповідно до кожної тематики. На останньому етапі була здійснена інтерпретація результатів, що допомогло виявити загальні закономірності та специфічні особливості досвіду жінок у кібербезпеці.¹⁶⁷

3.1.2. Суспільне сприйняття жінок в кібербезпеці

“Це, скоріше, такий загальний міф, що дівчата йдуть в ІТ, щоб знайти собі заможного хлопця чи чоловіка” (Респондентка 7).

Під час початку і протягом роботи в кібербезпеці респондентки стикалися з різним ставленням до вибору професії від оточення, близьких та колег. Це може впливати на бажання продовжувати діяльність у кібербезпеці як негативно, так і позитивно. Тому ставлення – важливий аспект, який потрібно досліджувати в контексті досвіду жінок перебування в кібербезпеці. З метою вивчення цього аспекту було розроблено блок 3 запитань в гайді (*Додаток А*).

Респондентки зазначали, що жінки стикаються з **об’єктивізацією та недоречними пропозиціями**, що можуть повністю знецінювати їхню професійну діяльність та знання. Їм можуть пропонувати способи заробітку, що передбачають фільмування або показ повністю чи частково свого оголеного тіла, аргументуючи це “легкою роботою та хорошим заробітком”.

“От якось, одним прекрасним днем мені написав мій одногрупник. Хотів поцікавитись, як справи, там все таке. Я кажу: "все добре, я влаштувалася за фахом, в банк". Такий: "А, круто! Не хочеш спробувати отут в приложусі, коротше, танцюєш і тобі донатять. От в купальнику потанцюєш і заробляєш” (Респондентка 3).

“Або навіть, оце, що я розповідала, що я працюю вже. І мені кажуть: "а може, краще все-таки ОнліФанс?”” (Респондентка 3)

Окрім цього, від респонденток часто звучало, що їхнє оточення могло приписувати жінкам в кібербезпеці вибір професії через **бажання знайти собі чоловіка**, щоб жити за його кошти. Така думка від різних людей в оточенні може бути пояснена з кількох причин: 1) жінка, що працює в такій стереотипно “чоловічій” сфері може сприйматися як виняток, тож її мотивація піддається сумнівам та інтерпретується через призму більш “традиційних жіночих цілей”, таких як пошук партнера; 2) такі твердження можуть свідчити про нерозуміння або навіть свідоме знецінення професійних інтересів, здібностей.

“Кожна твоя відповідь аналізується через призму цих стереотипів, що жінки приходять в цю професію, щоб знайти хлопця айтішника і жити за його рахунок” (Респондентка 4).

¹⁶⁷ Willig, C., & Rogers, W. (2017). The SAGE Handbook of qualitative research in psychology. (Vols. 1-0). SAGE Publications Ltd, <https://doi.org/10.4135/9781526405555>

“Була одна дівчинка, яка була прямо впевнена в тому, що я пішла на технічну спеціальність для того, щоб знайти собі хорошого залицяльника” (Респондентка 8).

Стереотипні уявлення про причини вибору жінками ІТ-сфери поширені й серед їхніх рідних. Як зазначали респондентки, близькі іноді приписували їхню мотивацію зовнішнім чинникам, таким як прагнення до фінансової вигоди (“швидкі гроші”) або, як було вже наведено раніше, через бажання знайти партнера у переважно чоловічому колективі (“пошук чоловіка”), ігноруючи фаховий інтерес.

“Інше питання, що люди здебільшого такі: “О, ти, певно, що пішла туди, що там є багато грошей, дають, чи, можливо, ти туди пішла, тому що там багато хлопців?”” (Респондентка 9).

Крім цього, серед близьких респонденток, особливо старшого покоління (дідусів, бабусь, батьків), поширене уявлення про кібербезпеку як “не жіночу” професію. Навіть за відсутності відкритих сімейних суперечок, жінки часто відзначають тривале нерозуміння та певну відстороненість рідних щодо їхньої роботи. Позитивній динаміці у зміні ставлення (від негативного до нейтрального/позитивного) сприяли переважно економічний аспект роботи та видима професійна реалізація й зацікавленість самих жінок.

“Вона [мама] не розуміла, чому я сиджу по 8 годин і звідки в мене з'являються гроші” (Респондентка 8).

“Мої друзі вже розуміють... вони просто щасливі, що робота безпечна і вона оплачується” (Респондентка 2).

Крім цього, декілька респонденток зазначали, що, навіть попри збільшення жінок у кібербезпеці, присутні певні **гендерні стереотипи** серед колег та керівництва – жінок продовжують **сприймати як менш компетентних у технічних аспектах**, а їхні знання – ставлять під сумнів.

“Однак, конкретно в цій першій [компанії], я просто бачу, що до нас, до дівчат, ставились якось більш зверхньо... якщо жінка скаже, що вона чогось не знає, то до неї будуть таке ставлення: “А, ну, я ж знав, ти ж жінка, жінки не знають” (Респондентка 4).

“Але я відчуваю, що якби мої знайомі дівчата відповіли, що вони працюють девелоперами, розробниками, то до них поставились так: “Ну не такий ти вже крутий розробник...Ну ти айтішник, але наполовину тільки, бо ти жінка”” (Респондентка 4)

Наслідки гендерних стереотипів системно ускладнюють шлях жінок у кібербезпеці. Це проявляється як у неявних упередженнях на роботі – наприклад, різному рівні довіри та “праві на незнання” для чоловіків і жінок, – так і в загальному тиску середовища. Існують **подвійні стандарти** для жінок і чоловіків у сфері

кібербезпеки. Це проявляється у тому, жінки змушені докладати більше зусиль для доведення своєї компетентності, тоді як чоловіки можуть обирати цю сферу через її “престижність”. Жінкам же доводиться активно боротися зі **стереотипами** за своє визнання, як показують наступні цитати.

“Я просто відчувала таке ставлення, наче якщо чоловік скаже, що він щось не знає, що йому треба більше інформації покопати, і до нього буде нормальне ставлення, бо всі чогось не знають. А якщо я казала, що я чогось не знаю, то до мене було таке ставлення: “Ну ти ж жінка, я і не очікував такого” (Респондентка 4).

“І якщо брати хлопців, то от вони, приходять сюди просто тому, що кібербезпека звучить круто, і все. Дівчатам, мені здається треба пробиратись через цей тиск, навіть в університеті, коли вони навчаються, бо їх оцінюють за стереотипами старими” (Респондентка 6).

Одна з респонденток також зазначила про поширення **упередженого ставлення серед колег старшого покоління** до жінок у сфері. Вона зазначала, що в державних структурах ситуація ставлення до молодих жінок в ІТ гірша, аніж в приватних компаніях. Це яскравий приклад **ейджизму** та **сексизму**.

“Якщо говорити про державний сектор, там ситуація гірша. Чоловіки за 50 років, які працюють у державних органах, не сприймають серйозно ні молодих спеціалістів, ні тим паче жінок” (Респондентка 6).

“Від чоловіків якихось 40+, відчувається, що вони намагаються у мене спитати: “Ти точно це розумієш? Ти точно знаєш, про що ми зараз розмовляємо?”” (Респондентка 4)

Крім того, жінки стикалися з **гендерно стереотипним ставленням** не лише від колег на вищих чи рівних посадах, а від тих, хто займав нижчі позиції. Компетентність вкотре піддавалася сумнівам не лише за **статевою ознакою**, а і за **віковою**:

“Ну чула я таке типу – “а це не занадто складно для дівчини?” чи “а ти знаєш що таке інтернет?” або “а ти знаєш що таке апі?”. Ну звичайно це такі питання, які я чула не так часто, але такі були” (Респондентка 5)

“Не завжди люди були налаштовані дуже так доброзичливо, всі завжди були такі: “О боже, це якась там молода нова спеціалістка, та вона там нічого не знає, хто вона взагалі така, звідки вона прийшла”” (Респондентка 9)

Також варто зазначити, що респондентки стикалися із **стереотипним ставленням** щодо вибору професії та перебування на певній посаді. Досвід ставлення, про який зазначила одна з респонденток, виходить за межі суто професійної дискримінації та охоплює також випадки приниження, що ґрунтується

виключно на гендерній приналежності. Це підкреслює глибокий рівень вкоріненості **сексистських упереджень** у робочому середовищі.

“Було ще щось, що якимось я там знімала светр, буквально отак, коли спочатку витягаєш руки з рукавів і просто знімаєш через голову. Тобто, без якихось там, як в кліпах, типу, така спочатку... [Колега каже]: “О, ХХХ стриптиз показує” (Респондентка 3).

Гендерні стереотипи не лише негативно впливали на ставлення інших колег до жінок, які працювали у сфері кібербезпеки – вони також заважали професійному саморозвитку респонденток. І що найважливіше, впливали на заробітну плату – зокрема, одна респондентка зазначила про те, що деяким жінкам не хотіли підіймати грошову винагороду через наявність у них партнерів та їхніх коштів.

“Моїй колезі на перегляді зарплати сказали: “Навіщо тобі більше грошей? У тебе ж хлопець є” (Респондентка 6).

Якщо ж відзначати **про ставлення до жінок та чоловіків у галузі** – воно також різниться. Одна з респонденток наголосила на відмінності у ставленні клієнтів до чоловіків та жінок, які надають послуги аудиту та консалтингу в межах її компанії. Вона зазначала, що клієнти частіше висловлюють незадоволення результатами роботи саме жінкам, ніж їхнім колегам-чоловікам, що свідчить про **гендерно стереотипне ставлення** деяких клієнтів:

“Буває, що коли спілкуємося із зовнішніми клієнтами, коментарі бувають такі, які явно були б іншими, якби я була чоловіком. [...] Усі йдуть, залишаюся тільки я, і хтось із клієнтів починає казати, що “це було жахливо”, що “ми змарнували час багатьох людей”. Хоча до цього всі були задоволені й ніхто на нараді нічого подібного не казав” (Респондентка 6).

До того ж одна респондентка зазначала, що **гендерні упередження** щодо жінок в ІТ проявляються навіть у публічному онлайн-просторі:

“На сайті Dou.ua дуже часто під постами про жінок в ІТ з'являються жахливі коментарі. Їх там майже не модерує адміністрація” (Респондентка 6).

Підсумовуючи, під час роботи у сфері кібербезпеки жінки стикаються з певним гендерно-стереотипним ставленням: зокрема, з сумнівами щодо компетентності, професійності чи навіть мотивації працювати на посаді. Воно спостерігається як у галузі, так і з боку оточення: друзів, сім'ї, колег, керівництва тощо. Таке ставлення яскраво показує, наскільки глибоко вкорінені сексистські упередження щодо роботи жінок у цій сфері.

3.1.3. Перешкоди в роботі в сфері кібербезпеки у жінок

“Тобі потрібно ще доказати, що ти щось вмієш” (Респондентка 8)

Під час працевлаштування та роботи у сфері кібербезпеки можуть виникнути ситуації, що заважають жінкам у їхній професійній діяльності – певні бар'єри. Це можуть бути коментарі чи конкретні дії від колег, керівництва чи клієнтів, що можуть ставити під сумнів професійність жінок, насміхатись над ними або просто не сприймати їх серйозно. Це може не тільки заважати жінкам входити у сферу ІТ чи кібербезпеки, а і продовжувати працювати в цій галузі. Такі перешкоди для кар'єрного розвитку, наприклад, включають **скляну стелю** та **скляні стіни**.

На етапі перших співбесід частина респонденток стикалися з підвищеними вимогами щодо їхніх технічних знань, що може створювати початкове відчуття власної некомпетентності. Вхід до технічної сфери для частини жінок супроводжується інтенсивним самонавчанням і подекуди — інформаційною ізоляцією, коли базові поняття не пояснюються, а вважаються нормою за замовчуванням.

“Ще на співбесіди походила. Мені викатали цілий список, що мені треба знати. Я просто записувала. І я через певний час зрозуміла, що я деякі речі настільки вперше чула, що я неправильно записала” (Респондентка 3).

Окрім високих вимог щодо технічної підготовки, значним бар'єром учасниці інтерв'ю відзначали непрофесійну поведінку інтерв'юерів, яка може свідчити про **гендерні упередження** щодо професійності жінок у кібербезпеці:

“Але були випадки, коли під час співбесід співрозмовники поводитися непрофесійно. Наприклад, хлопці розвалювалися на стільці, розставляли ноги й починали розмову зі слів “як справи?” (Респондентка 6).

Частина респонденток висловлювала впевненість у тому, що саме їхня стать стала чинником відмови у працевлаштуванні. Цей досвід є повторюваним: багаторазові відмови створюють у жінок переконання, що в цій сфері поширена недовіра до їхньої професійної компетентності. Одна з респонденток наголосила, що іноді **дискримінація є неформалізованою**, але очевидною для самої учасниці.

“Але ось, до речі, якраз під час пошуку були випадки, коли я чітко відчувала, що мене не хочуть брати просто тому, що я жінка” (Респондентка 7).

“Це був той момент, коли ти просто приходиш на дзвінок, ти бачиш людину, вона тобі каже буквально два слова і ти вже розумієш, що щоб ти не зробила, ти не пройшла, можна закривати коло. Таке було, мабуть, два рази за все моє життя” (Респондентка 7).

Водночас спостерігається і більш м'яка, але не менш проблемна форма гендерної диференціації — **патерналістське**, “пом'якшене” **ставлення**. Подібне ставлення знижує суб'єктність жінок і закріплює уявлення про їхню менш компетентну або менш серйозну роль у професійному полі. Замість повноцінної участі в технічному діалозі, жінка нерідко опиняється в позиції тієї, кого потрібно підтримати або пожаліти, що не відповідає її статусу рівноправної професіоналки.

“Насправді, як би це дивно не звучало, у більшості чоловіків, коли бачать дівчину, яка йде на кібербезпеку або в будь-яку технічну спеціальність, ставляться трошки легше. Мені так здалося” (Респондентка 8).

Після працевлаштування жінки часто змушені доводити свою компетентність значно ретельніше, ніж їхні колеги-чоловіки. Це свідчить про нерівномірний розподіл довіри в колективах, де чоловіки апоріорі сприймаються як більш компетентні.

“Я би сказала, що мені просто не вірили. Наприклад, мене постійно перевіряли. Я дуже боялась хоч щось сказати, щоб мені просто так повірили, і будь-яке моє слово не перевіряли по 20 разів. А чоловіків так не перевіряли” (Респондентка 4).

Особливо проблематичним є ставлення до жінок на керівних або наставницьких позиціях. Вік і гендер можуть стати підставами для заперечення авторитету, незалежно від об'єктивних фахових якостей.

“Той момент, коли мені видали інтернів. І інтерн попросив мене замінити, тому що він не вважав мене професіоналом, спеціалістом, якого він би слухав. Тому що, по-перше, я була молодша, по-друге, я була дівчина” (Респондентка 4).

“А деякі все ще вважають, що жінки не можуть працювати на серйозних посадах, особливо якщо це керівна посада, ну, з управлінням зв'язана” (Респондентка 8).

Крім того, **дискредитація жіночих досягнень** набуває форми присвоєння результатів жінок чоловіками собі. Такий досвід маргіналізує внесок жінок у професійний продукт і позбавляє їх визнання. Цей механізм часто залишається невидимим, адже формально дії колеги-чоловіків виглядають як “редагування” або “співпраця”.

“Ну тобто я написала круту політику, і просто прийшов мій бос, і просто її, розкритикував, просто її знищив. Ну, хоча він там не змінював досить багато, тобто, це була якась орфографія, але тіло цієї політики залишилось, але в майбутньому він казав всім, що це він написав цю політику, а не я” (P4).

Жінки у сфері кібербезпеки також стикаються з формами **латентного сексизму**, які маскуються під доброзичливість, але підсилюють уявлення про них як про непрофесійних суб'єктів. Такі звернення знецінюють професійні досягнення й фокусують увагу на гендері, а не на знаннях.

“На одній з попередніх робіт мені часто говорили “молодчинка”, що трохи дратувало. Моєму колезі Олексію так ніколи не казали” (Респондентка 6).

Деякі респондентки стикалися з **гендерно стереотипним ставленням**, що в подальшому вплинуло на їхню самооцінку та професійну спрямованість. Наприклад, *респондентка 4* розповідає про свій невдалий досвід в першій українській компанії, коли її роботу знецінювали.

“І після того, як я вийшла з цієї першої української компанії, я була абсолютно розбита, мені було дуже страшно йти на співбесіди будь-які” (Респондентка 4).

Хоч вона і мала досвід в іншій компанії до цього, її керівник жорстко контролював її роботу. Компанія складалась з 70% чоловіків і зазвичай вони працювали над проєктами і виступали з ними, тоді як респондентка залишалась в тіні. Її прирівнювали до інших працівників, що сприяло до її професійного вигорання. Також респондентка зазначила про **розрив в оплаті праці жінок та чоловіків** у її компанії, адже помітила, що зарплатня її друга-чоловіка була вища ніж її. Вона боялась після цього шукати іншу роботу, адже почувалась невпевнено і побоювалась такого ж ставлення.

“І мені навіть до недавнього часу було досить складно відновити в собі оцю впевненість, тому що мені було складно повірити, що на другій роботі до мене просто не прискіпуються. Тобто мені просто вірять, і я для когось спеціаліст. Мені було складно повернути це відчуття. Зараз вже нормально, я вже в собі впевнена, але так: ця перша робота була досить травматична для мене” (Респондентка 4).

Проте їй пощастило з наступним місцем працевлаштування, компанією, де до неї ставилися на рівні з іншими, що допомогло відновити її віру в себе. Подібний вплив страху і недовіри відчула на собі й *Респондентка 6*. На початку своєї кар'єри вона сумнівалась у здатності опанувати технічну професію. Постійне знецінення посилювало внутрішні сумніви та розвивало страх помилитися у роботі, що може суттєво гальмувати професійний розвиток.

“На початку кар'єри я навіть думала піти тестувальницею або бізнес-аналітикинею — через страх складнощів” (Респондентка 6).

Респондентка 6, працюючи в команді, яка займається аудитами й консалтингом, відмічає, що часто запам'ятовує імена тих, хто пише **сексистські коментарі** та дивиться, де вони працюють. Якщо потім компанії цих людей приходять із пропозиціями, вона відмовляє їм у співпраці, цитуючи вислови їхніх співробітників. Респондентка 6 акцентує увагу на відсутності реакції компаній на **сексизм**, що в подальшому сприяє його поширенню, адже ніхто не притягує співробітників до відповідальності за свої слова.

“Здебільшого компанії на це не реагують – максимум роблять зауваження своїм співробітникам, але не вживають серйозних заходів” (Респондентка 6).

Доцільно зробити висновок, що простежується систематичний **патерн упередженої поведінки** щодо жінок у кібербезпеці, який проявляється в сумнівах щодо професійності, недовірі, додатковому контролю, присвоєнні результатів і прихованій зверхності. Це може суттєво впливати на впевненість, самореалізацію та кар'єрні траєкторії жінок у галузі кібербезпеки та підтверджує потребу у висвітленні цієї теми, проведенні освітніх заходів на тему **гендерної дискримінації** на робочому місці та поширенні компаніями **антидискримінаційної політики**.

3.1.4. Персональні досягнення жінок в сфері кібербезпеки

Тобто [зараз] багато жінок і просто чоловіки будь-якого віку звикли до того, що з ними працюють жінки і вони постійно бачать, що досить багато жінок – професіонали.” (Респондентка 4)

Персональні досягнення важливі для професійного розвитку жінок в сфері ІТ. Респондентки зазначали, що досягнення стали результатом як особистої рішучості, так і підтримки з боку наставників. Багато респонденток зазначали важливість вміння подолати свої страхи та сумніви, що стало ключем до їхнього успіху. Наприклад, одна з респонденток згадує, як на початку її кар'єри було страшно на співбесіді та навіть на стажуванні, однак вона не дозволила страху зупинити себе.

“Коли мене кличуть на роботу, я кажу, ні, мені страшно, я там ніколи не була, але я все одно йду. Потім, ні, мені страшно, там, стажування, я боюсь, проте я йду. (Респондентка 1).

Крім того, респондентки підкреслюють важливість навчання та прагнення до технічної майстерності. Наприклад, одна з респонденток зазначила, що для того, щоб перейти в кібербезпеку, вона чітко спланувала свій кар'єрний шлях і була готова до змін.

“Я спланувала свій кар'єрний шлях і просто чекала моменту, коли буду достатньо гарною технічною спеціалісткою, щоб перейти в кібербезпеку.” (Респондентка 6)

Для деяких респонденток важливим кроком стало отримання сертифікацій та додаткових курсів. Наприклад, *респондентка 2* активно проходила курси від Google та IBM, що допомогло їй здобути необхідні технічні навички.

“Я проходила курси на курсері, пов'язані з кібербезпекою від Google. Також кілька курсів від IBM, які були в вільному доступі. А також курси, як то кажуть, злиті, які, наприклад, це курси були по підготовці для отримання сертифікату CompTIA Security Plus та інші подібні сертифікати” (Респондентка 2)

Отже, персональний досвід подолання певних перешкод жінками полягає не тільки у розв'язуванні професійних проблем, а й постійної боротьби з власними сумнівами та розвитку власних навичок.

3.1.5. Позитивні зрушення у практиках залучення та підтримки жінок в сфері кібербезпеки в Україні

“Хоча технічних спеціалісток поки менше, ніж нетехнічних, але їх стає більше, і це радує.” (Респондентка 6)

Водночас попри наведені вище виклики та труднощі, з якими стикалися та продовжують стикатися жінки під час роботи у сфері кібербезпеки, деякі респондентки все ж відмітили, що протягом останнього часу можна помітити певні **позитивні зрушення**. Зокрема, зменшення дискримінації, гендерно стереотипного ставлення чи не розуміння, а навпаки – підвищення видимості жінок у галузі, збільшення підтримки та прийняття.

“Уже легше, вже набагато легше в Україні. Мені здається, вже немає такої дискримінації, як було раніше. В ІТ мені здається, саме серед роботодавців, жінок сприймають так само, як і чоловіків” (Респондентка 2).

Однією з важливих тенденцій також є збільшення кількості жінок у навчальних групах та на робочих місцях. Як зазначають респондентки, у багатьох навчальних групах вже спостерігається збалансоване співвідношення жінок і чоловіків.

“У нас те саме 50 на 50. Тобто... І у нас... У нас дівчата... У нас топ-групи – це тільки дівчата, напевно.” (Респондентка 1) (щодо балансу чоловіків і жінок у навчальній групі).

“Тепер молоді люди цілеспрямовано йдуть у кібербезпеку, а раніше приходили туди випадково через інтерес і самоосвіту” (Респондентка 6).

На думку певних опитаних респонденток, покращене ставлення до жінок у цій сфері може бути пов'язане, зокрема, з **дефіцитом кадрів у цій галузі**. У зв'язку з війною в Україні, частина чоловіків вступають до війська, що зумовлює звільнення робочих місць у компаніях. Ці вакансії більше почали займати жінки, що, відповідно, сприяє зміні установок щодо професійності жінок у галузі:

“На даний момент таким чином складаються обставини, що позитивно, тому що багато чоловік йдуть на фронт, багато чоловік мобілізують, і це підіймається на кожній конференції, на якій я була [...], що жінок треба більше брати в цю сферу, тому що жінки, в принципі, дуже і дуже добре розуміються на кібербезпеці, якщо їх в це занурити” (Респондентка 1).

Жінки все більше інтегруються в цю галузь, зокрема, в освітні програми, що позитивно впливає на їхнє становище в професії. Крім того, все більше компаній

починають брати на роботу більше жінок, розширюючи можливості для кар'єрного зростання.

“Так, я дійсно помічаю позитивні зміни у ставленні до жінок у сфері кібербезпеки. З кожним роком все більше компаній відкривають двері для фахівчинь. Більше підтримки, менше стереотипів і більше довіри до професіоналізму незалежно від статі” (Респондентка 5).

Ще однією важливою зміною є **зменшення гендерної дискримінації** в деяких компаніях. Респондентки зауважують, що в організаціях спостерігається зниження **стереотипного ставлення** до жінок, і вони почуваються більш рівними з чоловіками в плані професійних можливостей.

“..зараз дуже багато жінок кібербезпеки ціниться, і якимось uplifting для того, щоб ці прогалини в кадровій системі якимось згладжувати” (Респондентка 1).

“Я проходила співбесіди, також в банки та інші організації, то, в принципі, особливого ставлення, що я жінка, напевно, не було” (Респондентка 1).

Це також підтверджується ставленням колег до жінок, де більшість респонденток не відчують дискримінації чи неповаги через свою стать, і навіть вказують на більшу лояльність серед жінок-професіоналів.

“Та ні, я б, напевно, сказала, що мені навіть трошки легше спілкуватися з, наприклад, клієнтами. Тому що більшість цих спілкувань було з менеджером або відповідальними особами. Наприклад, це те чи інший процес. Там було більше жінок. Тобто вони, наче, більш лояльніше ставилися до мене, чим до мого колеги, чоловіка” (Респондентка 2).

Також варто зазначити, що жіночі команди в компаніях та навчальних групах стають все більш видимими, що позитивно впливає на мотивацію інших жінок долучатися до цієї професії. Загалом, зміни в галузі вказують на покращення рівних можливостей для жінок і чоловіків у кібербезпеці:

“Завдяки зусиллям нашої влади, керівників вищого рівня, локальних керівників, йде тема просування жінок у сфері кібербезпеки.” (Респондентка 9)

“Я також бачу це по своїй компанії: у нас тепер дуже багато резюме від жінок” (Респондентка 6)

Отже, позитивні досягнення сфери кібербезпеці щодо становища жінок в цій сфері зводяться до збільшення кількості жінок у професії, зниження стереотипів щодо їхньої ролі в цій сфері та розширення можливостей для кар'єрного розвитку і підтримки з боку організацій та колег.

3.2 Результати експертних інтерв'ю щодо успіхів і викликів залучення жінок у сферу кібербезпеки в часи російсько-української війни.

Квят Софія, Гресь Анна, Селянінова Євгенія, Висовень Карина, Сташко Вероніка, Балабаш Анастасія, Овсюченко Олександр, Піменов Станіслав, Хлівна Єлизавета, Васютинська Анастасія

3.2.1 Методологічні основи опитування щодо успіхів і викликів доступу жінок до сфери кібербезпеки в Україні

Для дослідження успіхів та викликів доступу жінок до сфери кібербезпеки було використано інтерпретативну парадигму. Вибір цього підходу зумовлений його здатністю розпізнання суті соціальних явищ, що уможлиблює подальше формування гіпотез¹⁶⁸. А відповідно, дозволить поглибити знання про досліджувані явища у майбутньому.

За Е. Маккобі (1954)¹⁶⁹, інтерв'ю це – “вербальний обмін віч-на-віч, під час якого одна особа, інтерв'юер, намагається отримати інформацію, висловлення думок чи переконань від іншої особи, чи осіб”. Первинними соціологічними даними якісного дослідження є напівструктуровані експертні інтерв'ю. Вони дають змогу отримати комплексне бачення проблеми, що виходить за межі індивідуальної компетенції дослідни(ці)ка. У дослідженні застосовано дослідницьку (аналітичну) триангуляцію, що передбачає залучення кількох аналітиків до обробки одних і тих самих даних¹⁷⁰. Це дало змогу мінімізувати суб'єктивність в інтерпретації зібраних даних. Водночас це підвищило валідність результатів, достовірність висновків та дозволило глибше проаналізувати досліджуване явище через залучення різних перспектив і експертних оцінок¹⁷¹.

Пошук респондент(ок)ів здійснювався за допомогою пошукової системи Google, а також таких соціальних мереж, як Instagram, Facebook, LinkedIn. Також було застосовано метод “снігової кулі”, після збору та обробки рекомендацій вже опитаних експерт(ок)ів. Запрошення до участі отримали 24 респондент(к)и.

Фінальну вибірку дослідження склали 14 респондент(ок)ів (5 чоловіків та 9 жінок), що залучені до сфери кібербезпеки в Україні та погодилися на участь в інтерв'ю. Середній показник стажу у сфері кібербезпеки для всіх експерт(ок)ів становить 8,4 роки. Формальною ознакою вибірки була робота у сфері кібербезпеки (в державному чи приватному секторі) мінімум 1 рік. Лише 5 з 9 респонденток мають вищу освіту за спеціальністю “Кібербезпека”, а серед респондентів жоден не має вищої освіти за цим напрямком. Респондент(к)и, які не навчалися за цією спеціальністю, здобували знання протягом навчання на дотичних до сфери кібербезпеки напрямках (комп'ютерні науки, інженерія, право), на спеціалізованих

¹⁶⁸ Костенко, Н., & Скокова, Л. (2009). *Якісні дослідження в соціологічних практиках* (С. 24). Інститут соціології НАН України. https://i-soc.com.ua/assets/files/library/g_s_ok.pdf

¹⁶⁹ Массобу, Е. Е., & Массобу, Н. (1954). The Interview: A Tool of Social Science. In G. Lindzey (Ed.), *Handbook of Social Psychology* (Vol. 1, pp. 499). Reading, MA: Addison-Wesley.

¹⁷⁰ Бондар, В. С. (2002). Комбінація підходів щодо аналізу даних у якісному дослідженні. *Соціологія: Теорія, Методи, Маркетинг*, (1), 368–377.

¹⁷¹ Okoko, J. M., Tunison, S., & Walker, K. D. (2023). Introduction to a Variety of Qualitative Research Methods. In *Varieties of Qualitative Research Methods, Selected Contextual Perspectives* (pp. 1–8). Springer. https://doi.org/10.1007/978-3-031-04394-9_1

курсах чи безпосередньо на робочому місці. Критерієм експертності були знання у сфері рівних прав і можливостей, залучення жінок у сферу кібербезпеки, робота у напрямку формування спроможності жінок у сфері кібербезпеки тощо. Середня тривалість інтерв'ю – 1 година. Період проведення інтерв'ю: від 21 березня до 1 квітня 2025 року. Загальна характеристика респондент(ок)ів наведена в *Таблиці 3.2.1.1.*

Таблиця 3.2.1.1. Загальна характеристика експерт(ок)ів щодо успіхів і викликів залучення жінок у сферу кібербезпеки в часи російсько-української війни

№	Стать	Місце роботи	Стаж (роки)	Експертне знання з теми доступу жінок до кібербезпеки
Респондентка №1	жінка	громадська організація	6	глибоке технічне розуміння безпекових процесів та активна участь в ІТ-спільнотах для жінок
Респондентка №2	жінка	ІТ-компанія	7	практичний досвід в ІТ та громадська діяльність, зокрема щодо рівності
Респондент №3	чоловік	приватна ІТ-компанія у сфері захисту даних	3,5	дотичний досвід у сфері ІТ, без вираженої спеціалізації на питаннях рівності чи жіночої участі
Респондент №4	чоловік	приватна ІТ-компанія	1,5	має загальне розуміння тематики та потенціал до залучення в гендерно чутливі ініціативи
Респондент №5	чоловік	розробник в сфері ІТ	5	досвід релевантний для міжсекторальної співпраці
Респондентка №6	жінка	освітянка в кібербезпеці України, співзасновниця та проєктна координаторка у ГО, що підтримує жінок в кібербезпеці	25	лідерка стратегічних ініціатив з розвитку жіночого лідерства,

				включаючи цифрову сферу
Респондент №7	чоловік	освітянин в кібербезпеці в Україні	15	має загальне розуміння тематики та потенціал до залучення в гендерно чутливі ініціативи
Респондентка №8	жінка	аналітична компанія	20	комплексне стратегічне бачення, спрямоване на підсилення ролі жінок через аналітику та комунікацію
Респондентка №9	жінка	державна установа	3,5	має загальне розуміння тематики та потенціал до залучення в гендерно чутливі ініціативи
Респондент №10	чоловік	державна установа	10	має загальне розуміння тематики та потенціал до залучення в гендерно чутливі ініціативи
Респондентка №11	жінка	засновниця консалтингової компанії та проєктів/ініціатив у сфері кібербезпеки	8	юристка та експертка з кібербезпеки, розробляє політики та навчальні програми
Респондентка №12	жінка	адміністраторка відділу інформаційної безпеки	9 місяців на конкретній посаді	має загальне розуміння тематики та потенціал до залучення в гендерно чутливі ініціативи
Респондентка №13	жінка	співзасновниця ГО у сфері жіночого лідерства	3	лідерка стратегічних ініціатив з розвитку жіночого лідерства, включаючи

				цифрову сферу
Респондентка №14	жінка	ІТ-компанія	7	знання про керування технічними проєктами з можливістю впливу на залучення жінок в ІТ-сферу

Така кількість респондент(ок)ів може вважатися достатньою для аналізу. Відповіді респондент(ок)ів повторювалися, тому ми можемо вважати, що інформація досягла точки насичення.

Перед початком інтерв'ю, було отримано згоду на запис розмови. Респондент(к)и були ознайомлені з інформованою згодою, що включала інформацію про мету дослідження, умови конфіденційності та право відмовитися від участі в будь-який момент. З етичних міркувань, отримані в ході дослідження дані деперсоналізовано.

Гайд побудовано на основі попередньо підготовлених тематичних блоків, що забезпечувало структурованість дослідження, послідовність збору даних і можливість порівняти відповіді кожним інтерв'юером та інтерв'юеркою (*Додаток Б*).

Перший блок присвячено знайомству з експертом чи експерткою, задля уточнення раніше зібраної інформації про посаду, стаж у сфері кібербезпеки та освіти. Також зібрано інформацію щодо мотивації щодо роботи у сфері.

Другий блок з'ясовує думку експерт(ок)ів, щодо представленості жінок у сфері кібербезпеки в Україні. Респондент(ок)ів запитували про гендерну диспропорцію у сфері, представленість жінок на робочому місці та як на неї впливав початок повномасштабного російського вторгнення.

Третій блок гайду присвячено викликам жінок у сфері кібербезпеки в Україні. Питання блоку були зосереджені на тому, щоб дізнатися про вертикальна чи горизонтальна гендерні сегрегації, чи страждають жінки від гендерних упереджень, дискримінації чи сексуальних домагань на робочому місці.

Четвертий блок було присвячено успіхам доступу жінок до сфери кібербезпеки в Україні. Тут йшлося про підтримку жінок на організаційному та державному рівні. Крім того, з'ясовано чи відомі експерт(к)ам жіночі рольові моделі та їх успіхи у сфері кібербезпеки.

Метою останнього, п'ятого блоку були рекомендації фахівців та фахівчинь для залучення більшої кількості жінок у сферу кібербезпеки в Україні.

Для транскрибування інтерв'ю використовувався ШІ транскриптор Restream. Після транскрибування інтерв'юер(к)и вчитали транскрипти для точного відтворення інформації та перевірки помилок. Для обробки даних отриманих в результаті напівструктурованих експертних інтерв'ю було використано метод

тематичного аналізу¹⁷². Цей метод був обраний через можливість фокусуватися як на широких патернах у наявних даних, так і на аналізі окремих аспектів, включено з явними та латентними смислами висловлювань респондент(ок)ів. На етапі первинного кодування виділялися думки респондент(ок)ів, що відповідали змісту питань блоків інтерв'ю, після чого вони були згруповані тематично. Після цього, закодований текст було переглянуто та цитати були розподілені за відповідними темами. Це надало змогу виявити та структурувати ключові теми з відповідей респондент(ок)ів.

Таким чином, після проведення усіх етапів збору та обробки інформації було з'ясовано успіхи та виклики залучення жінок у сферу кібербезпеки в часи російсько-української війни.

За результатами аналізу, серед викликів у доступі жінок до сфери кібербезпеки в Україні респондент(к)и згадали низку критичних моментів, зокрема: прояви горизонтальної та вертикальної гендерної сегрегації, гендерні стереотипи та упередження щодо жінок, брак ініціатив та підтримки зі сторони держави та суспільства, а також прояви сексуальних домагань.

3.2.2. Виклики у доступі жінок до сфери кібербезпеки в Україні: гендерні стереотипи і упередження

“Так, помічав, і вказував, що сексизм – це небажано або недопустима річ, тому намагався це припиняти.” (Респондент 10)

Важливим викликом доступності сфери кібербезпеки для жінок є **гендерні стереотипи і упередження**. Вони підтримують гендерну поляризацію і переконання, що чоловіки та жінки однорідні (гомогенні) всередині групи¹⁷³. У сфері освіти та праці, вони формують уявлення про кібербезпеку, як про "чоловічу" галузь, знижують самооцінку та впевненість потенційних спеціалісток і впливають на рішення роботодавців щодо найму та кар'єрного просування. Не всі респондентки стикалися з проявами сексизму у своєму колективі, проте більшість все ж мають такий досвід або знають про такі випадки. Наприклад, Респондентка 8 вказує, що *“Жінкам потрібно доводити свою компетентність”*, що вказує на певне поблажливе та/або несерйозне ставлення до спроможності жінки на робочому місці. Окрім того, жінки наголосили, що кількість упереджень більша саме в державному секторі, порівняно з приватним:

“Коли я комунікувала з державними органами, дуже часто чула оцю фразу: “Ой, ти дівчина, що ти там... Що ти нам тут розкажеш?” ... Або: “Вона – жінка, нащо їй працювати над якимись оборонними об'єктами або об'єктами критичної інфраструктури?” (Респондентка 11).

¹⁷² Braun, V., & Clarke, V. (2012). Thematic analysis. In *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological*. (pp. 57–71). American Psychological Association. <https://doi.org/10.1037/13620-004>

¹⁷³ Маєрчик, М. (2017). *Гендер для медій: підручник із гендерної теорії для журналістики та інших соціокультурних спеціальностей* (3 видання, випр. і доп.). К.: Критика. (С. 44)

Варто зазначити, що респондентки зауважили, що їм доводилося *“тяжко (понаднормово) працювати, щоб у їхню компетенцію повірили, щоб доказати знання у чоловічому середовищі.”* (Респондентка 13). Також респондентки зазначають про поширене традиційне уявлення про сферу кібербезпеки, як маскулінну та/або психологічну напругу, спричинену цим уявленням:

“У Міністерстві Оборони у мене взагалі був кейс, що я вперше в житті плакала, бо організовувала захід з військовими. Я бачила пряму неповагу. Якщо я приходжу з керівником, з керівником говорять, коли я сиджу за столом переговорів і висловлюю свою думку, як зробити щось краще, чоловіки просто показово робили вигляд, що мене немає, типу не слухали, і говорили лише з моїм керівником.” (Респондентка 13).

Серед чоловіків лише 2 з 5 респондентів розповіли про сексизм щодо жінок на своєму робочому місці. Це свідчить про низький рівень обізнаності, розуміння та/або визнання проблеми сексизму серед чоловіків, навіть якщо такі випадки мають місце:

“Так. Це класична патріархальна нісенітниця . Особливо мені дуже подобається коли, знаєте, коли на їх типу статі ще й наголошують. Що, тіпа, така розумна, а ще й дівчина. І мене завжди такі постановки питань просто повільно вибивають. Особливо, коли ця людина 5 хвилин тому казала “Я не сексист”. От дивись, “От є, наприклад, ХХХ, от вона розумна, а ще й дівчина”, а потім думаєш “Ну ти не сексист, абсолютно”. Це воно несвідоме. Це не те щоб надто щось свідоме за якоюсь ознакою, просто такий побутовий сексизм.” (Респондент 7).

Сексизм зосереджує увагу на фізичних, інтелектуальних, творчих та інших перевагах однієї частини людей (чоловіків) над іншими (жінками)¹⁷⁴. Відповіді респондент(ок)ів свідчать про поширеність цього явища та підтримку традиційного стереотипного розподілу гендерних ролей у сфері освіти та праці на фемінні та маскулінні. Варто зазначити, що прояви цього є і всередині сфери кібербезпеки.

3.2.3. Виклики у доступі жінок до сфери кібербезпеки в Україні: горизонтальна гендерна сегрегація

“За всі свої роки роботи у кібербезпеці у неї ніколи не було колеги-жінки.”
(Респондентка 1)

Прояви **горизонтальної гендерної сегрегації** стосуються диспропорції у співвідношенні жінок та чоловіків у сфері кібербезпеки в Україні. Згідно з даними DOU, у 2022 році жінки становили 23,4% працівників у сфері ІТ, що є значним покращенням порівняно з 8% понад десятиліття тому¹⁷⁵. Майже всі респондентки погодилися що у сфері значно більше чоловіків, ніж жінок. Також жінок вважають

¹⁷⁴ Марценюк, Т. (2017). *Гендер для всіх. Виклик стереотипам*. К.: Основи. (С. 135)

¹⁷⁵ Paliychuk, U. (2023, August 9). *Women in technology: Insights from Ukraine, Bulgaria, and Poland*. Beetroot.

радше винятком, а не звичною часткою складу у сфері. Деякі з респондент(ок)ів взагалі не працювали з жінками:

“Я бачу ту кількість жінок, дівчат, які приходять на наші заходи. Я називаю жартома “це як мужицький дощ”. Коли ти приходиш на будь-який захід, який відноситься до кібербезпеки, а там маленька кількість жінок, і в основному чоловіки... Жінки – це більше як виключення, ніж якась нормальна ситуація...”
(Респондентка 13);

“Гендерна диспропорція дуже відчутна. Це дуже смішно... Ну як смішно... Істерично, іронічно смішно, що коли організують гендерні зустрічі по правах жінок (в кібербезпеці), то там десь відсотків 70-80 чоловіків...”
(Респондент 7).

Жінки і чоловіки часто зайняті в різних сферах праці, а за умови роботи в одному напрямку вони нерідко виконують різну роботу, мають різні посади, заробітну плату та темпи кар'єрного росту¹⁷⁶. Респондент(к)и також наголосили на тому, що гендерна сегрегація у сфері кібербезпеки є вищою, ніж в інших в межах напрямку ІТ. Це свідчить про гендерно стереотипне уявлення та поділ сфер праці на традиційно “фемінні” та “маскулінні”:

“Батьки приходять, наприклад, на день відкритих дверей в Могилянку і такі: “Ой, ну кібербезпека – це не дуже жіноча справа, давай краще програмістом будь”... Існує уявлення, що програмування для жінок окей, а кібербезпека - ні. Ну кібер, він же з інформаційної безпеки, КГБ-шників, і т.д., і т.п. проростає... І тому... Ну, не хочу бути ейджистом, у людей елегантнішого віку, ніж мій, є певна уява про те, що це повинен точно бородатий чоловік цим займатися.”
(Респондент 7).

“Я недавно знайшла досить гарну аналогію. Я порівнюю кібербезпеку з нашою армією. Там є жінки. Це факт. Але їх дуже мало, і є сфери, де їх абсолютно нема... Так, в кібербезпеці є пен-тестери, де я майже не бачила жінок взагалі. І в армії, наприклад, на бойових посадах, є дуже мало.”
(Респондентка 2).

Соціально-демографічні характеристики також впливають на доступ та представленість жінок у традиційно маскулінних сферах праці, зокрема у сфері кібербезпеки. Респондент(к)и зазначили про такі **характеристики**, як: молодий вік, відсутність сім'ї, вища освіта, лідерські якості та відчуття “відмінності від інших жінок”. Наприклад, зміни в професії, що пов'язані з народженням дитини, Кімел називає “доріжкою для матусь”, що сповільнює професійне зростання і розвиток. Або ж через усталені гендерні норми, уявлення та очікування від молодих

¹⁷⁶ Маєрчик, М. (2017). *Гендер для медій: підручник із гендерної теорії для журналістики та інших соціокультурних спеціальностей* (3 видання, випр. і доп.). К.: Критика. (С. 79)

спеціалісток будуть відрізнятись від вимог, щодо жінок з дітьми¹⁷⁷. Проте, майже половина респондент(ок)ів не змогли відповісти на це питання, оскільки не вважають, що особисті характеристики впливають на доступ жінок у сферу кібербезпеки. Зокрема це пов'язано з тим, що горизонтальна гендерна сегрегація у сфері зумовлена не браком компетенцій у жінок, а впливом усталених соціокультурних уявлень, які формують професійні орієнтири ще на етапі освіти та соціалізації:

“Це не пов'язано із тим, які жінки приходять в кібербезпеку. Це пов'язано з тим, як люди в принципі вибирають свою професію.” (Респондент 10).

Важливим викликом сфери є не лише низька представленість жінок, а й причини їх звільнення та/або перешкоди в кар'єрному зростанні. Респондент(к)и зазначають відсутність спільної мови з колективом, низьку зарплату, складність роботи та військову службу і її особливості, як причини звільнення жінок зі сфери. Також респондент(к)и зазначили про такі причини, як одруження та створення сім'ї. Це свідчить про відтворення традиційних гендерних ролей серед представни(ць)ків сфери кібербезпеки:

“Гендерні стереотипи були. Це більше було від людей вже більш старшого віку, тому що вони звикли, що вони працюють, а їхні дружини сидять і дивляться за дітьми.” (Респондентка 6).

Респонденти зазначали, що важко визначити причини звільнення жінок, оскільки вони є спільними для всіх. Також один з респондентів зазначає, що ці спільні причини, ймовірно, для жінок є гіперболізованими. Це свідчить про дещо розмиті уявлення про причини звільнення жінок, зокрема у кібербезпеці в межах військової служби:

“В когось це особисті причини. Тому що, чоловік виїхав туди-то. І для того, щоб сім'я була разом, дружина теж переводилась. В когось кращі умови роботи. Все-таки – це навіть такі речі можливі, коли трохи перспективніша робота, трохи вища оплата, людина переводиться в інший підрозділ, в іншу організацію. Мабуть, ці дві основні, але, знову ж таки, в цьому середовищі, в якому я зараз перебуваю, воно специфічне.” (Респондент 10).

Серед викликів сфери кібербезпеки для жінок також є брак державної та громадської підтримки для підтримки жінок у сфері кібербезпеки. Йдеться про відсутність та/або низьку кількість якісних та ефективних ініціатив, як тренінги, квоти, менторство та подібні:

¹⁷⁷ Маєрчик, М. (2017). *Гендер для медій: підручник із гендерної теорії для журналістики та інших соціогуманітарних спеціальностей* (3 видання, випр. і доп.). (С. 14-16; 79-85). К.: Критика.

“Переважно ініціативи йдуть від громадського сектору, держава іноді підхоплює або доєднується до вже існуючих ініціатив ГО. Немає централізованої державної програми підтримки жінок.” (Респондентка 11).

“...це краще ніж нічого. Звісно, такі ініціативи насправді потребують доопрацювань... Так, ми про це говоримо, але на превеликий жаль поки що ми говоримо про це недостатньо, тому що ця тема повинна проникати у всі шари забезпечення кібербезпеки, починаючи від верхніх, що стосується саме організації роботи регуляторів, закінчуючи тими людьми, які відповідають за кібербезпеку підприємств в регіонах малих містечках, селищах.” (Респондентка 2).

Це свідчить про те, що горизонтальна гендерна сегрегація у сфері кібербезпеки в Україні значною мірою зумовлена відсутністю системної державної політики щодо підтримки та інтеграції жінок у цю галузь. Виклики виникають зокрема через низьку обізнаність суспільства щодо державних ініціатив та реформ. Респондентки підкреслюють, що ініціативи з подолання гендерного дисбалансу здебільшого залишаються на рівні ГО, тоді як держава не формує цілісного підходу, який охоплював би всі рівні – від формування нормативної бази до впровадження практичних рішень на місцях. Це вказує на фрагментарність зусиль і недостатню інституційну підтримку, що, своєю чергою, підсилює гендерну сегрегацію в технічних сферах, зокрема у кібербезпеці.

3.2.4. Виклики у доступі жінок до сфери кібербезпеки в Україні: вертикальна гендерна сегрегація

“Я напевно одна з небагатьох жінок, яка керує компанією. Там десь є на менеджерських позиціях, на керівних посадах набагато менше.” (Респондентка 11)

Відповіді респондент(ок)ів свідчать і про вертикальну гендерну сегрегацію. Передусім, зазначають про недостатню представленість жінок на керівних посадах або тих, що пов'язані з технічною складовою:

“У моєму робочому колективі жінки найчастіше займають посади Product, Project-менеджери, marketing, sales-менеджери, Customer Success, Pre-sales або рідше на інженерних ролях.” (Респондент 3);

“Поки в нас немає жодної жінки, яка була б на посаді начальника відділу, начальниці управління, заступника директора або директора. В інших підрозділах нашої служби є жінки, котрі є на посадах начальниць управління, начальниць відділів і навіть є жінки заступниці директора департаменту. Є одна жінка директорка департаменту.” (Респондент №10).

В Україні гендерна статистика розподілу керівних посад є лише для державної служби та не охоплює весь ринок праці. Хоча формальних заборон для жінок

обіймати керівні посади немає, на практиці їхнє кар'єрне просування часто ускладнюється та/або припиняється через невидимі бар'єри¹⁷⁸. Жінки переважно обіймають допоміжні, адміністративні або клієнтоорієнтовані позиції (менеджмент, маркетинг, підтримка), тоді як посади, пов'язані з управлінням або технічною експертизою, залишаються переважно чоловічими. Це вказує не просто на структурну нерівність, а й на наявність гендерних бар'єрів, пов'язаних із професійною соціалізацією, упередженими уявленнями про лідерство та недостатньою інституційною підтримкою жінок на шляху до керівних або фахових позицій. Варто зазначити, що це звужує можливості жінок та обмежує потенціал розвитку самої галузі, через обмеженість думок і досвідів у процесах прийняття рішень.

Крім того, респондентки зазначають, що навіть за присутності жінок на керівних посадах, існують формальні бар'єри, що свідчать про прояви "скляної стелі". Скляна стеля – явище, яке узагальнює набір бар'єрів, що виникли на ґрунті індивідуальних і суспільних упереджень та заважають жінкам просуватися кар'єрною драбиною в межах своєї організації, обіймати посади управлінського рівня¹⁷⁹. Ця ієрархія не є формально закріпленою, однак підтримується через гендерні стереотипи, що закріплює жінок на "середньому" рівні управління, тоді як стратегічні, ресурсні та технічно складні позиції залишаються під контролем чоловіків. Це відтворює структурну гендерну нерівність, зокрема у сфері кібербезпеки:

"Тут є важливий момент, що є ієрархія на папері, а є фактична. Часто вона відрізняється, навіть чоловіки між собою не можуть розподілити і вона часто реально різниться. Навіть якщо жінки є на папері в ієрархії, це не означає, що вони по факту є в цій ієрархії." (Респондентка 2).

Причиною є уявлення про сферу, як "технічно-чоловічу", оскільки респондент(к)и вказали на те, що жінки присутні в секторах, з менш вираженою технічною складовою кібербезпеки (наприклад, адміністраторки систем, комунікації з клієнтами, бухгалтерія, аудит). В той час, як на посадах у підрозділах ближчих до основних напрямків розвитку кібербезпеки (інженер(к)и, CISO, розробни(ці)ки) спостерігається їх нестача.

Відповіді респондент(ок)ів засвідчили наявність тенденції до гендерного розриву в оплаті праці, хоча рівень його усвідомлення та оцінки варіювався. Гендерний розрив в оплаті праці (англ. *wage* або *pay gap*) — одна з найпоширеніших форм дискримінації на ринку праці, яка передбачає, що чоловіки залежно від країни отримують в середньому на 10–40 % більше за жінок¹⁸⁰. Проте респондент(к)и зазначають, що не мають конкретних цифр або не помічали розриву протягом свого професійного зростання, зокрема в державному секторі, де зарплати зазвичай фіксовані:

¹⁷⁸ Маєрчик, М. (2017). *Гендер для медій: підручник із гендерної теорії для журналістики та інших соціогуманітарних спеціальностей* (3 видання, випр. і доп.). (С. 85-92). К.: Критика.

¹⁷⁹ Марценюк, Т. (2017). *Гендер для всіх. Виклик стереотипам* (С. 58). К.: Основи.

¹⁸⁰ Марценюк, Т. (2017). *Гендер для всіх. Виклик стереотипам* (С. 55). К.: Основи.

“Розрив оплати праці присутній всюди, кібербезпека скоріше не виключення.”
(Респондент 7);

“Як це не дивно звучить, але в державному секторі дискримінація менша, ніж в приватному. А в приватному це, може, навіть не дискримінація, тому що це жінка, а, може, тому, що просто жінка менше бореться за свій рівень зарплатні.” (Респондентка 8).

Серед відповідей є і приклади зворотньої дискримінації, що радше пов’язані з прагненням жінок вимагати рівної оплати праці у приватному секторі:

“Одна з подруг в кібербезпеці працює, і у неї була більша зарплата, тому розрив є, але є там якісь окремі випадки, що навпаки він в іншу сторону, але це, мені здається, більше такий унікальний випадок, що загалом це все ж таки тенденції є до розриву в сторону того, що в жінок менше ніж в чоловіків” (Респондент 5).

Гендерний розрив в оплаті праці є неприпустимим явищем, що фактично порушує права жінок, оскільки права людей концептуально співвідносяться з ідеєю ґендерної рівності. До того ж розрив в оплаті праці є проявом дискримінації, про який зазначено в Конвенції ООН. За нею дискримінація це: “...будь-яке розмежування, ізоляція або обмеження... людських прав і фундаментальних свобод жінок у політичній, економічній, соціальній, культурній, цивільній або будь-якій іншій сфері, незалежно від сімейного стану...”¹⁸¹. Зважаючи на це, вертикальна гендерна сегрегація у сфері кібербезпеки свідчить про наявність стійких інституційних та культурних бар’єрів, які обмежують професійне зростання жінок, відтворюючи гендерну нерівність у доступі до ресурсів, влади та впливу в галузі.

3.2.5. Виклики у доступі жінок до сфери кібербезпеки в Україні: сексуальні домагання і насильство

“Відвертих упереджень або домагань я не бачив і це однозначно добре.”
(Респондент 3)

Про досвід **сексуальних домагань** зазначили декілька респонденток. Проте жоден з респондентів не був свідком сексуальних домагань щодо жінок. Жінки зазначають те, що сексуальні домагання сприймаються як норма і проявляються на різних рівнях: на інституційному рівні — через зловживання владою з боку представників силових структур; на міжособистісному — у формі сексуалізованих повідомлень; на культурному — через об’єктивацію жінок і закріплені гендерні стереотипи, які нормалізують подібну поведінку.

“В мене був випадок, коли я прийшла на захід, одягнувши спідницю до колін, підбори і блузку, познайомилась з чоловіком з сектору безпеки та оборони. І

¹⁸¹ Близнюк, В. (2004). *Гендерні відносини в економічній сфері*. У М.М. Скорик (ред.) *Основи теорії гендеру: навчальний посібник*. (С. 304; 334-339). К.: К.І.С.

мені вночі прилітають вульгарні повідомлення із закликами до сексу, повідомлення на кшталт «які в тебе гарні ноги» чи ще щось. Просто люди собі це дозволяють відкрито.» (Респондентка 13).

Важливо, що сприйняття за норму пов'язане також і з проявами “особливого ставлення” з боку викладачів та/або колег чоловіків, що також є одним із проявів домагань. Тобто на горизонтальному рівні відносин. Попри те, що у ЗУ “Про забезпечення рівних прав та можливостей жінок і чоловіків” йдеться радше про вертикальний рівень, закон визначає дії, що принижують чи ображають осіб, як сексуальні домагання¹⁸². Таким чином, прояви “особливого ставлення” можна розглядати як сексуальні домагання. Проте такі та подібні формулювання часто включають слово “небажані”, що ускладнює юридичне і соціальне визначення таких актів, оскільки акцент на “небажаності” може знижувати серйозність проблеми та створювати перешкоди для ефективного реагування і притягнення до відповідальності, звужуючи межі розуміння сексуальних домагань лише до відвертих проявів порушень. Наприклад, не всі респондентки та їхні колежанки вважають це проблемою, а інколи — навіть перевагою:

“Не зважаючи на те, що це негативно не впливало на неї, вона почувалася некомфортно, отримуючи пропозиції про додаткову допомогу із навчанням від викладачів-чоловіків чи позашкільні зустрічі” (Респондентка 9);

“Скажу чесно, можливо, до мене більшість адміністраторів ставляться трішечки м'якше, бо я дівчинка, і вони, можливо, якимось бояться мене образити. Бо, наприклад, якщо щось по роботі піти випросити, всі зазвичай такі: “Давай ти!” Мені ж то без проблем.” (Респондентка 12).

Окрім того, респондентки наголошують, що на прояви сексизму впливають повноваження і влада, оскільки, висока чи рівноцінна з чоловіками посада жінки сприяє покращенню до неї ставлення чоловіків. В таких випадках часто чоловіки не дозволяють ніякі сексистські жарти чи упередження в сторону жінки:

“Я говорила про історію з сексизмом з жінкою, яка займає керівну посаду в секторі безпеки і оборони. Тобто вона постійно йшла по кар'єрній драбині до цієї посади, і вона мені сказала, що вона не бачить ніякої гендерної упередженості у цій сфері. Я зрозуміла для себе таку річ, що коли в тебе висока посада і ти керуєш людьми зверху, особливо чоловіками, вони не можуть собі дозволити у твою сторону ніякі сексистські жарти і так далі (ред.: йшлося про домагання і тд), тому що вони можуть втратити посаду” (Респондентка 13).

Прояви сексуальних домагань і насилля порушують етичні та професійні норми, є травмуючими та жорсткими діями, що порушують права людини. Окрім

¹⁸² Марценюк, Т. О. (2008). *Гендерна дискримінація на ринку праці в Україні (на прикладі сексуальних домагань)*. Наукові записки НАУКМА. Соціологічні науки, 83, 50-55.

того, вони створюють бар'єри для розвитку кар'єрного потенціалу жінок у галузі, сприяючи їхній маргіналізації. Подолання цих проблем потребує комплексного підходу, включаючи зміну організаційних структур, зміцнення законодавчих норм, зокрема шляхом концептуалізації термінів та розвиток корпоративної культури, яка підтримує інклюзивність, рівність та створення безпечного гендерно чутливого середовища.

3.2.6. Успіхи у доступі жінок до сфери в Україні: подолання горизонтальної гендерної сегрегації

“...дискримінація відійшла на “другий” план”

(Респондент 10)

Окрім викликів, респондент(к)и зазначили і про успіхи різного типу, щодо доступу та видимості жінок у сфері кібербезпеки. Це свідчить про те, що попри наявні виклики респондент(к)и відзначили позитивні зрушення щодо можливостей та безпосереднього долучення жінок та видимості жінок у професійній спільноті. Ці успіхи включають різні процеси подолання горизонтальної та вертикальної гендерної сегрегації. Тобто, стосуються умов входу жінок у сферу кібербезпеки та обмежень у кар'єрному просуванні вже всередині сфери.

Передусім, **початок повномасштабної війни позитивно вплинув на доступ та представленість жінок** у сфері. Респондент(к)и відзначили, що кількість жінок у сфері кібербезпеки на різних рівнях збільшилась з початком повномасштабного вторгнення. Це пов'язано з популяризацією залучення та інтеграції жінок у сферу кібербезпеки, як дисциплінарною в STEM, серед бізнесів та посадов(иць)ців. Наприклад, Міністерство освіти і науки України реалізовує концепцію STEM освіти з наголосом на важливість відмови від поділу сфер освіти та праці на чоловічі та жіночі.¹⁸³ Також збільшилась кількість вакансій, через потребу в працівни(ця)х для передбачення та виправлення проблем, що виникають через кіберзагрози та атаки. Зважаючи на це та мобілізаційні процеси, є й велика кількість вільних робочих місць:

“Загалом війна... Вона пришвидшила інтеграцію жінок у технічні команди, попит на кадри зріс, і дискримінація на фоні кваліфікації відійшла на другий план. Багато чоловіків на фронті, від цього також з'являється необхідність, потреба в закритті позиції, і таким чином, тобто вимушено, але все одно ми йдемо до цього, до зменшення диспропорції, що є добре...” (Респондент 3).

Це свідчить про зменшення горизонтальної гендерної сегрегації у сфері кібербезпеки України, що точно є успішною зміною. Проте часто ці процеси відбуваються не через активні реформи та/або свідоме ставлення до протидії дискримінації.

¹⁸³ Сидоренко, О. (2019, 19 грудня). Як залучати дівчат і жінок в ІКТ. Гендер в деталях. <https://genderindetail.org.ua/library/nauka-i-tehnologii/yak-zaluchati-divchat-i-zhinok-v-ikt.html>

Також успіхом на шляху до подолання горизонтальної гендерної сегрегації є **менша схильність молоді в Україні вдаватися до гендерних упереджень**. Про те, що молодь рідше погоджується з тим, що є професії, які підходять виключно для чоловіків і виключно для жінок, ніж старше покоління, свідчать дослідження різних міжнародних організацій¹⁸⁴. Зважаючи на це, можна зробити висновок, що в сучасній Україні формується соціальне середовище, в якому жінки можуть легше обирати професії, що гендерно марковані як “чоловічі”. Прояви цього явища помітні як і у сфері освіти, так і на ринку праці.

“Молодше покоління більш лояльно відноситься, і воно не розділяє, ти дівчинка чи хлопчик. Для них ти — професіонал, в першу чергу, а далі вже як буде” (Респондентка 7).

І хоча упередження щодо жінок та гендерні стереотипи все ще присутні і серед української молоді, можна зауважити зміну уявлень про гендерні ролі та більшу увагу до кваліфікації працівни(ць)ків, а не на їх стать.

Серед успіхів також варто відзначити **розвиток менторських програм та тренінгів для жінок**, особливо щодо протидії дискримінації та сексизму. Такий формат підтримки спрямований на залучення жінок у сферу кібербезпеки та розвиток навичок на ранніх етапах входу в професію.

“Ініціативи щодо залучення жінок часто існують лише на верхівці професійної піраміди, у великих організаціях та центральних органах. Натомість вони не охоплюють регіональні рівні, де безпосередньо здійснюється реалізація заходів із кібербезпеки на місцях” (Респондентка 2).

Це свідчить про те, що гендерна рівність та програми на цю тему впроваджується, що є плюсом. Але все ж вони досі розглядаються, як факультативні та/або символічні, а не як системна вимога до всієї галузі.

Окрім того, активно **запроваджуються ініціативи та реформи для підтримки жінок у сфері кібербезпеки на державному рівні**. Найчастіше це стосується забезпечення умов для ширшого доступу жінок до сфери загалом. Жінок системно включають до програм розвитку у форматі тренінгів, долучення до делегацій та програм лідерства. Це свідчить про реальні приклади реалізації політики інклюзивності у професійному середовищі. Тобто практика, за якої жінки не просто долучаються до сфери, а й мають доступ до можливостей професійного росту перебуває на етапі формування:

“...дивлячись по тому, що є у відділі, ну ось мене та моїх колег-жінок значно частіше просувають саме на якісь тренінгові програми, програми лідерства. Тобто там постійно, якщо от відправляється ну якась умовна делегація, хоча б з декількох людей на навчання, тобто обов'язково в цій делегації повинна бути щонайменше одна жінка.” (Респондентка 2).

¹⁸⁴ UNFPA Ukraine. (2021.). Презентація програми “Трамплін до рівності”. https://ukraine.unfpa.org/sites/default/files/pub-pdf/prezetation_trampoline_ukr_1.pdf

Цікавими та ефективними є всеукраїнські та регіональні ініціативи для залучення жінок задля подолання гендерної нерівності, що отримали підтримку на рівні держави, зокрема від посадових осіб та керівництва державних структур високого рівня. Результативність регіонального розвитку та ефективність регіональної політики значною мірою залежать від здатності узгодити інтереси держави з потребами суспільства, зокрема в громадах¹⁸⁵. Наприклад, ініціатива й подальше рішення Національного координаційного центру кібербезпеки (НКЦК) та міжнародні форуми:

“Рішенням НКЦК було прийнято започаткування ініціативи для залучення жінок у кібербезпеку для гендерної рівності. Тобто, це перший законодавчий кейс щодо гендерної рівності у сфері кібербезпеки” (Респондентка 13);

“Цього місяця вдруге проводився іівський міжнародний форум кіберстійкості. І під час цього заходу традиційно відбувались кіберзмагання. Вперше в Україні в них приймала участь національна жіноча команда. Це були представниці Збройних Сил України, СБУ, Міноборони, ДССЗЗІ виключно жіноча команда. І вона показала круті результати.” (Респондентка 13).

Важливість цього рішення полягає у тому, що саме ця ініціатива однією з перших порушила питання гендерної рівності та активного залучення жінок до сфери на державному рівні. Додатково до ініціативи впроваджуються освітні та менторські програми. Високу ефективність та залученість суспільства показали такі програми, як SheCyber Hub, що реалізовувалась за підтримки Фондації жіночого лідерства та стратегічних ініціатив (WLSIF) та Національного університету “Києво-Могилянська академія”. Метою є навчання студенток технічним навичкам в поєднанні з розвитком жіночого лідерства:

“Що ми ще робимо для жінок? У нас в планах дуже багато всього. І тренінги - не просто навчити якимись технічними спеціальностями, а саме лідерські, про побудову кар'єри, про професійний етикет, про розвиток саме як професійних жінок. Також ми запустили ініціативу ShesCyber Hub - тут ми йдемо вже з іншої сторони. Ми дівчатам студенткам і студентам хлопцям також даємо доступ до жінок-лідерок, які працюють у кібербезпеці.” (Респондентка 7);

“У нас тренінги не просто навчити технічним спеціальностям, а саме лідерські, про побудову кар'єри, про професійний етикет, про розвиток жінок саме як професіоналок своєї справи.” (Респондентка 13).

Така ініціатива та реформи відіграють важливу роль у підтримці гендерної рівності у сфері кібербезпеки. Вони сприяють формуванню спільноти жінок-лідерок, які не лише долають усталені гендерні стереотипи, але й виступають рольовими

¹⁸⁵ Інститут суспільно-економічних досліджень. (2017). *Нова регіональна політика для нової України: Аналітична доповідь*. Київ: Інститут суспільно-економічних досліджень.

моделями для інших жінок. Що важливо, вони виступають рольовими моделями і для чоловіків, оскільки все більше чоловіків підтримують розвиток та спроможність жінок у сфері кібербезпеки. Безпосередній діалог та робота із жінками, які досягли успіху у сфері, дозволяє іншим жінкам не просто отримати корисні поради, а й відчувати підтримку в межах своєї професійної спільноти.

3.2.7. Успіхи у доступі жінок до сфери в Україні: подолання вертикальної гендерної сегрегації

“В кібербезпеку йдуть жінки, які мають гарну освіту (орієнтовану на точні науки та факти) і готові до інтелектуальних викликів.” (Респондентка 8)

Серед успіхів у доступі жінок до сфери кібербезпеки в Україні є можливість працювати на посадах різних напрямків та рівнів для жінок. Що важливо — **кар’єрне просування жінок до провідних та/або керівних позицій:**

“Є старші інженери, є головні інженери, у нас просто йде система грейдерування. Наприклад, у мене там 14-й грейд, і чим вищий грейд, то відповідно, тим вища посада. Є там 17-і грейд, 18-і грейд. Тобто це є такі уже доволі нормальні керівні посади”. (Респондентка 7).

Зокрема, можна виділити представленість жінок на таких посадах у державному секторі. Одна з респонденток зазначила:

“У нас (в Україні) жінки займають керівні посади у ключових відомствах, які відповідають за розвиток та безпеку країни.” (Респондентка 13).

Серед найбільших досягнень жінок виокремили те, що керівницею Національного координаційного центру кібербезпеки є Наталя Ткачук, про яку йшлося раніше. Важливо також відзначити Катерину Черногоренко, яка на посаді заступниці Міністра оборони України відповідає, зокрема, за розвиток кібербезпеки в системі Міноборони. А також те, що Євгенія Волівник очолювала урядову команду реагування на надзвичайні інциденти впродовж повномасштабного вторгнення.

Аналіз відповідей респондент(ок)ів засвідчує наявність позитивних зрушень щодо формування гендерно чутливого середовища сфери кібербезпеки в Україні. Йдеться не лише про формальне збільшення присутності жінок у цій галузі, але й про реальні можливості для їхнього професійного зростання, розширення соціальних зв’язків, менторської підтримки та інституціоналізації гендерно чутливих ініціатив. Це свідчить про орієнтацію на впровадження гендерно чутливого підходу, задля підвищення кваліфікації, видимості та залученості жінок до сфери кібербезпеки.

Знаковим успіхом для подолання вертикальної гендерної сегрегації сфери кібербезпеки України є **наявність та обізнаність про жіночі рольові моделі**. Вони ж зазвичай пов’язані з успішними жінками на вищих та/або провідних позиціях, що руйнує "скляну стелю". Не менш важливо, що серед рольових моделей респондент(к)и згадували своїх колежанок, що свідчить про формування мережі

підтримки жінок:

“Я тішуся, що мені по роботі доводиться періодично спілкуватися, достатньо активну позицію займає Ткачук Наталія Андріївна, вона є секретаркою НКЦК при РНБО України.” (Респондентка 10).

12 з 14 респондент(ок)ів назвали ім'я та спеціалізацію мінімум 1 жінки, що є рольовою моделлю в їхньому розумінні. Були й ті, хто назвали трьох і більше. Зважаючи на це ми можемо припустити, що ці знання залежать радше від зацікавленості та обізнаності кожної та кожного. Серед тих, кого респондент(к)и згадували найчастіше — керівниця Служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталя Ткачук; співзасновниця та CEO Фондації жіночого лідерства та стратегічних ініціатив, — Анастасія Островська та співзасновниця платформи з пошуку роботи в кібербезпеці CyberPeople — Ольга Насібуліна; крім того, респондент(к)и згадували Ганну Мартинюк та Євгенію Наконечну.

3.3. Українські медіа про жінок у кібербезпеці

Бойко Діана, Петровець Маргарита, Михайлів Віталій, Вірич Анна, Костюк Олена, Давиденко Віктор

3.3.1. Методологія аналізу медійних повідомлень

Дослідження проведено в межах інтерпретативного підходу із застосуванням якісного тематичного аналізу медійних матеріалів. Тематичний аналіз — це метод, що дає змогу структурувати та інтерпретувати якісні дані шляхом виявлення повторюваних смислових елементів, які пов'язані з дослідницьким питанням¹⁸⁶. Даний аналіз не є прив'язаним до певної теоретичної парадигми, тому його можна застосовувати як у дедуктивних, так і в індуктивних підходах.

Початковий щабель збору матеріалів здійснювався за допомогою сервісу Shukach Pro¹⁸⁷ — української спеціалізованої платформи для автоматизованого пошуку медійного контенту в українському онлайн-просторі. Це інформаційно-аналітичний програмний продукт, розроблений групою компаній “NOKs fishes”, яка спеціалізується на медіа-моніторингу та аналізі інформаційного поля в економічній, політичній і соціальній сферах. Завдяки директору компанії “NOKs fishes” та старшому викладачу кафедри зв'язків з громадськістю НаУКМА, Олегу Кононенко, було забезпечено доступ до цієї платформи, що значно полегшило роботу з медіаматеріалами. Було сформовано низку ключових запитів, зокрема: “жінки в кібербезпеці”, “фахівчині з кіберзахисту”, “гендерна рівність у

¹⁸⁶ Squires, V. (2023). Thematic analysis. In J. M. Okoko, S. Tunison, & K. D. Walker (Eds.), *Varieties of qualitative research methods: Selected contextual perspectives* (pp. 463–469). Springer Nature.

¹⁸⁷ <https://www.shukach.pro/>

цифровій сфері”, “жінки в ІТ”. У результаті пошуку було виявлено 710 публікацій, які потенційно відповідали тематиці дослідження (Таблиця 3.3.1.1).

Таблиця 3.3.1.1. Дизайн багатоетапної вибірки дослідження репрезентації жінок у сфері кібербезпеки в українських медіа, квітень 2025 року.

Щабель відбору	Опис етапу	Критерій включення	Кількість одиниць
1	Пошук матеріалів через Shukach Pro за ключовими словами	Тематична релевантність за ключовими запитами	710 публікацій
2	Видалення новин без аналітики, дублювань, фрагментарних чи рекламних матеріалів	Формат: інтерв'ю, історія, аналітика; наявність опису досвіду	124 публікації
3	Ручне очищення вибірки	Змістова насиченість, професійні історії, інституційна залученість	71 публікація
4	Остаточне структурування	Тематична насиченість, відсутність дублів, глибина	44 публікації

На другому щаблі здійснювався відбір за критерієм змістовної насиченості та тематичної релевантності. Із загальної кількості матеріалів були вилучені дублікати, рекламні, фрагментарні публікації та ті тексти, що не мали змістовної аналітичної складової. У результаті залишились лише ті публікації, які містили персональні історії, інтерв'ю, експертні коментарі, опис професійного шляху жінок у сфері ІТ та/або роздуми про гендерну рівність у технологічному середовищі.

На третьому щаблі здійснено ручний перегляд і первинне очищення вибірки. Вибірка була доукомплектована матеріалами з аналітичних платформ, блогів, сайтів неурядових організацій, які працюють на перетині тем цифрових прав, кіберзахисту, інформаційної гігієни та жіночого лідерства в технологіях. Такий підхід дозволив забезпечити тематичне розмаїття та охопити широкий спектр інформаційних посередників.

На четвертому шаблі здійснено остаточне структурування вибірки — до фінального аналізу увійшли 44 публікації. Вони були обрані за такими критеріями: 1) належність до формату аналітичного матеріалу, інтерв'ю чи персональної історії; 2) змістова насиченість (наявність опису досвіду, викликів, соціального контексту тощо). Така форма подачі матеріалів дозволила дослідити не лише формальну присутність жінок у медіа, але й глибину, тональність та фокус цієї репрезентації. Відібрані публікації охоплюють часовий період із 2017 до 2025 року (див. *Додаток В*).

Під час аналізу матеріалів використовувались попередньо визначені теми: *жінки в ІТ та кібербезпеці на ринку праці, освітні програми для жінок у сфері кібербезпеки, жінки у військовій кібербезпеці та обороні, жінки як експертки з кібербезпеки*.

У процесі аналізу медіатекстів було застосовано два аналітичні підходи — гендерно чутливий та гендерно нейтральний, які використовувалися для інтерпретації змісту відібраних матеріалів.

Гендерно чутливий підхід передбачає виявлення та осмислення того, як у медійному дискурсі репрезентується жіночий досвід, чи артикулюються проблеми структурної нерівності, дискримінації або виклики, з якими стикаються жінки у сфері кібербезпеки¹⁸⁸. Натомість гендерно нейтральний підхід означає, що стать персонажа або героїні не відіграє значущої ролі в структурі матеріалу. У таких публікаціях жінки зображені виключно через призму професіоналізму, без згадки про специфіку їхнього досвіду як представниць меншості у сфері¹⁸⁹.

3.3.2. Жінки в ІТ та кібербезпеці на ринку праці: залучення та гендерна (не)рівність

У межах гендерно чутливого підходу до висвітлення теми жінок у кібербезпеці в низці аналізованих публікацій згадувалося про сприяння гендерної рівності на ринку праці у сфері кібербезпеки та подолання дотичних до цієї теми стереотипів. В одній із публікацій наводили цитату заступниці Генерального секретаря НАТО, в якій йшлося, що ексклюзивність жінок зі сфери кібербезпеки є неприпустимою:

“Кібербезпека – це командна гра, а ми залишаємо половину наших гравців на лаві запасних... НАТО прагне такої ж самої гендерної рівності в галузі кіберзахисту, як і в усіх інших аспектах безпеки, які ми маємо. Це не лише правильно, а і необхідно для нашої колективної оборони” (Матеріал №37, 2017).

Коментували питання гендерної нерівності в межах ширшої галузі інформаційних технологій, до якої входить кібербезпека, й самі чоловіки. На думку

¹⁸⁸ Марценюк, Т. (2019). *Інтеграція гендерної складової в аналітичні матеріали*. МФ “Відродження”, с. 8–11.

¹⁸⁹ Маєрчик, М., Плахотнік, О., & Ярманова, Г. (Ред.). (2017). *Гендер для медій: Підручник із гендерної теорії для журналістики та інших соціогуманітарних спеціальностей* (3-є вид., випр. і доп.). Критика.

Сергія Токарева, IT-підприємця, гендерні стереотипи й упередження заважають жінкам входити до сфери IT та розвиватися в ній:

“Багато українок досі, попри бажання вчитися та працювати в IT, ставляться до цієї індустрії з пересторогою. Зазвичай через гендерні упередження...І починається це ще зі школи. Давайте разом пройдемо шлях середньостатичної дівчинки, яка планує увійти в IT-сферу. У школі вона старанно вивчає математику, фізику та інші точні науки, цікавиться програмуванням. Але вже тут вона стикається з міфом про те, що більшість дівчат – гуманітарії, а хлопці – “технарі”” (Матеріал №27, 2022).

З цією тезою погоджувалися й жінки, уже залучені до сфери IT:

“Після серії обговорень із вченими у цій галузі ми дійшли висновку, що стереотипи є основною причиною, чому жінки рідше обирають технічні програми порівняно з чоловіками” (Матеріал №44, 2021).

Водночас у медіа висвітлювали погляди дівчат і жінок, які протестують такому шаблонному мисленню, говорячи про безсенсовність поділу професій за гендерною ознакою. Це сприяє наданню більшої об’єктивності питанню залученості жінок до сфери кібербезпеки в інформаційному полі, кидає виклик усталеним нормам і відкриває простір для публічної дискусії про гендерні ролі. Такий підхід медіа також може стимулювати переосмислення політик і практик, що відтворюють нерівність у цій сфері та інших суміжних.

“Анна розуміє, що не має сенсу розділяти професії за гендерним принципом: “Звичайно! Я вважаю, що не доречно розділяти спеціальності для “дівчат” та “хлопців”, тому що розумові здібності не визначаються статтю. Важливіші такі якості як розум, наполегливість, логічне та критичне мислення, цілеспрямованість. І якщо дівчина має ці якості, то чому б ні?”” (Матеріал №12, 2023).

В особистих історіях прослідковуються показові приклади залучення жінок до сфери кібербезпеки. Наприклад, в одній із публікацій проілюстровано практику позитивної дискримінації, коли компанія цілеспрямовано надала перевагу кандидатці, аби зменшити гендерний дисбаланс у сфері IT. Такий підхід не заперечує професійні якості кандидатки, а натомість визнає, що структурна нерівність потребує активного втручання для її подолання. Водночас це також підкреслює, що жінки в технічних галузях можуть здобувати можливості не лише завдяки винятковості, а й завдяки наявності інституційної підтримки та зміни корпоративної культури. Це свідчить про поступовий зсув у напрямку егалітарної моделі, де створюються умови для реального залучення жінок до традиційно “чоловічих” сфер.

“До слова, саме завдяки тому, що я жінка, мені вдалося потрапити в IT-сферу швидше, ніж очікувала. Виявилось, що коли я проходила співбесіду в

Drupal-школу, було два гарних кандидати на останнє місце: я і хлопець. Конкурент був навіть трохи сильнішим — він уже мав досвід роботи з Drupal, і з php працював більше ніж 2 місяці, на відміну від мене. Але в компанії була мета: збільшити присутність жінок в IT-сфері. Тому вони обрали мене, за що я їм дуже вдячна” (Матеріал №6, 2021).

Водночас у низці аналізованих публікацій, в яких хоч і йшлося про сприяння гендерного паритету у сфері кібербезпеки, все ж прослідковувалося винесення жінок у цій галузі на другий план:

“Залучення жінок до сфери кібербезпеки значно підсилює нашу здатність протидіяти кіберзагрозам. Жінки мають унікальне мислення, яке доповнює підходи чоловіків” (Матеріал №22, 2024).

Зрештою, медіа наголошували на важливості **егалітарного підходу** роботодавців до публікацій оголошень про вакансії у сфері кібербезпеки, підкреслюючи необхідність уникати гендерно упереджених формулювань, які можуть несвідомо відштовхувати кандидаток, а натомість використовувати інклюзивну мову, що сприяє формуванню відкритого та різноманітного професійного середовища:

“Оголошення про вакансію в галузі кібербезпеки мають бути написані так, щоб жінки-професіонали відчували себе бажаними та цінованими в цій сфері” (Матеріал №32, 2021).

Ба більше, згідно зі статтею **17 Закону України “Про забезпечення рівних прав та можливостей жінок і чоловіків”**¹⁹⁰ від 8 вересня 2005 року, у вакансіях заборонено, за винятком окремих випадків, вказувати бажаний гендер майбутнього працівника: “Роботодавцям забороняється в оголошеннях (рекламі) про вакансії пропонувати роботу лише жінкам або лише чоловікам, за винятком специфічної роботи, яка може виконуватися виключно особами певної статі, висувати різні вимоги, даючи перевагу одній із статей, вимагати від осіб, які влаштовуються на роботу, відомості про їхнє особисте життя, плани щодо народження дітей”.

3.3.3. Освітні програми для жінок у сфері кібербезпеки

Гендерно нейтральний підхід у матеріалах про навчання та професійний розвиток жінок у сфері кібербезпеки виявляється в акцентах на професійних компетенціях і мотивації, а не на статі. Стать подається як нейтральна змінна — важливішими є амбіції, знання, навички. Наприклад, програма “Women in Cyber” позиціонується як така, що не вимагає досвіду, але підтримує тих жінок, які мають прагнення навчатися і розвиватися:

¹⁹⁰ Верховна Рада України. (2005, 8 вересня). Закон України “Про забезпечення рівних прав та можливостей жінок і чоловіків” № 2866-IV. <https://zakon.rada.gov.ua/laws/show/2866-15>

“Ця програма орієнтована на жінок, які хочуть зробити перші кроки у сфері кібербезпеки або поглибити свої знання в цій галузі. Програма надасть учасницям можливість освоїти основи кібербезпеки та отримати підтримку від успішних лідерок галузі... Хто може взяти участь? Жінки з мотивацією та бажанням розвиватися у кібербезпеці (попередній досвід не потрібний)” (Матеріал № 11, 2025).

Ще один приклад — вебінар, у межах якого наголошується, що професійне зростання залежить від внутрішньої рішучості та здатності формувати амбітні кар’єрні цілі:

“Проєкт USAID “Кібербезпека критично важливої інфраструктури України” вирішив організувати вебінар для дівчат-студенток, щоб розповісти три історії харизматичних кібер-експертток... Дівчата, запрошуємо саме вас долучитись... Впевнені, що наші спікерки надихнуть вас відкинути свої побоювання (якщо ви стикалися із ними) та ставити амбітні цілі на карті вашого кар’єрного шляху” (Матеріал № 9, 2023).

Підтвердженням гендерно нейтрального підходу є також позиціонування кібербезпеки як сфери, відкритої для всіх людей із високим рівнем логічного мислення та зацікавленістю в технологіях. Зокрема, в одному з конкурсів для підлітків акцентується, що ключовими критеріями відбору є аналітичні здібності та навички кодування, а не гендерна приналежність учасниць:

“Дівчатка у віці 13–15 років візьмуть участь у тестах на логіку та кодування, створення мереж і криптографії... Британське розвідувальне агентство Центр урядового зв’язку вважає, що дівчата-підлітки, які проводять багато часу в інтернеті та соцмережах, можуть стати розвідницями майбутнього” (Матеріал № 13, 2017).

Використання гендерно-нейтрального підходу прослідковується й у наголошуванні на первинності інтересів і навичок, а не гендерних упереджень при виборі кібербезпеки як спеціальності для здобуття у ЗВО. Так, наприклад, студентка цього фаху Державного університету інформаційно-комунікаційних технологій зауважує:

“Я вважаю, що не доречно розділяти спеціальності для “дівчат” та “хлопців”, тому що розумові здібності не визначаються статтю. Важливіші такі якості як розум, наполегливість, логічне та критичне мислення, цілеспрямованість. І якщо дівчина має ці якості, то чому б ні?” (Матеріал №12, 2023).

Відсутність гендерних упереджень чи особливих критеріїв для дівчат у відборі до освітніх програм прослідковується й у матеріалах, присвячених початку набору

дівчат до Київського військового ліцею імені Івана Богуна, де готують зокрема й майбутніх фахівців і фахівчинь із кібербезпеки:

“Цього року плануємо набрати від 10 до 30 дівчат. Перший рік ми попросили мінімальну кількість. Якщо це буде вдалий рік, будемо обґрунтовувати пропозиції для керівництва і збільшувати кількість”, - наголосив Гордійчук. За його словами, дівчата дуже фахово могли б забезпечувати інформаційно-психологічні операції, кібербезпеку, спецрадіозв'язок та ін. Відповідаючи на питання щодо особливостей вимог до дівчат-абітурієнтів, Гордійчук підкреслив: “У нас гендерна рівність, тож вимоги як до хлопців, так і до дівчат однакові” (Матеріал № 30, 2019).

Позиціонування кібербезпеки як галузі, у якій можлива успішна професійна реалізація незалежно від статі, знаходимо й у матеріалі обласного центру зайнятості Волині:

“У нас немає поділу на чоловічу чи жіночу роботу”, “...три особи взяли ваучер на навчання у новій професії, одна з них освоїла спеціальність “Кібербезпека”” (Матеріал №25, 2023).

Крім цього, у низці матеріалів було зафіксовано гендерно чутливий підхід до опису освітніх ініціатив, які спрямовані на підтримку жінок у сфері ІТ і кібербезпеки. Ці заходи не обмежуються виключно передачею знань, а враховують соціальний контекст і структурні бар'єри, з якими стикаються жінки. Вони пропонують спеціалізовану підтримку, що охоплює емоційне підкріплення, менторство, підготовку до реального ринку праці та зниження тривожності перед входом у маскулінізовану галузь.

Учасницям надається доступ не лише до лекцій і практичних сесій, а й до консультацій із кар'єрного розвитку, психологічної стійкості та лідерства:

“Захід переконав 95% відвідувачок у тому, що ІТ – це бізнес для жінок. На заході розглядалися теми ефективного лідерства в мінливій реальності, кібербезпеки, стійкості ESG, а також лектори розповідали про кар'єрний розвиток, психічне здоров'я та добробут. На знак солідарності з українськими жінками частину заходу “День Кар'єри Жінок в ІТ” відвели воркшопам, які проводили українки для українок. Ментори та експерти з України ділилися порадами щодо вибору професії, пошуку високооплачуваної роботи та підготовки до співбесіди” (Матеріал № 41, 2022).

Ще одним прикладом освітньої ініціативи, що сприяє розвитку студенток у сфері кібербезпеки була менторська програма для жінок “Кібербезпека критично важливої інфраструктури України”. Наставницями були жінки, що мають досвід побудови успішної кар'єри в цій галузі. Такі ініціативи сприяють не лише розвитку

професійних навичок, але й обміну досвідом у подоланні бар'єрів із якими стикаються фахівчині в традиційно “чоловічих” професіях.

“Проект USAID “Кібербезпека критично важливої інфраструктури України” руйнує стереотипи про виключно “чоловічі” професії та підтримує жінок у галузі кібербезпеки. Відібрані учасниці разом з досвідченими фахівчинями працюватимуть над створенням власної мапи професійного розвитку” (Матеріал №10, 2022).

У матеріалах простежується акцент на важливості створення **фахових жіночих спільнот**, які функціонують як професійна підтримка та спосіб протидії системним упередженням у сфері кібербезпеки. Вони сприяють обміну досвідом, розвитку менторських практик і загальному посиленню присутності жінок у високотехнологічних секторах.

“Цей захід має на меті розповісти про можливості залучення до професійних асоціацій жіноцтва, яке працює у сфері кібербезпеки, а також ознайомити з деякими європейськими та українськими жіночими кіберасоціаціями. Наші спікерки з Women4Cyber, EUGAIN, Kharkiv ACM-W Chapter та ISCA поділяться власним досвідом створення своїх асоціацій та жіночих кіберспільнот. Також ви дізнаєтеся про візії асоціацій, умови членства у професійних кіберасоціаціях, їхні менторські програми та заходи з професійного розвитку, які допоможуть побудувати зв'язки з кібергермадою” (Матеріал № 7, 2023).

Ще одним прикладом гендерно чутливого підходу у впровадженні освітніх ініціатив у галузі кібербезпеки є програма “Кібербезпека для дівчат: можливості й професія”. Вона передбачає не лише засвоєння технічних знань, але запозичення досвіду від успішних фахівчинь у цій царині:

“У грудні 2024 року стартує нова освітня ініціатива від STEM is FEM для дівчат віком 16–21 рік. Програма “Кібербезпека для дівчат: можливості й професія” допоможе учасницям опанувати базові навички захисту в діджиталі та розглянути кар'єрні перспективи у сфері кібербезпеки. Окрім технічних знань, учасниці дізнаються про кар'єрні можливості в кібербезпеці, історії успіху жінок у цій галузі та про освітні ресурси для розвитку у сфері” (Матеріал №42, 2024).

Особлива увага також приділяється профорієнтаційним ініціативам для дівчат віком 12–16 років. Такі заходи спрямовані на подолання гендерного стереотипу про ІТ як “чоловічу” сферу та відкриття можливостей ще до моменту вибору професії. Організатори та організаторки підкреслюють важливість позитивних жіночих прикладів у ролі лекторок, менторок і героїнь історій успіху. На заняттях дівчата можуть спробувати себе в різних напрямках, таких як дата-аналітика, вебпрограмування або машинне навчання:

“Потрібно показувати юним дівчатам, що ІТ — це крута галузь для розвитку, що це не страшно, що тут є приклади для наслідування.

Часто дівчата не йдуть в ІТ, адже вони не бачать потенційних однодумиць поряд. Тому для вирішення цієї проблеми треба створювати тематичні клуби та спільноти, щоб кожна учасниця могла звернутися за порадою чи підтримкою до своєї товаришки.

Саме таке завдання ми ставили перед собою, коли створювали громадську організацію STEM is FEM” (Матеріал № 27, 2022).

Ще одним прикладом заходу для подолання гендерних упереджень при виборі професії в школярок є й екскурсії технологічними та науково-дослідними компаніями:

“8 жовтня 2019 року одночасно у всіх областях України відбувся Національний День дівчат в технологіях. У цей день близько 50 технологічних компаній та науково-дослідних центрів відкрили свої двері для школярок 8-10 класів та студенток, щоб пробудити їхній інтерес до науки, техніки, інженерії та математики (STEM) та зруйнувати їхні стереотипні уявлення про професії... Компанія “EY” підготувала для юних дівчат-науковців цікаву двогодинну програму, аби залучити їх до STEM-професій. З подивом дізналися вони, що дівчата можуть успішно працювати у напрямках кібербезпеки та ІТ-консультацій у компанії великої четвірки “EY”, зокрема, по розробці ІТ-стратегії, проводити ІТ-аудити” (Матеріал № 15, 2019).

Гендерно чутливий підхід ми вбачаємо й у створенні освітніх можливостей для розвитку жінок у кібербезпеці на всіх рівнях. Оскільки крім горизонтальної сегрегації ринку праці, фахівчині нерідко стикаються і з вертикальною, що передбачає їхній обмежений доступ до керівних посад. Тому важливим є впровадження відповідних програм, не лише для входу в нову галузь, але й на подальших щаблях розвитку кар'єри. Про це згадує й керівниця служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, секретарка Національного координаційного центру кібербезпеки Наталія Ткачук:

“Ми маємо створювати можливості для професійного зростання та розвитку на всіх рівнях — від здобуття освіти до керівних посад, сприяючи залученню нових талантів у сферу кібербезпеки” (Матеріал №31, 2020).

Ще одним прикладом програми, яка сприяє розвитку кар'єри жінок у кібербезпеці на різних рівнях є національна ініціатива з розвитку жіночого лідерства в кібербезпеці:

“Цей проєкт сприятиме розширенню кадрового потенціалу та інноваційних можливостей України, забезпечуючи гендерну рівність та залучення жінок до стратегічних і оперативних завдань у кібербезпеці. Ініціатива не тільки відповідає принципам соціальної справедливості та дотримання прав

людини, а й є стратегічною необхідністю для України в умовах війни та зміцнить позиції України як міжнародного лідера у сфері кібербезпеки” (Матеріал № 1, 2024).

3.3.4. Жінки у військовій кібербезпеці та обороні

Прямі прояви гендерно нейтрального підходу, який прагне нівелювати значення статі й універсалізувати роль військового або фахівця з кібербезпеки, в аналізованих публікаціях практично відсутні. У жодній із них не містяться твердження на кшталт “кібербезпека не має статі” або подібні, що повністю ігнорували б гендер як категорію.

Навіть у цитатах, які можуть натякати на рівність (*“рівність можливостей”* у Матеріалі №18, 2025), акцент все одно робиться на жінок, які демонструють цю рівність або користуються цими можливостями. Тобто гендер не “стирається”, а навпаки, підкреслюється як фактор, що раніше міг бути причиною нерівності.

Цей факт свідчить про те, що на даному етапі розвитку українського суспільства та медіадискурсу (після 2014 року, особливо в контексті війни), присутність жінок у військових і безпекових, зокрема кібербезпекових, структурах все ще є досить новим і поки що недостатньо поширеним явищем. Саме тому медіа схильні не ігнорувати гендерний аспект, а навпаки — сфокусовані на підвищенні видимості жінок.

Одним із прикладів застосування гендерно чутливого підходу в медіаматеріалах є акцент на участі жінок у військовій сфері з представленням статистичних даних.

“Активна участь жінок у захисті країни підкреслює рівність можливостей у Силах оборони. Вони ефективно займають як штабні, так і бойові посади, зокрема у сферах медицини та БПЛА. Зв’язок і кібербезпека – 6% [про відсоткове значення жінок у силах оборони]” (Матеріал №18, 2025).

Ця цитата показує, що медіа не просто згадують про жінок, але й наводять конкретну статистику їхньої присутності у відповідній галузі. Фраза *“Активна участь жінок”* сама по собі є маркером гендерної чутливості, оскільки акцентує саме на жіночій участі. Показник “6%” є важливим емпіричним даним, який ілюструє, хоч і невелику, але зафіксовану частку жінок у цьому секторі, роблячи їхню присутність відчутною.

Схожий приклад наявний у матеріалі №3 (2020), присвячений Військовому інституту телекомунікацій та інформатизації імені Героїв Крут. У ньому зазначається *“більше ніж десять відсотків дівчат”* серед курсантів і факт набору *“дівчат на командні спеціальності”*. Це прямо вказує на зростання кількості жінок у військовій освіті, зокрема на технічних спеціальностях, таких як кіберзахист, і робить цей тренд помітним для аудиторії.

“Також у нас навчаються і дівчата, які здебільшого обирають спеціальності з комп’ютерних наук та кіберзахисту. Наприклад, якщо дівчина

опануватиме фах 'кібербезпека', буде хакером і зможе воювати на відстані за допомогою мереж — це принесе користь для держави. Таким жінкам потрібно аплодувати! У випадку, коли жінка-зв'язківець стає начальником радіорелейної станції, до складу якої входить машина з важким антенно-щогловим пристроєм, вони можуть фізично з обов'язками не впоратись. Треба чітко розуміти, де і на яких посадах зможуть служити дівчата й враховувати це. Хоча варто додати, що торік уперше дівчат набрали на командні спеціальності. Загалом, серед курсантів більше ніж десять відсотків дівчат” (Матеріал №3, 2020).

Деякі медіа наголошують на тому, що жінки самі виявляють інтерес до здобуття знань і навичок у галузі кібербезпеки.

“У закладах освіти фіксують тенденцію збільшення кількості охочих здобути військову освіту за інженерно-технічним, розвідувальним профілем. Жінки-військові бажають вивчати комп'ютерні науки та питання кібербезпеки” (Матеріал №36, 2020).

Це свідчить про визнання суб'єктності жінок та їхнього свідомого вибору опанувати ці раніше “чоловічі” спеціальності.

“Дівчата, які здебільшого обирають спеціальності з комп'ютерних наук та кіберзахисту... дівчина опануватиме фах “кібербезпека”, буде хакером і зможе воювати на відстані за допомогою мереж” (Матеріал №3, 2020).

Тут не просто констатується вибір, а й окреслюється потенційна роль (“буде хакером”) та її цінність для держави (“зможе воювати на відстані”). Це робить роль жінки-кіберфахівчині більш конкретною та вагомою в дискурсі.

Значна частина посилів у медіа сфокусована на проблемах, пов'язаних із гендерними стереотипами та нерівністю, та наголошує на необхідності їх подолання.

“Необхідно відмовитися від стереотипів щодо ролі жінок у сфері кібербезпеки... Підтримка гендерної рівності... має стати пріоритетом”. (Матеріал №8)

Ця цитата є прикладом критичного ставлення до існуючих бар'єрів (стереотипів, що “заважають розвиватися”) та водночас – закликом до дій задля досягнення рівних можливостей. Такий дискурс є визначальним для гендерно чутливого підходу, який не замовчує проблеми, а навпаки – виносить їх на обговорення.

Це висловлювання, хоча й стосується НАТО, але водночас ретранслює важливий меседж про нерівність:

“половину наших гравців на лаві запасних... лише майже одна з десяти осіб, що працюють в галузі кіберзахисту, жінка” (Матеріал №37, 2017)

Ці фрази метафорично та статистично демонструють проблему недопредставленості жінок, що є фундаментальною нерівністю, яку гендерно чутливий підхід прагне викрити та виправити.

Хоча медіа прямо не заглиблюються у специфічні гендерно обумовлені виклики у сфері кібербезпеки (зокрема, кіберпереслідування, сексизм у цифровому середовищі тощо), у Матеріалі №3 (2020), де йдеться про військову освіту та кар'єрні перспективи, порушується тема фізіологічних особливостей жінок. Наприклад, звучать твердження на кшталт: “фізично не впоратися з обов'язками” або “треба чітко розуміти, де і на яких посадах зможуть служити дівчата”. Подібні висловлювання можуть репрезентувати стереотипний підхід до спроможності жінок виконувати військові функції, навіть у тих сферах, де фізичне навантаження не є ключовим, як-от у кібербезпеці. Водночас, подібні обговорення можуть слугувати і прикладом гендерної чутливості — коли визнається, що жінки та чоловіки можуть мати різні потреби, які важливо враховувати при організації служби. Хоча це стосується фізичних аспектів, сам принцип “враховувати гендерні відмінності для ефективності та комфорту” є універсальним для гендерно чутливого підходу і може бути застосований до будь-яких аспектів служби, включаючи забезпечення відповідних умов праці для жінок-кіберфахівчинь.

Секретарка НКЦК Наталія Ткачук на засіданні Національного кластера кібербезпеки на тему “Роль жінок у забезпеченні кіберстійкості України: виклики та перспективи” зазначила:

“Під час повномасштабного вторгнення РФ залучення жінок до сфери кібербезпеки — це не просто питання рівності чи дотримання міжнародних стандартів. Це життєва необхідність для зміцнення національної безпеки та забезпечення стійкості держави. Жінки завжди відігравали важливу роль у розвитку нашої країни, і сьогодні їхній внесок стає ще більш значущим. Ми маємо створювати можливості для професійного зростання та розвитку на всіх рівнях — від здобуття освіти до керівних посад, сприяючи залученню нових талантів у сферу кібербезпеки” (Матеріал №22, 2024).

Цей фрагмент чітко демонструє перехід від гендерно нейтрального до гендерно чутливого підходу. Держава визнає не просто присутність жінок, а необхідність їхнього активного залучення до безпекової політики. У цьому контексті важливо не тільки рівне представництво, а й розуміння, що жінки відіграють незамінну роль у формуванні кіберстійкості держави. Це підсилюється цитатою заступника Секретаря РНБО України Сергія Демедюка:

“Жінки мають унікальне мислення, яке доповнює підходи чоловіків, створюючи синергію, що дозволяє успішно вирішувати найскладніші завдання. Ми повинні сприяти тому, щоб більше жінок та дівчат знаходили своє місце в кіберсфері, адже їхній потенціал здатний посилити нашу спроможність на всіх рівнях — від оперативних дій до стратегічного планування та ухвалення ключових рішень” (Матеріал №22, 2024).

Ця заява підкреслює цінність гендерної різноманітності як ресурсу в ухваленні рішень. Жінки не просто долучаються до наявної ієрархії — вони змінюють її структуру, привносячи інший тип мислення, що є критично важливим в умовах російсько-української війни.

Важливо зауважити, що ще до початку повномасштабного вторгнення росії в Україну, у 2021 році, було розпочато активну роботу над розвитком кіберзахисту, зокрема з метою створення кібервійськ. Як зазначила Н. Ткачук:

“перед Міністерством оборони України стоїть дуже важлива і необхідна задача побудови кібервійськ”.

“Діяльність кібервійськ зможе стати нашою асиметричною відповіддю агресору” (Матеріал №24, 2021).

Ці кроки стали основою для формування відповідних структур і підготовки кадрів, зокрема жінок, що забезпечили надійний захист національної кіберінфраструктури в умовах війни. Внесок жінок у створення й функціонування кібервійськ може бути вирішальним у контексті стратегічного зміцнення обороноздатності України під час війни.

3.3.5 Жінки як експертки з кібербезпеки

В аналізованих публікаціях медіа були схильні зображати жінок-експерток у сфері ІТ, зокрема кібербезпеки, як рольових моделей, які покликані надихати інших – особливо дівчат – долучатися до галузі. Тобто йшлося про певні історії успіху та подолання бар'єрів:

“Зоя Рашевська, розробниця в компанії ELEKS, спершу була економісткою, а 5 років тому, після декрету, перейшла працювати в ІТ-сферу. Вона розповіла нам про те, яким складним був її шлях в ІТ, про найбільший виклик і щоденну роботу у сфері, де більшість колег — чоловіки” (Матеріал №6, 2021).

Про важливість прикладів успішних жінок-експертів із кібербезпеки згадувалося й у цьому вислові:

“Багато молодих жінок... повоюють галузі, яка традиційно вважається чоловічою... Втім, сьогодні у кібербезпеці працює багато успішних жінок, які можуть поділитись власним натхненням...” (Матеріалі №7, 2023).

Тобто в подібних медіаматеріалах жінки-експертки фігурують не як фонові учасниці, а радше як повноправні та необхідні суб'єкти кіберзахисту, чия участь є не просто бажаною, а стратегічно важливою.

Також показ жінок на відповідальних посадах у сфері безпеки та кібербезпеки (як у Матеріалі №23 (2021), де згадується *“...керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук”*) є важливою складовою гендерно чутливого підходу. Сам факт згадки жінки на такій високій і

відповідальній посаді в ключовому державному органі, що займається питаннями безпеки та кібербезпеки, є безумовно позитивним з погляду підвищення видимості жінок у цій сфері. Це демонструє, що жінки досягають високих рівнів експертизи та займають значущі позиції, що є важливим сигналом для подолання стереотипів про обмежені можливості жінок у “чоловічих” галузях.

Разом із тим, повна гендерна чутливість передбачає не лише змістову репрезентацію, а й уважність до мовного оформлення. Використання форми “керівник” замість фемінітиву “керівниця” може свідчити про вплив традиційних мовних норм або непослідовність медіа, адже використання фемінітивів є технічною ознакою чутливості, що спостерігається в інших матеріалах, зі згадками жінок-лідерок, наприклад, слова “лідерка” (Матеріал №11, 2025) чи “президентка” (Матеріал №34, 2025). Таким чином, показ жінки на посаді є змістовно чутливим, але мовне оформлення — менш послідовним. Це вказує на потребу в глибшій інтеграції гендерно чутливого підходу не лише у змісті, а й у формі медіарепрезентації.

Висновки

Історичний аналіз показує, що, починаючи з ХХ століття, жінки відігравали важливу роль у розвитку комп'ютерних наук та інформаційних технологій, хоча їхній внесок часто недооцінювали або залишали невидимими через панівні гендерні стереотипи. За актуальними даними, жінки залишаються недостатньо представленими у сфері кібербезпеки: їхня частка серед ІТ-фахівців у світі коливається на рівні 24-30%. Першопричини формуються ще на етапі освіти, коли дівчат менше заохочують до вивчення STEM-предметів, що призводить до їхнього меншого представництва на технічних спеціальностях університетів. Міжнародні програми, такі як CyberCorps: Scholarship for Service в США та ініціативи таких організацій, як Women in CyberSecurity (WiCyS), довели свою ефективність у наданні стипендій, менторства та кар'єрної підтримки жінкам, тим самим сприяючи їхньому залученню в галузь кібербезпеки. Крім того, корпоративні програми, такі як Tech Re-Entry від IBM, сприяють реінтеграції жінок після перерв у кар'єрі, надаючи подальшу підтримку у їхньому професійному зростанні. Ці зусилля в сукупності підкреслюють важливість постійних багаторівневих заходів – від ранньої освіти до розвитку кар'єри – для подолання гендерного дисбалансу на ринку праці у сфері кібербезпеки.

Кібербезпека, як галузь, де переважають чоловіки, зберігає значний гендерний дисбаланс через низку соціокультурних, освітніх та інституційних бар'єрів, включаючи стереотипи, упередженість під час працевлаштування та недостатню підтримку жінок у професійному середовищі. Ці фактори, посилені феноменом "leaky pipeline", обмежують залучення та утримання жінок у галузі, що є особливо критичним в умовах дефіциту кадрів у сфері кібербезпеки. Врахування гендерного розмаїття та збільшення представництва жінок у сфері є стратегічно важливим для підвищення ефективності кіберзахисту та інноваційного розвитку галузі в умовах сучасних кіберзагроз. Це підтверджує необхідність систематичного впровадження гендерно чутливих політик у сфері кібербезпеки.

Успішні стратегії подолання бар'єрів у кібербезпеці базуються на поєднанні мікро-, мезо- та макрорівневих механізмів: від індивідуальної підтримки та рольових моделей до інституційних трансформацій в освіті (університетські програми та спеціалізовані курси CyberFirst, Women4Cyber та ін.), корпоративних програм (Google, Microsoft, IBM) і державних політик (квоти, гнучкі графіки, реінтеграція після декрету), спрямованих на створення гендерно чутливого середовища та усунення структурної дискримінації. Водночас важливим аспектом є боротьба з глибоко вкоріненими гендерними стереотипами в суспільстві щодо ролі жінок у технологічних галузях. Саме ці стереотипи, які визначають кібербезпеку як "чоловічу" сферу, створюють структурні бар'єри для входження та кар'єрного розвитку жінок і підтримують гендерну сегрегацію в галузі.

У результаті дослідження статистичної інформації щодо жінок у сфері кібербезпеки в роботі й освіті були виявлені спільні тенденції як на міжнародному рівні у сфері праці та освіти, так і в українській освіті. Головною тенденцією є явна горизонтальна гендерна сегрегація сфери, де частка жінок в середньому складає

<30%. В міжнародній сфері найбільшу частку жінок серед регіонів світу має Північна та Південна Америка, коли найменшу — Африка. В той же час у деяких країнах, таких як Нігерія та Мексика, частка зайнятих у кібербезпеці жінок може досягати третини від загальної кількості. У сфері української освіти, в обраних для аналізу університетах, середня частка жінок в навчанні на спеціальності 125 “Кібербезпека” складала меншість, в середньому 26%.

Поряд із тим наявна тенденція до зростання частки жінок у сфері кібербезпеки. На глобальному рівні це підтверджується гендерно-віковою структурою: жінки у віці <30 років складають 24% від загальної кількості працівників, що на 9% більше в порівнянні з часткою жінок у віковій категорії 40+. Аналогічні зміни можна побачити в українських закладах вищої освіти, де частка жінок на першому курсі навчання в закладах вища, ніж на старших курсах. Однак ця тенденція не є повсюдною і може мати різні пояснення. Вона може бути обумовлена як об'єктивними чинниками, такими як російське повномасштабне вторгнення в Україну у 2022 році, так і внутрішніми процесами закладів освіти, наприклад, систематичним відрахуванням студенток на старших курсах або іншими причинами.

Наразі в світі, в межах кібербезпеки, жінки вже в середньому мають кращу освіту за чоловіків. Дані з українських ЗВО також кажуть про кращі оцінки жінок, порівняно з чоловіками. Однак у світі жінки все ще мають меншу заробітну плату, ніж чоловіки, на тих самих позиціях і займають тільки 16% від всіх керівних посад, що вказує на потребу в додаткових заходах для подолання горизонтальної і вертикальної сегрегацій.

Одним із можливих рішень може бути сприяння залученню жінок до програм, що надають початкові освітні ступені, необхідні для кар'єри у кібербезпеці, такі як ступінь молодшого спеціаліста або базова вища освіта. Це дозволить жінкам займати позиції в тих підпрофесіях, де вони наразі недостатньо представлені. На відміну від збільшення частки жінок із магістерськими та докторськими ступенями, які нерідко залишаються нереалізованими в професійній сфері, така стратегія може сприяти реальному зменшенню гендерного дисбалансу.

Отже, у сфері кібербезпеки наявний значний гендерний розрив, попри позитивні тенденції останніх років до підвищення зацікавленості та залученості жінок. Це свідчить про потребу продовження активних заходів для досягнення повної гендерної рівності.

Попри поступове усвідомлення важливості інтеграції жінок, цей процес характеризується певною суперечливістю, хоча й демонструє значні успіхи. Так, у чинній нормативно-правовій базі помітні прогресивні елементи: Закон України “Про забезпечення рівних прав та можливостей жінок і чоловіків” закріплює обов'язок державних органів впроваджувати гендерну рівність та надає інструмент гендерно-правової експертизи, тоді як Закон “Про запобігання та протидію дискримінації” формалізує можливість юридичного оскарження дискримінаційних практик. Доповнює ці норми загальний принцип недискримінації, закладений у профільному Законі “Про основні засади забезпечення кібербезпеки України”. Не менш вагомими є позитивні зрушення у напрямку підтримки жінок, ініційовані державою, громадськістю та бізнесом. Наприклад, Національний координаційний

центр кібербезпеки активізував підтримку жіночого лідерства, а включення гендерних аспектів до Національного плану дій з виконання резолюції РБ ООН 1325 відкрило жінкам доступ до спеціалізованого навчання та участі у формуванні політик. Також, розвиваються платформи на кшталт SheCyber Hub, Women4Cyber Ukraine, CDTO Campus реалізуються програми перекваліфікації, подібні до "Reskilling Ukraine", та впроваджуються лідерські й менторські програми від міжнародних партнерів. IT-компанії також демонструють прихильність до політик DEI, а міжнародні корпорації запускають освітні проєкти для жінок, зокрема тих, хто постраждав від війни, що разом створює сприятливіші умови для професійного зростання.

Не дивлячись на досягнуті успіхи, шлях до гендерної інтеграції в українській кібербезпеці ускладнений системними проблемами. Передусім, занепокоєння викликає недостатня гендерна чутливість ключових нормативно-правових актів: вони часто декларують нейтральність, проте оминають увагою специфічні цифрові загрози для жінок, зокрема кібернасильство, сексторшен та онлайн-переслідування. Чинні механізми реалізації антидискримінаційного законодавства, на жаль, демонструють низьку ефективність через брак чітких процедур та належної інституційної підтримки. Також стратегічні документи, включно з Планом реалізації Стратегії кібербезпеки, здебільшого ігнорують гендерний вимір, підкреслюючи домінування технократичного підходу над інклюзивним баченням. Суттєвою перепорою залишаються глибоко вкорінені структурні бар'єри: стійкі гендерні стереотипи щодо "нежіночого" характеру професії, засилля неформальних чоловічих професійних мереж та так званий ефект "скляної стелі" продовжують обмежувати кар'єрне зростання жінок, особливо на технічних і керівних посадах. До цього додаються виразні прояви горизонтальної та вертикальної гендерної сегрегації, а також значний гендерний розрив в оплаті праці, який не виявляє стійких тенденцій до скорочення. Освітня сфера також стикається з викликами, серед яких недостатність спеціалізованих програм технічної підготовки, орієнтованих на жінок, та брак формалізованих менторських мереж. Зрештою, критичною проблемою є дефіцит системних, гендерно-дезагредованих даних та комплексних досліджень стосовно становища жінок в українському секторі кіберзахисту, особливо в умовах війни. Ця інформаційна прогалина суттєво ускладнює розробку обґрунтованої політики та моніторинг її ефективності.

Зазначені системні проблеми та успіхи набувають особливої динаміки в умовах повномасштабної війни росії проти України, яка стала каталізатором суперечливих трансформацій. З одного боку, екстремальні обставини та кадровий дефіцит дійсно відкрили певні "вікна можливостей" для жінок, посиливши їхню присутність та видимість у секторі кібербезпеки. Проте, з іншого боку, мілітаризація суспільного дискурсу та економічні потрясіння ризикують поглибити вже наявні вразливості й зміцнити традиційні гендерні стереотипи, що додатково ускладнює шлях до рівності. В цих умовах, для досягнення сталої гендерної рівності та ефективного використання потенціалу всіх фахівців задля зміцнення національної кіберстійкості, критично необхідним є комплексний та стратегічно виважений підхід. Це вимагає не лише продовження програм підтримки, а насамперед системної інтеграції гендерних перспектив у законодавство, освітні стандарти, формування інклюзивних

корпоративних культур, та, що особливо важливо, налагодження систематичного збору й аналізу гендерно-дезагредованих даних для розробки доказової політики та дієвого моніторингу її результатів.

У підсумку, це дослідження засвідчило, що жінки у сфері кібербезпеки в Україні можуть стикатись з комплексом структурних та символічних перешкод, що можуть початися ще на етапі входження в професію і бути присутніми протягом кар'єрного шляху. Низка респонденток зазначали, що не мали досвіду дискримінації, але мали підтримку на робочому місці, проте ці позитивні приклади можуть бути радше винятками, ніж усталеною нормою. Найпоширенішими перешкодами були зазначені сумніви в професійності респонденток, знецінення знань, гендерні стереотипи під час співбесід та відсутність реакції компанії на дискримінаційні дії.

Проте, як і зазначалось раніше, респондентки також відмічали поступові позитивні зрушення в цьому питанні. Зростає кількість жінок у навчальних групах і компаніях, з'являється більше освітніх та менторських ініціатив, а також прикладів підтримки з боку колег та керівництва. Деякі респондентки зазначили про формування рівноправного середовища в окремих організаціях, що може свідчити про потенційні позитивні зміни.

Отже, створення інклюзивного та комфортного середовища у сфері кібербезпеки вимагає комплексного підходу – від змін на інституційному рівні, до особистої впевненості та активності жінок. Усі запропоновані рекомендації мають на меті подолати структурні перешкоди, знизити вплив гендерних стереотипів та сприяти професійному розвитку жінок. Однак поряд із зовнішніми змінами, надзвичайно важливою залишається внутрішня стійкість і віра у власні сили.

Отже, за результатами аналізу експертних інтерв'ю щодо успіхів і викликів залучення жінок у сферу кібербезпеки в часи російсько-української війни визначено виклики та успіхи у доступі, представленості та підтримці жінок у сфері кібербезпеки. Серед викликів та проблем: горизонтальна та вертикальна сегрегація; психологічна напруга та підвищений рівень відповідальності, що пов'язані з гендерними стереотипами й упередженнями щодо ролей чоловіків та жінок у суспільстві; гендерний розрив в оплаті праці; сексуальні домагання, часто у форматі "особливого ставлення" до жінок на робочих місцях, зокрема у державних установах; необізнаність та/або неефективність щодо впроваджуваних ініціатив та реформ, зокрема на державному рівні.

До ключових успіхів належать: покращення доступності та представленості жінок у сфері кібербезпеки; збільшення кількості жінок, що займають провідні/керівні посади; наявність позитивних жіночих ролевих моделей та поширення обізнаності про них; розвиток менторських програм та тренінгів для жінок; впровадження ініціатив та реформ для підтримки жінок сфери кібербезпеки на державному рівні; зменшення схильності до гендерних упереджень серед молодого покоління в Україні.

Основними рекомендаціями респондент(ок)ів стали: створення та впровадження програм менторства та наставництва; проведення інформаційних кампаній на всіх рівнях освіти; розвиток професійної та інклюзивної спільноти;

заохочення жінок до участі у різних подіях та проєктах; стипендії та гранти для студенток; підтримка жіночих рольових моделей.

Застосування якісного тематичного аналізу в межах інтерпретативного підходу дало змогу отримати глибоке розуміння того, як українські медіа репрезентують участь жінок у сфері кібербезпеки. Тематичний аналіз, як гнучкий інструмент дослідження якісних даних, дозволив не лише структурувати великий масив інформації, а й виявити ключові патерни змісту, зосереджені на питаннях гендерної рівності, професійної ідентичності та соціального визнання жінок у високотехнологічному секторі.

Вибірка була багатоступеневою: відбір одиниць аналізу проводився в чотири етапи, що дозволило сформувати репрезентативну базу даних. З 710 початково ідентифікованих медійних одиниць на завершальному етапі до вибірки увійшло 44 матеріали (опубліковані за період з 2017 по 2025 рік). Їхній аналіз здійснювався за допомогою тематичного кодування, що дало змогу виявити ключові теми: 1) Жінки в ІТ та кібербезпеці на ринку праці: залучення та гендерна (не)рівність. 2) Освітні програми для жінок у сфері кібербезпеки. 3) Жінки у військовій кібербезпеці та обороні. 4) Жінки як експертки з кібербезпеки. Комбінація автоматизованого пошуку через платформу Shukach Pro та подальшого ручного очищення вибірки дала змогу сформувати релевантне та якісне джерело даних для подальшого аналізу. Чітко визначені етапи формування вибірки дозволили уникнути випадкового включення нерепрезентативних або поверхневих матеріалів, натомість забезпечивши глибоке охоплення тематики.

У межах дослідження було обрано егалітарний підхід до аналізу репрезентацій жінок у сфері кібербезпеки, оскільки в процесі аналізу не було виявлено медіаматеріалів, які б демонстрували відверті прояви гендерної нерівності або стереотипного зображення жінок. Натомість проаналізовані публікації фокусувалися переважно на підтримці, посиленні ролі жінок, просуванні освітніх ініціатив і подоланні бар'єрів участі, що загалом відповідає принципам гендерної рівності й інклюзії.

Застосування якісного тематичного аналізу медіа виявило дві основні тенденції: гендерно чутливий підхід (акцент на нерівності, жіночому досвіді та структурних бар'єрах) та гендерно нейтральний (фокус на професійних якостях без акценту на статі).

Медіа порушують питання недопредставленості жінок у кібербезпеці, зокрема у військовій сфері (де їхня частка сягає лише 6%), а також висвітлюють ініціативи з їхньої підтримки – менторські програми, квоти, освітні курси. Менторські програми – проєкт USAID для студенток спеціальності "Кібербезпека", де досвідчені фахівчині допомагають у професійному розвитку. Квоти – позитивна дискримінація в ІТ-компаніях, наприклад, прийом жінок для зменшення гендерного дисбалансу; законодавча заборона вказувати гендер у вакансіях законом України 2005 року. Освітні курси – вебінар для студенток (Матеріал №9, 2023), де кібер-експертки розповідають про свій досвід та надихають дівчат обирати кар'єру в кібербезпеці. А також заходи на кшталт Національного дня дівчат в технологіях для знайомства з STEM-професіями.

Однак є й публікації, у яких жінок все ж зображено як “доповнення” до чоловіків, або в яких ігнорують фемінитиви.

Важливим кроком до рівності є руйнування гендерних стереотипів ще на рівні освіти, профорієнтація дівчат і створення умов для їх кар’єрного зростання. Позитивним трендом є зростання кількості матеріалів, де жінки представлені як експертки з кібербезпеки та лідерки, що сприяє формуванню нових соціальних норм.

У процесі дослідження медіа показали себе не лише як дзеркало суспільних процесів, а і як агенти соціальних змін. Вони займають вагоме місце в трансформації уявлень про професійні можливості жінок у стратегічно важливих галузях, зокрема в умовах повномасштабної війни, де кібербезпека відіграє важливу роль.

Рекомендації

Рекомендації щодо покращення становища жінок у кібербезпеці

У результаті інтерв'ю було визначено рекомендації компаніям та жінкам у сфері кібербезпеки. Рекомендації компаніям стосувалися створення сприятливого робочого середовища для жінок, а рекомендації жінкам – особистого розвитку у кібербезпеці.

Одним із механізмів, які компанії можуть застосовувати для покращення становища їхніх співробітниць, є рівне ставлення до жінок та чоловіків на робочому місці, що включає відсутність гендерно зумовлених вимог чи очікувань, а також рівну оплату праці.

“Я просто кажу про те, що найкраще ставлення до жінок, це ставлення таке, як і не то, що до чоловіків, щоб було рівне ставлення до всіх. Тобто не має бути жінка-чоловік, має бути просто фахівець” (Респондентка 2).

“Я знаю, є прям компанії, які не доплачують жінкам. Насправді це доволі дивно. Не доплачувати жінкам у нашій сфері. Треба просто, щоб була однакова цінність людини” (Респондентка 8).

Респондентки також радили збільшити кількість жінок у компаніях, як один із способів подолання гендерних стереотипів щодо непрофесійності жінок у кібербезпеці. Безпосередня взаємодія з жінками у командах дозволяє колегам сформулювати об'єктивне уявлення про їхню компетентність. Крім того, активніше залучення жінок у цю галузь підвищує їхню видимість у суспільстві загалом, що сприяє переосмисленню кібербезпеки як виключно “чоловічу сферу”.

“Загалом, я думаю, що чим більше жінок в компанії працює, тим менше сексизму. Тому що чоловіки напряду бачать жінку, яка працює в цій професії і все круто. Вона там нічого не ламає, вона не прийшла псувати всім життя” (Респондентка 4).

Збільшення присутності жінок у кібербезпеці можливе завдяки впровадженню заходів, які мотивують жінок працювати у цій сфері. По-перше, компанії можуть поширювати інформацію про можливості навчання та роботи у цій галузі серед школярок. Дівчата можуть не розглядати кібербезпеку як потенційну сферу зайнятості через гендерні стереотипи, що ототожнюють її з “чоловічою”. Відповідно, освітні заходи та інші програми можуть дозволити дівчатам дізнатися про переваги роботи у цій галузі та сприяти формуванню інтересу до неї.

“Обізнаність. Кібербезпека – це дуже така сфера обширна, де потрібні люди з дуже різноманітними навичками. Як я казала на початку. І я б піднімала обізнаність в цьому плані серед дівчат, які обирають, де їм навчатись. Бо це не просто популярна, актуальна сфера. Вона також дуже цікава і дуже

корисна загалом для суспільства. Тому я б, напевно, проводила якісь профорієнтаційні заходи.” (Респондентка 3)

По-друге, компанії можуть мотивувати та підтримувати студенток кібербезпеки шляхом проведення конференцій, які дозволяють жінкам демонструвати свої професійні навички та досягнення, а також запровадження грантових програм (Респондентка 1). Крім того, частина респонденток наголошувала на важливості наставни(ць)ків у їхньому професійному розвитку. Тому впровадження програм менторства в компаніях може бути ефективним механізмом підтримки та адаптації співробітниць.

“Якби я мала можливість щось змінити, то напевно акцентувала б увагу на розвитку менторської культури та підтримки. Часто жінкам у цій сфері просто не вистачає прикладів підтримки чи впевненості. Створення спільнот, відкритих майданчиків для обміну досвідом і внутрішніх корпоративних програм менторства могло б суттєво вплинути на розвиток рівних можливостей” (Респондентка 5).

Окрім залучення більшої кількості жінок у сферу кібербезпеки, респондентки наголошували на важливості розроблення чітких стратегій формування сприятливого робочого середовища, зокрема, йдеться про створення планів навчання співробітни(ць)ків та ефективних механізмів реагування на випадки дискримінації:

“Компаніям порадила б звернути увагу не лише на гендерне різноманіття, а й створювати реальні умови для балансу: гнучкий графік, програми розвитку, безпечне та поважне середовище, також чіткі механізми реагування на дискримінацію” (Респондентка 5).

Респондентки також надали поради безпосередньо для жінок, які працюють у галузі кібербезпеки – незалежно від їхнього професійного досвіду. Одним із ключових моментів стала необхідність зниження рівня страху перед новими викликами та готовністю проявити себе. Зазначалося, що жінки часто бояться брати участь у конкурсах і заходах, таких як STF або багбаши, через невпевненість у своїх силах. Саме тому важливо підтримувати жінок і заохочувати їх до активної участі в таких заходах, щоб підвищити впевненість у своїх здібностях.

“Дуже заохочувати жінок проявляти себе і показувати себе на змаганнях, на STF-ах, в багбашах, тому що це дуже корисно, і це дуже багато жінок бояться STF-и і багбаши, через якраз таке відчуття, що вони типу, що вони недостатні, що недостатньо щось, типу, вміють” (Респондентка 1).

Також акцентувалось на важливості не боятися невдач, адже вони є частиною процесу навчання і розвитку. Респондентки підкреслювали, що зневіра і страх – це нормальні емоції на шляху до успіху. Страх не повинен зупиняти, а навпаки – мотивувати до подолання перешкод.

“...не боятися. Тому що страх, це завжди буде перше, що, типу, зупиняє тебе. Бо якщо б я сиділа і боялась, я би не потрапила на співбесіду, я би не потрапила в Могилянку, я би не пройшла НМТ” (Респондентка 1).

“Якщо ти боїшся чогось, то це не означає, що це не твоє. Це якраз таки означає, що це твоє. І що ти хочеш це робити. І хочеш робити це добре. Тому зневіра і страх – це нормально. І не треба боятися страху” (Респондентка 3).

Респондентки наголошували на наполегливості, впевненості у собі та постійному розвитку для досягнення успіху в кібербезпеці. Наполегливість у виконанні професійних завдань та впевненість у своїх власних силах дозволяють подолати перешкоди, які часто виникають через страх перед невідомим чи новими викликами.

“Бути максимально наполегливими й не боятися поразок. Не варто здаватися після кількох невдалих співбесід” (Респондентка 6).

Крім того, респондентки підкреслюють важливість безперервного навчання та розвитку професійних навичок. Вони радять постійно шукати нові можливості для підвищення кваліфікації та підтримувати зв'язки з професійною спільнотою через участь у тренінгах, конференціях та інших заходах.

“Завжди шукати щось нове для себе, дізнаватися, спілкуватися з людьми, бути активною учасницею, ходити на форуми різноманітні, брати участь в конференціях” (Респондентка 9).

Рекомендації для компаній:

- забезпечувати рівне ставлення до жінок і чоловіків на робочому місці, включаючи рівну оплату праці за однакову кількість роботи;
- збільшення кількості жінок у компаніях в сфері кібербезпеки для подолання гендерних стереотипів і підвищення їхньої видимості в суспільстві;
- поширення інформації про можливості навчання та роботи у кібербезпеці серед школярів для зменшення стереотипів щодо цієї професії і упередженого ставлення;
- проведення конференцій, освітніх заходів і грантових програм, спрямованих на мотивацію і підтримку жінок у кібербезпеці;
- розроблення чітких стратегій для створення сприятливого робочого середовища, включаючи програми навчання, гнучкі графіки і механізми реагування на дискримінацію.

Рекомендації для менторів:

- впровадження менторських програм у компаніях для підтримки та адаптації жінок в сфері кібербезпеки;

- створення спільнот та майданчиків для обміну досвідом та підтримки між жінками у професійному середовищі.

Рекомендації для жінок, що планують йти в сферу кібербезпеки:

- активно приймати участь у професійних заходах, для підвищення впевненості у своїх здібностей і професійному розвитку;
- не боятись нових викликів і приймати участь у конкурсах і заходах як засіб для особистого і професійного зростання;
- бути наполегливою та готовою до викликів, що допомагає подолати страх перед невдачами і розвиватись професійно.

Рекомендації щодо доступу жінок до сфери кібербезпеки в Україні: освітні чинники

Експерт(к)и також поділилися своїми рекомендаціями щодо доступу жінок до сфери кібербезпеки в Україні. Таким чином, було виділено три основні категорії рекомендацій: зміни в освіті, як середній і вищій, так і додатковій; покращення поінформованості щодо сфери кібербезпеки, зокрема серед дівчат то жінок; формування та підтримка спільнот для професійної взаємодії та розвитку жінок у цій галузі.

“Мені здається, якісь історії треба ще в садочку, в школі змінювати, бо там коли в підручнику бачиш задачі по математиці: Василь зібрав годинник, а Маша збрала яблука в саду. Воно йде змалечку, закладаються ці стереотипи, упередження.”
(Респондент 5)

Результати експертного інтерв'ювання виявили, що **освітня складова** доступу жінок до сфери кібербезпеки в Україні займає центральне місце серед рекомендацій. Одним з ключових напрямів думок є зміна підходу до **формування уявлень про гендерні ролі та можливості з раннього віку**. У шкільній освіті важливо боротися зі стереотипами через коригування навчальних матеріалів та впровадження інформаційних кампаній, які демонструють дівчатам можливості в технологічній сфері. Респондент(к)и зазначають, що залучення учнів ще у школах до ознайомлення з можливостями розвитку у сфері кібербезпеки сприятиме формуванню інтересу та позитивного сприйняття цієї галузі незалежно від статі:

“Тобто яюсь в школі можливо розказувати на інформатиці, що існує така сфера взагалі.” (Респондентка 2).

Говорячи про вищу освіту, респондент(к)и підкреслили **необхідність активізації процесів оновлення освітніх програм**, що передбачає інтеграцію сучасних практик та безпосереднє залучення спеціаліст(ок)ів з кібербезпеки у викладання. Важливо виділили створення та впровадження грантових програм та спеціальних стипендій для жінок, що слугуватиме додатковим стимулом для залучення жінок та поглибленого вивчення цієї сфери. Водночас, респондент(к)и

акцентують увагу на потребі структурованих змін у вищій освіті, зокрема модернізації навчальних підходів та посиленні зацікавлені викладачів у підготовці висококваліфікованих фахівців.

“Друге [з інновацій на державному рівні] – це змінити освітню систему. І це проблема не тільки залучення дівчат, а загалом усієї системи освіти з Тому що те, що ми маємо зараз – це застарілі умови та викладачі, які часто не зацікавлені вкладати зусилля у навчання навчати студентів. Насправді є лише декілька університетів, які дійсно готують крутих фахівців і вкладають в своїх студентів.” (Респондентка 13).

Післядипломна освіта та професійне навчання виділяються як важливі інструменти подальшого кар'єрного розвитку жінок у сфері кібербезпеки. Особливо респондент(к)и виділяють менторство як ключовий компонент професійного розвитку. Респондент(к)ами було запропоновано активно впроваджувати наставницькі програми, які б допомагали жінками долати кар'єрні та психологічні бар'єри та набувати впевненості у своїх силах. Власним досвідом поділилася одна Респонденток, розповівши, як її менторка допомогла їй змінити ставлення до своєї кар'єри та викликів, з якими вона стикалася:

“У мене менторка була колишня генеральна директорка Майкрософту України. І це класно, тому що ти можеш по-іншому подивитися на свою кар'єру, на виклики, за якими працюєш, попросити поради в тій чи іншій сфері, зрозуміти, що це нормально, люди зіштовхуються з такими викликами в такому-то віці або з такими-то справами.” (Респондентка 11).

Тобто респондент(к)и звернули увагу на те, наскільки інституція освіта відіграє вирішальну роль як і у підтримці жінок у сфері кібербезпеки, так і розвитку сфери загалом, та запропонували шляхи, якими залучення жінок може покращити сферу загалом.

Рекомендації щодо доступу жінок до сфери кібербезпеки в Україні: обізнаність про сферу та можливості жінок

“Чим більше ти бачиш можливостей, ти будеш більше йти.”

(Респондентка 11)

Рекомендації респондент(ок)ів щодо підвищення поінформованості про сферу кібербезпеки та доступ до неї жінок в Україні охоплюють кілька ключових напрямків. На загальному рівні було запропоновано **активізувати інформаційні кампанії**, спрямовані на руйнування гендерних стереотипів та популяризацію кібербезпеки як доступної галузі для жінок. Респондент(к)и наголосили на важливості розвитку фахових медіа, які б забезпечували якісну і доступну інформацію про сферу як для фахівців, так і для широкого загалу. Також, проведення відкритих конференцій та форумів, спрямованих на молодь, сприятиме формуванню спільноти для молоді та

зниженню інформаційних бар'єрів для входження у сферу. Один з Респондентів звернув увагу на необхідність змін у суспільному ставленні до жінок, звертаючи увагу на те, що воно впливає на всі аспекти досвіду жінок:

“Ну, перш за все має змінюватися суспільна думка, щоб не було упереджень щодо жінок, і законодавчі інструменти - вони вже вторинні, які будуть доносити цю думку.” (Респондент 5).

Особливо респондент(к)и наголошували на ініціативах та реформах, щодо **обізнаності про сферу зі школярством та студентством**. Серед пропозицій згадувались такі, як створення спеціальних стипендіальних програм та залучення дівчат до змагань з кібербезпеки. Також, один з Респондентів звернув увагу на важливість роботи з батьками у процесі професійного орієнтування дівчат, оскільки думки серед батьків на кшталт *“Ой, ну кібербезпека це не дуже жіноча справа, краще програмістом будь”* (Респондент 7) залишаються актуальними. Також важливим аспектом зазначали активне впровадження раніше згаданих програм наставництва та менторства, що зможуть підтримувати молодих жінок на етапах навчання та початку кар'єри.

Щодо безпосередніх заходів заохочення фахівчинь, респондент(к)и також рекомендували посилити **можливості для стажувань у державних та приватних установах**, регулярне проведення хакатонів, STF-змагань зі спеціальною участю жіночих команд, а також більше залучення жінок до міжнародних проєктів для обміну досвідом та набуття практичних навичок. Державна підтримка, зокрема фінансування навчальних програм та впровадження податкових пільг для компаній, що активно залучають жінок, була підкреслена як ефективний стимулюючий фактор:

“Це звичайно, податкові пільги, які будуть працювати для компаній, які наймають жінок в кіберсфері, держфінансування курсів для початківців у кібербезпеці, освітні програми з менторства і тому подібні програми.” (Респондент 3).

Багато респондент(ок)ів також звертали увагу на важливості **представленості рольових моделей жінок в інформаційному просторі**. Було виділено такі аспекти, як активніше висвітлення успішних прикладів жінок у сфері кібербезпеки, проведення цілеспрямованих інформаційних кампаній, які б демонстрували досягнення жінок та їх активну участь у сфері. На думку респондент(ок)ів, це сприятиме подоланню міфів та стереотипів, які існують в суспільстві, та підвищуватиме видимість жінок у сфері кібербезпеки. Одна Респондентка поділилася своїми особистими бажаннями та переживаннями, щодо важливості привернення уваги до жінок у сфері:

“Більше показувати, підсвічувати рольові моделі, тобто успішних жінок. Я б хотіла, щоб журналісти зверталися за коментарями саме до жінок, щоб показати, що вони існують у нашій сфері, щоб їхнім досягненням пишалися і підсвічували їх, а не навпаки робили цю історію як тіньовою “є і є - добре, що

працюють”. (Респондентка 13).

Рекомендації щодо доступу жінок до сфери кібербезпеки в Україні: спільнота та підтримка жінок

“Чесно, от чого мені зараз дуже бракує в Україні, це професійного ком'юніті.”
(Респондентка 11)

Респондент(к)и також звернули увагу на важливість **створення та підтримки професійної спільноти жінок у сфері кібербезпеки**, наголошуючи про необхідність сприятливого середовища для взаємодії та професійного розвитку. Зокрема, вони відзначали важливість формування інфраструктури, що надасть можливість фахівчиням об'єднуватись та обмінюватись знаннями та досвідом. Однією з таких рекомендацій стала пропозиція регулярно організовувати відкриті форуми та конференції, які будуть доступними для молодих спеціалістів. Додатково, було запропоновано створити веб-портал з інформаційними ресурсами, що сприятиме включенню нових учасників, особливо жінок, у професійну спільноту. Респондент(к)и підкреслювали важливість заохочення жінок приєднуватись до існуючих жіночих спільнот і брати участь у різних подіях на державному рівні:

“Знаєте, я б тут, мабуть, сказала, що на державному рівні треба звертати увагу на саме розбудову певного нетворкінгу щодо жінок у сфері кібербезпеки. Чому? Бо ми зазвичай звикли до того, що якщо проводиться якийсь хакатон, якщо проводиться якийсь айти конкурс тощо, то зазвичай приймають участь одні хлопці.” (Респондентка 6).

Окремо респондент(к)и наголошували на важливості **підтримки жінок всередині самої спільноти**. Окрім вже неодноразово згаданих практик менторства та наставництва, виділяють також створення гнучких умов праці, залучення жінок до керівних посад, проведення заходів, спрямованих на боротьбу з гендерно зумовленим насильством та забезпечення прозорих умов праці, включаючи відкритість інформації про заробітну плату. Таким чином, респондент(к)и підкреслюють важливість уваги до жінок, їх викликів та успіхів у самій спільноті. Одна Респондентка наголосила на тому, що така стратегія дозволить попереджати випадки дискримінації та упередженого ставлення до жінок:

“Можливо дослухатися до них, якщо все ж такі жінки розповідають, що з ними щось трапилося на роботі саме через те, що вони жінки, то аби керівництво мало це на увазі і якимось... попереджали такі випадки, щоб у наступний раз нічого такого не ставалося, не дай Боже.” (Респондентка 12).

Список використаних джерел

1. Аналітичний центр Асоціації жінок-юристок України “Юрфем”. (2023). Гендерний вимір війни: Аналітичне дослідження. Асоціація жінок-юристок України. <https://jurfem.com.ua/wp-content>
2. Вступ 2024. (2024). Рейтинговий список вступників на перший курс денної форми навчання за освітньо-професійною програмою підготовки бакалавр за спеціальністю 125 “кібербезпека та захист інформації” до Національного університету “Львівська політехніка”. <https://vstup2024.lpnu.ua/detail/22/25206/8/1>
3. Вступ до НАУКМА. (2024). Рейтинговий список вступників за освітньо-професійною програмою підготовки бакалавра, на спеціальність 125 “кібербезпека та захист інформації” у 2024 році. <https://konkurs.ukma.edu.ua/#2024/spec/1378844>
4. Вступ.Освіта.UA. (2024). Кібербезпека та захист інформації, бакалавр. <https://vstup.osvita.ua/y2024/r4/44/1303791/>
5. Громадський Простір. (2023). “Гендерне різноманіття в кібербезпеці: реалії та можливості для жінок в Україні”: відбувся Діалог в межах програми “Діалог про кібербезпеку”. <https://www.prostir.ua/?news=genderne-riznomanittya-v-kiberbezpetsi-realiji-ta-mozhlyvosti-dlya-zhinok-v-ukrajini-vidbuvsya-dialoh-v-mezhah-prohramy-dialoh-pro-kiberbezpeku>
6. Департамент навчально-виховної роботи КПІ ім. Ігоря Сікорського. (2024). Рейтинг успішності студентів Фізико-технічного інституту (ФТІ) за результатами зимового семестрового контролю 2024/2025 н.р. <https://dnvr.kpi.ua/2025/02/05/%D1%80%D0%B5%D0%B9%D1%82%D0%B8%D0%BD%D0%B3-%D1%83%D1%81%D0%BF%D1%96%D1%88%D0%BD%D0%BE%D1%81%D1%82%D1%96-%D0%B7%D0%B8%D0%BC%D0%B0-2024-2025/>
7. Державний університет інформаційно-комунікаційних технологій. (2024). Рейтинговий список студентів ННІ кібербезпеки та захисту інформації(за осінній семестр 2024-2025 н.р.). <https://duikt.edu.ua/ua/1890-reyting-studentiv-navchannya>
8. Довгань, О. (2023). Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест. Київ: Інститут інформації, безпеки і права НАПРН України.
9. DOU. (2022). Менторська програма для студенток спеціальності “Кібербезпека”. <https://dou.ua/calendar/44411/>

10. DOU. (2022, 10 березня). Портрет IT-спеціаліста 2022: Де працюють, скільки заробляють і які перспективи? <https://dou.ua/lenta/articles/portrait-2022/>
11. DOU. (2022, серпень). USAID Cybersecurity Activity: менторська програма для студенток кібербезпеки. <https://dou.ua/events/usaids-cybersecurity-mentoring-2022>
12. DOU. (2023, 16 травня). Вебінар “Побудова кар’єри жінок у сфері кібербезпеки: рекомендації та поради успішних професіоналок”. <https://dou.ua/calendar/47133/>
13. DOU. (2023, травень). Побудова кар’єри жінок у сфері кібербезпеки: рекомендації та поради успішних професіоналок. <https://dou.ua/events/building-women-cybersecurity-2023>
14. DOU. (2024). Жінки в українській IT-індустрії: як змінюється гендерний баланс та роль жінок. <https://dou.ua/lenta/articles/women-in-ukrainian-tech-industry-2024/>
15. Жерьобкіна, Т., Кабанець, Ю., Куделя, М., Ломоносова, Н., Назаренко, Ю., Слободян, О., & Філіпчук, Л. (2021). Досвід Cedos: соціальні дослідження для суспільних трансформацій (р.76-77). Київ: Аналітичний центр Cedos.
16. Іпполітова, І. (2023, 23 травня). Рейтинг IT-вишів 2023. <https://dou.ua/lenta/articles/ukrainian-universities-2023/?from=strichan>
17. Київська міська державна адміністрація. (2022). Звіт про виконання Національного плану дій з виконання резолюції Ради Безпеки ООН 1325 "Жінки, мир, безпека" на період до 2025 року. https://media-stg.kyivcity.gov.ua/kyivcity/sites/26/2024/08/29/zvit2_1325_do2025za2022.pdf
18. Маерчик, М., Плахотнік, О., Ярманова, Г. (ред.). (2017). Гендер для медій: Підручник із гендерної теорії для журналістики та інших соціогуманітарних спеціальностей (3-є вид., випр. і доп.). Критика.
19. Марценюк, Т. (2019). Інтеграція гендерної складової в аналітичні матеріали. МФ “Відродження”, с. 8-11.
20. Офіційний Вебпортал Парламенту України. (2005). Про забезпечення рівних прав та можливостей жінок і чоловіків <https://zakon.rada.gov.ua/laws/show/2866-15>
21. Офіційний Вебпортал Парламенту України. (2012). Закон України “Про засади запобігання та протидії дискримінації в Україні” № 5207-VI від 6 вересня 2012 року. <https://zakon.rada.gov.ua/laws/show/5207-17>
22. Офіційний Вебпортал Парламенту України. (2017). Закон України “Про основні засади забезпечення кібербезпеки України” № 2163-VIII від 5 жовтня 2017 року. <https://zakon.rada.gov.ua/laws/show/2163-19>
23. Офіційний Вебпортал Парламенту України. (2021). Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року “Про План

- реалізації Стратегії кібербезпеки України” № 37/2022.
<https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>
24. Приймак, К. (2021). Бар’єри кар’єрного зростання, з якими зіштовхуються жінки під час служби в Збройних Силах України (дипломна робота).
<https://publications.kse.ua/publications/barieri-kariernogo-zrostannia-iakimi-zishtovkhuiutsia-204>
 25. Офіційний Вебпортал Парламенту України. (2014, 1 липня). Про вищу освіту.
<https://zakon.rada.gov.ua/go/1556-18>
 26. Проєкт USAID "Кібербезпека критично важливої інфраструктури України". (2023). Рекомендації для подолання перешкод у професійній реалізації жінок у сфері кібербезпеки на рівні освіти.
<https://issuu.com/usaidcybersecurity/docs/ua>
 27. Рада національної безпеки і оборони України. (2024). Діяльність Ради національної безпеки і оборони України у сфері кібербезпеки.
<https://www.rnbo.gov.ua/ua/Diialnist/7087.html>
 28. Рада національної безпеки і оборони України. (2023). Зміни в сфері кібербезпеки України та залучення жінок у боротьбу з кіберзагрозами.
<https://www.rnbo.gov.ua/news/zmini-v-sferi-kiberbezpeki-ukraini-ta-zaluchennya-zhinok-u-borotbu-z-kiberzagrozami/>
 29. ІЖ “Кібербез”. (2024). Роль жінок у кібербезпеці посилюється, НКЦК започатковує ініціативу "гендерного балансу" в умовах війни.
<https://cybersec.net.ua/novyny/743-rol-zhinok-u-kiberbezpetsi-posyliuietsia-nktsk-zapochatkovuie-initsiatyvu-hendernoho-balansu-v-umovakh-viiny.html>
 30. Сорока, Л. (2023). Цифрове насильство щодо жінок у період війни. У зб.: Гендерна політика в умовах воєнного стану: правовий вимір. Репозиторій БНАУ.
https://rep.btsau.edu.ua/bitstream/BNAU/8785/1/Vplyv_viiny.pdf
 31. Танська, В., Майданюк, І., Овчаренко, О., Денисенко, А., & Стрілецька, Н. (2024). STEM, як інноваційна стратегія інтегрованої освіти: світовий досвід та перспективи. Перспективи та інновації науки, 10(44), 696-609.
[https://doi.org/10.52058/2786-4952-2024-10\(44\)-596-609](https://doi.org/10.52058/2786-4952-2024-10(44)-596-609)
 32. Український Кластер Кібербезпеки. (n.d.). Про нас.
<https://www.cybercluster.org.ua/>
 33. Шопіна.І. (2024). Гендерний баланс та гендерна рівність в секторі безпеки і оборони: проблеми і перспективи.
<https://academy-vision.org/index.php/av/article/view/1548/1479>
 34. UA Crisis. (2025). Жінок закликають активніше йти в ІТ-сектор.
<https://uacrisis.org/uk/zhinok-zaklykayut-aktyvnish-e-jty-v-it-sektor>
 35. Яблоновська, Т. (2020, 5 жовтня). Рейтинг вишів для ІТ-галузі 2020.
<https://dou.ua/lenta/articles/ukrainian-universities-2020/>

36. Allied Market Research. (2024). Military cybersecurity market size, share | forecast - 2033. <https://www.alliedmarketresearch.com/military-cybersecurity-market-A323349>
37. Bachschmidt, J., & Cohignac, M. (2025). Technological and security issues: 2025, a pivotal year for women. Fondation Robert Schuman, 782, pp.1–6. <https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-782-en.pdf>
38. Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT professional*, 2(1), pp.24-31. https://www.researchgate.net/publication/224110561_Women_in_Cybersecurity_A_Study_of_Career_Advancement
39. Bazeley, P. (2013). *Qualitative data analysis: practical strategies*. SAGE Publications. 125-155 p.
40. Blackburn, H. (2017). The status of women in STEM in higher education: A review of the literature 2007–2017. *Science & Technology Libraries*, 36(3), pp.235-273. <https://www.tandfonline.com/doi/full/10.1080/0194262X.2017.1371658>
41. Behncken, K. (2023). The world needs cybersecurity experts – Microsoft expands skilling effort with a focus on women. *Microsoft On the Issues*. <https://blogs.microsoft.com/on-the-issues/2023/04/19/cybersecurity-skills-initiative-expansion-nonprofits/>
42. Bongiovanni, I., & Gale, M. (2023). *Women in Cyber: Exploring the Barriers, Redesigning the Profession*. The University of Queensland, 50. <https://business.uq.edu.au/files/97978/women-in-cyber-exploring-the-barriers-report.pdf>
43. Borgeaud, A. (2024, 10 травня). Average cybersecurity salary worldwide in 2023, by gender. <https://www.statista.com/statistics/1465491/average-global-cybersecurity-salary-by-gender/>
44. Bouher, K. (2024, 3 вересня). *Unlocking potential: How women can shape Southeast Asia’s digital... PGI*. <https://www.pgiti.com/insights/unlocking-potential-women-southeast-asia-digital-security-landscape>
45. Cheryan, S., Master, A., & Meltzoff, A. N. (2015). Cultural stereotypes as gatekeepers: Increasing girls’ interest in computer science and engineering by diversifying stereotypes. *Frontiers in psychology*, 6, 49. https://www.researchgate.net/publication/272837457_Cultural_stereotypes_as_gatekeepers_increasing_girls'_interest_in_computer_science_and_engineering_by_diversifying_stereotypes

46. Corneliussen, H. G. (2020). What brings women to cybersecurity? A qualitative study of women's pathways to cybersecurity in Norway. Proceedings of the 2020 European Interdisciplinary Cybersecurity Conference. pp. 1-2. <https://doi.org/10.1145/3424954.3424965>
47. Council of the European Union. (2024). Directive of the European Parliament and of the Council. <https://data.consilium.europa.eu/doc/document/PE-33-2024-INIT/en/pdf>
48. Devlin, H. & Hern, A. (2017). Why are there so few women in tech? The truth behind the Google memo. The Guardian. <https://www.theguardian.com/lifeandstyle/2017/aug/08/why-are-there-so-few-women-in-tech-the-truth-behind-the-google-memo>
49. Digital Reskilling for Ukrainian Women Evacuees in Poland Programme Launched at Warsaw Ceremony. (2023). UNITAR. <https://unitar.org/about/news-stories/stories/ukrainian-evacuee-finds-inspiration-unitar-digital-reskilling-programme#:~:text=The%20programme%20was%20launched%20in,of%20improving%20their%20livelihood%20potential.>
50. Ensmenger, N. (2010). Making Programming Masculine. Gender Codes: Why women are leaving computing, T.J. Misa (Ed.). 115-142. <https://doi.org/10.1002/9780470619926.ch6>
51. Euronews. Massimo Diana (2024). Women are saving Ukraine's wartime economy. <https://www.euronews.com/2024/03/08/women-are-saving-ukraines-wartime-economy>
52. European Cyber Security Organisation (ECSO), Ministry of Digital Transformation of Ukraine. (2024, jan). ECSO-Ukraine collaboration: Achieving convergence between Ukrainian and European cybersecurity ecosystems. <https://ecs-org.eu/ecso-uploads/2024/01/Collaboration-between-ECSO-and-Ukraine-Dec-2023.pdf>
53. European Cyber Security Organization. (2023, December). Collaboration between ECSO and Ukraine. <https://ecs-org.eu/ecso-uploads/2024/01/Collaboration-between-ECSO-and-Ukraine-Dec-2023.pdf>
54. European Institute for Gender Equality. (2017, 23 jun). Cyber violence against women and girls. https://eige.europa.eu/publications-resources/publications/cyber-violence-against-women-and-girls?language_content_entity=en
55. European Institute for Gender Equality. (2022). Gender-based violence: Combating cyber violence against women and girls. Publications Office of the European Union. https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf

56. European Organisation of Military Associations and Trade Unions. (2023). EUROMIL survey – gender equality/women in the armed forces. https://euromil.org/wp-content/uploads/2023/06/2306_Survey-Gender-Equality-in-the-Armed-Forces.pdf
57. European Parliament and Council of the European Union. (2011). on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0093>
58. Girls Who Code. (n.d.) About us. <https://girlswhocode.com/about-us/research>
59. Global Cybersecurity Forum, Boston Consulting Group. (2024). 2024 cybersecurity workforce report: Bridging the workforce shortage and skills gap. <https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap/>
60. Global People Strategist. (2024, 11 dec). Gender pay gap in the Ukraine. <https://globalpeoplestrategist.com/gender-pay-gap-in-the-ukraine/>
61. Global Security Forum (GFT). (2024). 2024 Cybersecurity workforce report: bridging the workforce shortage and skills gap. <https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap>
62. Goodman, M. D. (2003). Cyber deterrence: Tougher in theory than in practice? University of Maryland Digital Commons.
63. Google for Developers. (2025). Women Techmakers Initiatives. <https://developers.google.com/womentechmakers/initiatives>
64. Gwinn, M. (2022, 11 dec). Why representation matters for girls and women in STEM. US EPA. <https://www.epa.gov/perspectives/why-representation-matters-girls-and-women-stem>
65. Hicks, M. (2017). Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing. MIT press. 352pp.
66. IBM. (2025). Return to the workforce with the IBM Tech Re-Entry Program. <https://www.ibm.com/careers/blog/return-to-the-workforce-with-the-ibm-tech-re-entry-program>
67. ISC2. (2022). Cybersecurity workforce study 2022. <https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf>
68. ISC2. (2023). Women in cybersecurity: Inclusion, advancement and pay equity.
69. ISC2. (2023). Cybersecurity workforce study 2023. How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.

- https://edge.sitecorecloud.io/internationf173-xmc4e73-prodabc0f-9660/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
70. ISC2. (2024a). Key findings. 2024 ISC2 Cybersecurity Workforce Study. <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study#KeyFindings>
 71. ISC2. (2024b). Women in cybersecurity: Inclusion, advancement and pay equity are keys to attracting and retaining more women. <https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Inclusion-Advancement-Pay-Equity>
 72. ISC2. (2025, 6 mar). Survey: Women comprise 22% of the cybersecurity workforce. Cybersecurity Certifications and Continuing Education. <https://www.isc2.org/insights/2025/03/women-comprise-22-percent-of-the-cybersecurity-workforce>
 73. Katzcy. (n.d.). About Us. <https://www.katzcy.com/about-us>
 74. Kaura, A. (2024). Global Demand for Cybersecurity Talent Continues to Cool. LinkedIn Economic Graph. <https://economicgraph.linkedin.com/content/dam/me/economicgraph/en-us/PDF/global-cybersecurity-talent-trends.pdf>
 75. Kim, H. H. (2020, 14 sep). Computing's gender divide: Why tech is stuck in the 1980s. Welcome to the Jungle. Career Hacking. <https://www.welcometothejungle.com/en/articles/btc-tech-women-gender>
 76. Kupper, C. (2021). Military women use skills to excel in cybersecurity. Military Families. <http://publications.militaryfamilies.com/articles/military-women-use-skills-to-excel-in-cybersecurity>
 77. Light, J. S. (1999). When Computers Were Women. JSTOR. Technology and Culture. 40(3), 455–483. <http://www.jstor.org/stable/25147356>
 78. Liu, X.M. & Murphy, D.R. (2016). Engaging females in cybersecurity: K through Gray. 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 255-260.
 79. Luta Security. (2025). Founder & CEO. <https://www.lutasecurity.com/founder-ceo>
 80. Mandel, L. (1967). The computer girls. Cosmopolitan. <https://archive.org/details/the-computer-girls-cosmopolitan-magazine-april-1967/The%20Computer%20Girls%20-%20Cosmopolitan%20magazine%20%28April%201967%29%20%5Bocr%5D/>
 81. Massachusetts Institute of Technology. (2025a). Free Online Course Materials. MIT OpenCourseWare. https://ocw.mit.edu/search/?f=Lecture%20Videos&f=Lecture%20Audio&q=cybersecurity&s=department_course_numbers.sort_coursenum
 82. Massachusetts Institute of Technology. (2025b). MIT Women's Technology Program. <https://web.mit.edu/wtp/>

83. Military OneSource. (2024). 2023 demographics profile. <https://www.militaryonesource.mil/data-research-and-statistics/military-community-demographics/2023-demographics-profile/>
84. National Center for Women & Information Technology. (2024). By the numbers. <https://ncwit.org/resource/bythenumbers/>
85. National Cyber Security Centre. (2024a). CyberFirst. Girls Competition. <https://www.ncsc.gov.uk/cyberfirst/girls-competition>
86. National Cyber Security Centre. (2024b). This is a CyberFirst World. Fnnual highlight report 2023–2024. <https://www.ncsc.gov.uk/files/CyberFirst-Annual-Report-2023-24.pdf>
87. National Cyber Security Centre. (2025a). Schoolgirls across UK prepare to vie for crown of cyber security champion. <https://www.ncsc.gov.uk/news/schoolgirls-across-uk-prepare-to-vie-for-crown-of-cyber-security-champion>
88. National Cyber Security Centre. (2025b). This is a cyberfirst world. Annual highlight report 2024-2025. <https://www.ncsc.gov.uk/files/CyberFirst-Annual-Report-2024-25.pdf>
89. National Cybersecurity Cluster of Ukraine. (2024). https://www.linkedin.com/posts/ncsc_the-role-of-women-in-strengthening-ukraines-activity-7295440315245592576-OcYw?utm
90. National Science Foundation (NSF). (2023). CybeCorps: Scholarship for Service (SFS). Program Solicitation. <https://www.nsf.gov/funding/opportunities/sfs-cybercorps-scholarship-service/nsf23-574/solicitation>
91. OECD. (2023). Building a Skilled Cyber Security Workforce in Latin America. OECD Skills Studies. OECD Publishing, Paris. <https://doi.org/10.1787/9400ab5c-en>
92. Orange Cyberdefense. (2023, 7 mar). For a safer digital society: Breaking down gender barriers in cybersecurity. <https://www.orange cyberdefense.com/dk/blog/research/for-a-safer-digital-society-breaking-down-gender-barriers-in-cybersecurity>
93. Orange Cyberdefense. (2024, 6 mar). For a safer digital society: Breaking down gender barriers in cybersecurity. <https://www.orange cyberdefense.com/be/blog/for-a-safer-digital-society-breaking-down-gender-barriers-in-cybersecurity>
94. Osborne, C. (2023, 27 березня). Women to hold 30 percent of cybersecurity jobs globally by 2025. Cybercrime Magazine. <https://cybersecurityventures.com/women-in-cybersecurity-report-2023/>
95. Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, M. A. M., AlShaalán, M. B. H. (2022, sep). Empowering women to work in cybersecurity: Is a win-win. Boston Consulting Group.

- https://api.gcfforum.org/api/files/public/upload/70f628b0-7cd5-42c0-9280-f64bfc8ad1d_Empowering-Women-to-Work-in-Cybersecurity-Is-a-Win-Win.pdf
96. PRIF blog. (2024, 14 mar). Beyond the code: Unveiling Gender Dynamics in AI and Cybersecurity for International Security. <https://blog.prif.org/2024/03/14/beyond-the-code/>
 97. Qubit Labs. (n.d.). Women in Tech Statistics: Surprising Facts & Qubit Labs` Impact. <https://qubit-labs.com/women-in-tech-statistics>
 98. Reskilling Ukraine. (n.d.). About us. <https://www.reskillingukraine.com/>
 99. Rubin, H. J., & Rubin, I. S. (2011). Qualitative Interviewing: The Art of Hearing Data (3rd ed.). Sage Publications. p. 103–106
 100. Sentsova, A., Lychak, M., O`Connor, S., Thomas, W. (2024, November 18). Women in Russian-speaking cybercrime: Mythical creatures or significant members of underground? SANS Institute. <https://www.sans.org/blog/women-in-russian-speaking-cybercrime-mythical-creatures-or-significant-members-of-underground/>
 101. Shukach.pro. (n.d.) About us. <https://www.shukach.pro/>
 102. Squires V. (2023). Thematic analysis. In J. M. Okoko, S. Tunison, K. D. Walker (Eds.), Varieties of qualitative research methods: Selected contextual perspectives (pp. 463–469). Springer Nature.
 103. Stanford Women in Computer Science. (2025). Events. <https://stanfordwomenincomputerscience.com/events.html>
 104. The Gurus. (2025). Advancing Gender Equality in 2025 and Beyond. IT Security Guru. <https://stanfordwomenincomputerscience.com/events.html>
 105. The NATO Committee on Gender Perspectives (NCGP). (2023). 2022 Summary of the National Reports of NATO Members and Partner Nations. https://www.nato.int/nato_static_fl2014/assets/pdf/2025/1/pdf/2022-ncgp-summary.pdf
 106. The White House. (2025). Megan Smith. Office of Science and Technology Policy. <https://obamawhitehouse.archives.gov/administration/eop/ostp/about/leadershipstaff/smith>
 107. Times Higher Education. (2025). World University Rankings 2025. <https://www.timeshighereducation.com/world-university-rankings/latest/world-ranking>
 108. Official website of the U.S. Office of Personnel Management. (2025). CyberCorps: Scholarship for Service (SFS). <https://sfs.opm.gov/>
 109. Willig, C., & Rogers, W. (2017). The SAGE Handbook of qualitative research in psychology. (Vols. 1-0). SAGE Publications Ltd. pp. 17-23 <https://doi.org/10.4135/9781526405555>

110. Women in CyberSecurity & Aleria. (2023). The 2023 State of Inclusion Benchmark in Cybersecurity. WiCyS.org
https://www.wicys.org/wp-content/uploads/2024/04/2023-State-of-Inclusion-Benchmark-in-Cybersecurity-Report.pdf?utm_source
111. Women in Cybersecurity (WiCyS). (2024, jun). WiCyS 2024 Conference Evaluation Report.
https://www.wicys.org/wp-content/uploads/2024/08/WiCyS-2024-Evaluation-Report-External_8.24.24.pdf
112. Women in CyberSecurity (WiCyS). (2025a). Skills Development Training Programs.
<https://www.wicys.org/initiatives/programs/>
113. Women in CyberSecurity (WiCyS). (2025b). WiCyS military.
<https://www.wicysmilitary.org/>
114. Women in CyberSecurity (WiCyS). (2025c). Lack of respect, career opportunities lead to exclusion for women in cybersecurity.
https://www.wicys.org/lack-of-respect-career-opportunities-lead-to-exclusion-for-women-in-cybersecurity/?utm_source
115. Women4Cyber Foundation. (2024). 2024 Conference organised by Women4Cyber. European Cyber Security Organisation (ECSO).
<https://ecs-org.eu/events/2024-conference-organised-by-women4cyber/>
116. Women4Cyber Montenegro. (2025a). Projects. <https://w4c.me/en/projects/>
117. Women4Cyber Montenegro. (2025b). 2023 Annual Report.
<https://women4cyber.eu/wp-content/uploads/2024/07/W4C-Annual-Report-2023-2.pdf>
118. World Economic Forum. (2025, jan). Global cybersecurity outlook 2025.
https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Додатки

Додаток А. Гайд для проведення напівструктурованого інтерв'ю у дослідженні “Жінки в українській кібербезпеці: голоси тих, які подолали перешкоди”

Інформована згода

Вітаю! Мене звати (ім'я), я студентка 3 курсу спеціальності “Соціологія” Національного університету “Києво-Могилянська Академія”. Я пишу наукову роботу на тему “Жінки в українській кібербезпеці: голоси тих, які подолали перешкоди” в рамках проходження курсу “Гендерні студії” під керівництвом кандидатки соціологічних наук та доцентки кафедри соціології Тамари Марценюк. Дякую, що погодилися взяти участь у моєму дослідженні. Інтерв'ю буде проходити у формі бесіди, протягом якої Вам буде задано декілька питань. Наша розмова триватиме близько однієї години. Будь-яка надана Вами інформація буде використовуватись окремо від Ваших персональних даних, Ваше ім'я чи інші дані, які можуть вказати на Вас, розголошуватися не будуть.

Протягом інтерв'ю не може бути правильних чи неправильних відповідей. Намагайтеся, будь ласка, відповідати відкрито та щиро. Також, під час участі в інтерв'ю Ви маєте право у будь-який час відмовитись від відповіді на будь-яке питання чи відмовитись від участі взагалі. Будь ласка, зверніть увагу, що розмова буде записана, але лише для мого внутрішнього аналізу в узагальненому вигляді. Попри це, Ви маєте право на відмову від запису.

Якщо у Вас виникнуть питання щодо інтерв'ю, Ви завжди можете сконтактувати зі мною за телефоном... або надіслати електронний лист на пошту:

Чи Ви згодні взяти участь в інтерв'ю на таких умовах?

Блок 1. Вступ: знайомство. Освіта, кар'єрний шлях та професійний досвід (20 хвилин)

- Розкажіть, будь ласка, трохи про себе та посаду, на якій працюєте?
- Чи маєте ви університетську освіту в сфері кібербезпеки чи отримали знання за допомогою інших ресурсів (зокрема, онлайн/офлайн-курсів)
- Що спонукало вас обрати сферу кібербезпеки?
- Які основні фактори вас мотивували розвиватися в цій галузі? **(Для інтерв'юєра: Хай респондентка назве, до прикладу, три основних)**
- Чи були у вас “наставни(ця)к”, які допомогли б вам у цій сфері з працевлаштуванням, або поглибленням в цю сферу?
- Чим Ви наразі займаєтесь в компанії/організації на Вашій посаді?
- Скільки часу Ви працюєте в цьому напрямку?
- Як, на вашу думку, до вас ставиться керівництво?

Блок 2. Перешкоди та виклики під час працевлаштування та кар'єри (20 хвилин)

- Яке співвідношення чоловіків та жінок у вашому колективі?

● Як ви почувались у перші часи? Чи помічали труднощі у спілкуванні/знайомстві?

● Чи помічали ви, що через свою стать не можете стати повноправною членкинею колективу?

● Чи відчували ви підвищену конкуренцію під час працевлаштування?

Якщо на попереднє запитання відповідь була “так, відчувала”:

● Чи помічали ви, що до вас ставляться інакше, як до кандидатки, через вашу стать?

● Чи відчували ви дискримінацію або упередження у професійному середовищі?

Якщо на попереднє запитання відповідь була “так, відчувала”:

● Як ці бар’єри вплинули на вашу кар’єру та особистий розвиток? Який із бар’єрів вплинув на вас найбільше?

● Чи були ситуації, коли ви відчували, що ваш успіх приписують “випадковості” або “щастю”, а не вашим знанням та зусиллям?

● Чи доводилося вам докладати додаткові зусилля для доведення своєї компетентності через гендерні стереотипи?

● Чи були моменти, коли ви замислювалися про зміну кар’єри через ці бар’єри?

Блок 3. Сприйняття суспільством (10 хвилин)

● Як, на Вашу думку, суспільство сприймає жінок у технічних сферах?

● Чи стикались Ви з осудом чи нерозумінням зі сторони інших людей, щодо вашої професії/галузі інтересів?

● Чи змінювались думки людей з часом щодо Вашого вибору професії?

● Чи стикались Ви з позицією, що “жінки не для кібербезпеки”?

● Які недоречні запитання щодо вашої професії ви чули?

● Як ваша сім’я та друзі ставляться до вашої роботи? Чи розуміють вони, чим саме ви займаєтесь?

Блок 4. Завершальний (5 хвилин)

● Чи спостерігали Ви зміни у ставленні до жінок у цій сфері протягом Вашої роботи?

● Якби у вас була можливість змінити щось у сфері кібербезпеки (наприклад, культуру, підходи чи ставлення до жінок), що саме ви б змінили і чому?

● Що б ви порадили компаніям, які прагнуть створити більш сприятливе середовище для жінок у кібербезпеці? (**Уточнююче питання:** Які практичні кроки могли б цьому сприяти?)

● А також, скажіть, будь ласка, які поради ви б дали жінкам, які лише розпочинають свій шлях у кібербезпеці? Що могло б допомогти їм подолати можливі труднощі та розвиватися в цій сфері?

● Чи є щось, про що Ви б хотіли поговорити, але це не було проговорено протягом нашого інтерв’ю?

Додаток Б. Гайд для проведення напівструктурованого експертного інтерв'ю у дослідженні “Доступу жінок до сфери кібербезпеки в Україні”

Вітаю, (ім'я). Дякую, що ви погодились на це інтерв'ю.

Мене звати (ім'я), я студент(ка) Національного університету “Києво-Могилянська академія”. У рамках курсу “Вступ до гендерних студій” ми з командою досліджуємо доступ жінок до сфери кібербезпеки в Україні. Результати нашого інтерв'ювання будуть використані для наукового дослідження “Доступ жінок до сфери кібербезпеки в Україні”. Ми вирішили звернутись до вас як до респондент(а)ки.

Метою даних досліджень є з'ясувати, якими є успіхи та виклики доступу жінок до сфери кібербезпеки в Україні.

Я записуватиму нашу розмову, щоб точно зафіксувати всі відповіді для подальшого аналізу. Я гарантую вам конфіденційність. Ваші відповіді буде деперсоналізовано та проаналізовано в узагальненому вигляді. Запис розмови буде використаний з академічною метою (для написання наукових публікацій). Якщо під час розмови Ви б хотіли сказати щось офф-рекордс – повідомте мені.

Чи погоджуєтесь Ви на запис інтерв'ю?

Орієнтовна тривалість інтерв'ю – приблизно 1 год.

Я говоритиму українською мовою, а Ви можете висловлюватись тією мовою, якою буде зручно.

Скажіть, чи зрозумілою була ця інформація і чи Ви даєте згоду на це інтерв'ю та його запис?

Якщо наразі не маєте питань до мене, перейдімо до інтерв'ю.

Блок 1. Знайомство

1. Для початку я б хоті(в)ла дізнатися про Ваш досвід роботи у сфері кібербезпеки
2. Яка Ваша поточна посада?
3. Скільки років Ви працюєте у сфері кібербезпеки?
4. Чи здобували Ви освіту за спеціальністю “Кібербезпека”?
(якщо відповідають НІ: Як Ви здобули навички потрібні для професії в кібербезпеці?)
5. Що мотивувало Вас обрати професію в сфері кібербезпеки?
6. Як ви вважаєте, що є найбільшими викликами та успіхами сфери кібербезпеки в Україні сьогодні?
7. Як би ви прокоментували важливість сфери кібербезпеки в контексті повномасштабного вторгнення загалом російсько-української війни?

Блок 2. Представленість жінок у сфері кібербезпеки в Україні

8. Як гадаєте, чи відчутна у сфері кібербезпеки в Україні диспропорція у співвідношенні чоловіків та жінок?

9. Як би Ви оцінили рівень представленості жінок і чоловіків на Вашому робочому місці? Якщо можливо певним чином узагальнити, то які саме жінки приходять у сферу кібербезпеки (беручи до уваги вік, сімейний стан та інші соціально-демографічні характеристики), тобто, для яких категорій жінок сфера кібербезпеки є найбільш зручною і чому?
10. Як Ви вважаєте, чи вплинув початок повномасштабного російського вторгнення на доступ та діяльність жінок у сфері кібербезпеки в Україні? Яким є цей вплив і чому саме таким?

Блок 3. Виклики доступу жінок до сфери кібербезпеки в Україні

11. Які посади займають жінки у Вашому робочому колективі?
12. Як Ви вважаєте, чи присутній розрив в оплаті праці між чоловіками та жінками у сфері кібербезпеки в Україні?
- 12А **для чоловіків:** Чи помічали Ви упередження до жінок у своєму робочому колективі? Які саме категорії жінок зазнають подібного ставлення і чому? Чи ставали Ви свідками сексуальних домагань до жінок у своєму робочому колективі?
- 12Б **для жінок:** Чи стикалися Ви з гендерними упередженнями, стереотипами чи сексуальними домаганнями у своєму робочому колективі? Чи стикалися ваші колеги - жінки?
13. Які фактори, на вашу думку, змушують жінок звільнитися з посад у сфері кібербезпеки в Україні?

Блок 4. Успіхи доступу жінок до сфери кібербезпеки в Україні

14. Чи впроваджує організація, де Ви працюєте, ініціативи для залучення (підтримки) жінок до роботи в кібербезпеці? (квоти, тренінги, курси підвищення кваліфікації...)
15. Чи є ефективними ініціативи державного рівня у підтримці жінок у роботі у сфері кібербезпеки? (Інформаційні кампанії, гранти, жіночі спільноти, закони для підтримки гендерної рівності...)
16. Чи могли б Ви навести приклад успішних жінок, які побудували кар'єру в кібербезпеці у світі? В Україні?
17. Що Ви вважаєте трьома найбільшими досягненнями жінок у сфері кібербезпеки в Україні?

Блок 5. Рекомендації

18. Які новації на державному рівні зробили б сферу кібербезпеки доступнішою для жінок?
19. Які заходи слід вживати, аби жінки активніше долучались до сфери кібербезпеки України?
20. Яким чином структури/компанії/інституції у сфері кібербезпеки України можуть підтримувати вже працевлаштованих жінок?
21. Чи є щось, що Ви хотіли б додати?

22. Чи могли б Ви порекомендувати 2-3 колег/колежанок, що могли б поділитися думками щодо успіхів та викликів жінок у сфері кібербезпеки у форматі експертних інтерв'ю? (тобто в тому самому форматі)

Дякуємо за Вашу увагу та час!

Додаток В. Перелік одиниць аналізу

Таблиця В.1. Перелік медіаматеріалів, що увійшли до вибірки дослідження репрезентації жінок у кібербезпеці в українських медіа

Номер матеріалу	Медіа	Кількість матеріалів	Посилання	Назва матеріалу	Дата публікації
1	0522.ua	1	https://www.0522.ua/news/3854596/natalia-tkacuk-nkck-zapocatk-ovue-iniciativu-z-posilenna-roli-zinok-u-kiberbezpeci	Наталія Ткачук: НКЦК започатковує ініціативу з посилення ролі жінок у кібербезпеці	06.11.2024
2	24 Канал	1	https://news.24tv.ua/zhinki-viyskovih-konfliktah-neymovirni-novini-ukrayini-i-svitu_n1458175	Жінки у військових конфліктах: неймовірні досягнення НАТО за останні роки	12.11.2020
3	АрміяInform	1	https://armyinform.com.ua/2020/01/29/general-major-yevgen-stepanenko-rozpoviv-yak-gotuyut-kibervoyiniv-i-zvyazkivziv/	Генерал-майор Євген Степаненко розповів, як готують кібервоїнів і зв'язківців	29.01.2020
4	Гендер в деталях	1	https://genderindetail.org.ua/news/kiberbezpeka-u-2020-yak-koristuvatis-internetom-abi-ne-stati-zhertvoyu-ataki-1341603.html	Кібербезпека у 2020: як користуватись інтернетом, аби не стати жертвою атаки	23.11.2020

5	Громадське	2	https://hromadske.ua/suspilstvo/238640-min-oborony-nazvalo-iaki-v-akansiyi-obyraiut-zinky-u-rekrutynhovyykh-tse-ntrakh	Міноборони назвало, які вакансії обирають жінки у рекрутингових центрах	27.01.2025
6			https://hromadske.ua/posts/zavdyaki-tomu-s-ho-ya-zhinka-meni-vda-lo-sya-potrapiti-v-it-yak-zminiti-profesiyu-i-stati-programistkoyu	“Завдяки тому, що я жінка, мені вдалося потрапити в ІТ”. Як змінити професію і стати програмісткою	23.06.2021
7	Громадський Простір	4	https://www.prostir.ua/event/vebinar-zhinky-u-kiberbezpetsi-stvorennya-profesijnyh-asotsiatsij-na-osnovi-uspishnyh-praktyk/	Вебінар “Жінки у кібербезпеці: створення професійних асоціацій на основі успішних практик”	10.03.2023
8			https://www.prostir.ua/?news=genderne-riznomanittya-v-kiberbezpetsti-dlya-zhinok-v-ukrajini-vidbuvsya-dialoh-v-mezhah-prohramy-dialoh-pro-kiberbezpeku	“Гендерне різноманіття в кібербезпеці: реалії та можливості для жінок в Україні”: відбувся Діалог в межах програми “Діалог про кібербезпеку”	03.11.2023
9			https://www.prostir.ua/event/pobudova-kariery-zhinok-u-sferi-kiberbezpeky-rekomendatsiji-ta-porady-uspishnyh-profesionalok/	Побудова кар’єри жінок у сфері кібербезпеки: рекомендації та поради успішних професіоналок	10.05.2023
10			https://www.prostir.ua/?grants=nabir-na-mentorsku-prohramu-dlya	Набір на менторську програму для	28.07.2022

			a-studentok-spetsialno sti-kiberbezpeka	студенток спеціальності “Кібербезпека”	
11	Детектор медіа	1	https://detector.media/infospace/article/239800/2025-04-08-u-cdt-o-campus-tryvaie-nabir-na-dvi-programy-dlya-zhinok-liderstvo-v-tsyfrovizatsii-ta-kiberbezpeka/	У CDTO Campus триває набір на дві програми для жінок: лідерство в цифровізації та кібербезпека	08.04.2025
12	ДУІКТ	1	https://duikt.edu.ua/ua/news-1-574-11911-divchata-u-kiberbezpeci-anna-talan-kriz-obektiv-kiberzahisnika-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki	Дівчата у кібербезпеці. Анна Талан: кризь об'єktiv кіберзахисника	11.12.2023
13	Еспресо.tv	1	http://espreso.tv/news/2017/01/18/brytanska-rozvidka-planuye-zaluchaty-divchatok-pidlitkiv-u-yakosti-kiberagentiv	Британська розвідка планує залучати дівчаток-підлітків у ролі кіберагентів	19.01.2017
14	КИЇВСЬКА МАЛА АКАДЕМІЯ НАУК	2	https://don.kyivcity.gov.ua/news/divchata-vi-khovanki-kiiivskoi-man-vidznachili-natsionalniy-den-divchat-u-tekhnologiyakh	Занурення у бізнес компанії “ІТ-Інтегратор” у рамках Національного Дня дівчат в технологіях	11.10.2019
15			http://kyiv.man.gov.ua/news/Novini_akademii/Ekskursija_majbutnih_auditorok_ta_finansistiv_u_kompaniju_EY_u_ramkah_Natsional	Екскурсія майбутніх аудиторок та фінансистів у компанію “EY” у рамках Національного Дня	11.10.2019

			nogo_Dnja_Divchat_v_tehnologijah/	Дівчат в технологіях	
16	Львівський портал	1	https://portal.lviv.ua/news/2023/02/02/start-it-cisco4ukaine-bezkostovne-onlajn-navchannia-u-sferi-it-dlia-ukraintsiv	Start IT. Cisco4Ukraine: безкоштовне онлайн-навчання у сфері ІТ для українців	02.02.2023
17	Маріупольський державний університет	1	https://mu.edu.ua/news/zhinki-v-kiberbezpecei-vnesok-ukrajinskih-naukovic-u-cifrovu-stiykist	Жінки в кібербезпеці: внесок українських науковиць у цифрову стійкість	06.02.2025
18	МІСТО	1	https://mi100.info/2025/01/27/vid-shtabiv-do-kiberbezpeky-20-kandydativ-u-sily-oborony-zhinky/	Від штабів до кібербезпеки: 20% кандидатів у Сили оборони – жінки	27.01.2025
19	Новини Харкова	1	http://uanews.kharkiv.ua/society/2018/03/22/181785.html	Як захиститися від хакерів	22.03.2018
20	Новини.LIVE	1	https://society.novyny.live/google-zapustiv-bezkostovnij-kurs-z-kiberbezpeki-dlia-ukrayintziv-97473.html	Google запустив безкоштовний курс з кібербезпеки для українців	30.05.2023
21	Подобиці	1	https://podrobnosti.ua/2495041-u-stolitsi-vdubvsja-forum-talanovitoi-molodi-nagorodi-ta-dosjagnennja.html	У столиці відбувся Форум талановитої молоді: нагороди та досягнення	26.01.2025
22	Рада національної безпеки і оборони	3	https://www.rnbo.gov.ua/ua/Dialnist/7087.html	Роль жінок у зміцненні кіберстійкості України стала	18.12.2024

	України			головною темою засідання Національного кластера кібербезпеки	
23			https://www.rnbo.gov.ua/ua/Dialnist/5010.html	Перший Національний Саміт Кібербезпеки об'єднає вітчизняних та іноземних лідерів у сфері кібербезпеки	22.09.2021
24			https://www.rnbo.gov.ua/ua/Dialnist/5079.html	Кібервійська можуть стати нашою асиметричною відповіддю агресорові	12.10.2021
25	Район Бізнес	1	https://business.rayon.in.ua/topics/574686-volin-zhinki-i-robota-pid-chas-voennogo-stanu	Волинь: жінки і робота під час воєнного стану	13.02.2023
26	Рубрика	1	https://rubryka.com/article/jaanika-merilo/	Жінка в ІТ: як просувати е-реформи, ламаючи стереотипи. Історія Яніки Мерило	26.05.2020
27	Українська правда - Life	1	https://life.pravda.com.ua/columns/2022/10/18/250896/	Як збільшити кількість дівчат в українському ІТ	18.10.2022
28	Українські новини	1	https://ukranews.com/ua/news/741206-na-vebinari-vid-stem-is-fem-ta-oon-zhinky-rozpoznavly-pro-metody-zahyst	Як убезпечити себе в Інтернеті – поради з вебінару STEM is FEM та "ООН-Жінки"	27.11.2020

			u-vid-kiberzlochyniv		
29	Укрінформ	2	https://www.ukrinform.ua/rubric-ato/2568246-kiberoborona-bez-pecni-vibori-j-zinoca-persist.html	Кібероборона: безпечні вибори й жіноча першість	29.10.2018
30			https://www.ukrinform.ua/rubric-kyiv/2670101-u-vijskovij-licej-boguna-vperse-nabiratimut-divcat.html	У військовий лицей Богуна вперше набиратимуть дівчат	29.03.2019
31	Юридична газета	1	https://jur-gazeta.com/golovna/zhinkiprofesionali-u-galuzi-kiberbezpeki-.html	Жінки-професіонали у галузі кібербезпеки	25.09.2020
32	ЕОР	1	https://www.eop.org.ua/zhinky-v-kiberbezpecezi/	Жінки в кібербезпеці	29.12.2021
33	Finance.ua	1	https://about.pumb.ua/presscenter/news/item/6296-pumb-stal-uchastnikom-nacionaljnogo-dnya-devochek	ПУМБ став учасником Національного дня дівчат у технологіях	13.10.2021
34	IGate.com.ua	1	https://igate.com.ua/news/30553-set-university-ta-darkowl-pochinayut-spvpratsyu-u-sferi-kiberbezpeki	SET University та DarkOwl починають співпрацю у сфері кібербезпеки	19.03.2025
35	Klik Ukraine Support	1	https://www.kliksolutions.com.ua/great-info/zhinky-v-it-realiyi-hhistolittya/	Жінки в IT: реалії XXI століття	22.07.2021
36	KRIVBASS.CITY	1	http://krivbass.city/news/view/v-ukraini-zrostaepopulyarnist-vijskoe-populyarnist-vijsko	В Україні зростає популярність військової освіти	22.09.2020

			voi-osviti-sered-zhinok	серед жінок	
37	NATO - News	1	https://www.nato.int/cps/ru/natohq/news_147863.htm?selectedLocale=uk	Заступниця Генерального секретаря НАТО взяла участь в Конференції з кібербезпеки	24.10.2017
38	Novator.io	1	https://novator.io/novosti/15-najbilshih-venchurnih-ugod-na-rinku-kiberbezpeki-2021-roku	15 найбільших венчурних угод на ринку кібербезпеки 2021 року	15.09.2021
39	NV	1	https://nv.ua/ukr/project/zhinki-i-biznes-yak-viy-na-zminila-gender-nu-strukturu-v-ekonomici-ukrajini-50466406.html	Нові реалії: як змінюються ролі жінок у бізнесі?	18.11.2024
40	PRportal	1	https://prportal.com.ua/Fakty/posilannya-na-neisnuyuchi-storinki-peretvorili-na-profilu-uspishnih-zhinok-naukoviv	Посилання на неіснуючі сторінки перетворили на профілі успішних жінок-науковиць	10.02.2025
41	Root Nation (UA)	1	https://root-nation.com/ua/news-ua/it-news-ua/ua-onlayn-zahid-den-kar-eri-zhinok-v-it-ob-ednav-ponad-2-8-tis-uchasnits/	Онлайн-захід “День Кар’єри Жінок в ІТ” об’єднав понад 2,8 тис. учасниць	30.11.2022
42	SPEKA	1	https://speka.media/yak-divcatam-zaxistiti-sebe-onlain-startuje-osvitnya-programa-z-kiberbezpeki-v7yzky	Як дівчатам захистити себе онлайн: стартує освітня програма з кібербезпеки	27.11.2024

43	Vector	1	https://vctr.media/ua/yak-kiberakademiya-cy-berin-transformuye-novenykh-u-profesionaliv-264708/	Як кіберакадемія CyberIN трансформує новеньких у професіоналів	26.03.2025
44	WoMo	1	https://womo.ua/berta-herrero-pro-riznomanittya-inklyuziya-ta-rivni-mozhливosti-u-tsifrovomu-sviti/	Берта Херреро про різноманіття, інклюзію та рівні можливості у цифровому світі	01.01.2021