MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL UNIVERSITY OF “KYIV-MOHYLA ACADEMY”

Faculty of Social Sciences and Social Technologies

Department of Sociology

RESEARCH PAPER

WOMEN’S ACCESS TO THE CYBERSECURITY FIELD IN UKRAINE

completed within the course “Introduction to Gender Studies” (winter–spring 2025)

Research Coordinator:
Tamara Martsenyuk, Candidate of Sociological Sciences, Associate Professor of the Department of Sociology, NaUKMA;

Coordinators of the Research Groups:
Sofiia Hessin, Volodymyr Hryvtsov, Rostyslav Sydorov, Iulianiia Semernykova, Sofiia Kviat, Diana Boiko; with the participation of Kateryna Zaremba

Team of Authors:
Participants of the course “Introduction to Gender Studies” (winter–spring 2025) – detailed by subsections
Text under the general editorship of Tamara Martsenyuk

Consultants:
Trokhym Babych, Head of the Bachelor’s Program in Cybersecurity at NaUKMA, research consultant
Anna Prokhorova, Senior Lecturer of the Department of Sociology, NaUKMA, consultant on qualitative methods
Anastasiia Ostrovska, Co-founder and CEO of WLSIF, owner of Ostrovska Consulting agency, consultant on strategic communications, women’s leadership, and professional community development in cybersecurity

Technical Review:
Sofiia Kolisnyk, student of the Department of Philology, NaUKMA

Literary Editing:
Sofiia Kolisnyk, student of the Department of Philology, NaUKMA

Completed in cooperation with the NGO “Women’s Leadership and Strategic Initiatives Foundation”

Introduction

In the context of global digitalization, cybersecurity has emerged as a key element of international stability and national security. Its strategic importance is increasing, especially during wartime: amid hybrid threats, information pressure, and digital attacks. However, despite the urgent need for qualified personnel, the cybersecurity field still demonstrates a gender imbalance: women are significantly less represented among specialists than men. This gap is caused not only by technical barriers but also by deeply rooted sociocultural attitudes and stereotypes that have led to educational segregation and a lack of institutional support. Currently, international attention to gender inequality in this field is growing, as the involvement of women in cybersecurity is becoming particularly relevant in view of the effective use of overall human potential to counter modern cyber threats.

Worldwide, there is a growing focus on programs that encourage more women to join the cybersecurity profession. Educational programs, professional communities, and public policies are being implemented to overcome barriers faced by women in this sector. Awareness of the importance of workforce diversity is based not only on the principles of equality but also on evidence that gender-balanced cybersecurity teams are more flexible, innovative, and capable of effective adaptation under crisis conditions.

Thus, the study of international experience in engaging women in the field of cybersecurity is important, as it makes it possible to identify barriers and factors contributing to the successful integration of women into the digital sphere. Through this, women can demonstrate different perspectives on existing problems and find additional solutions to address them.

At the same time, it is important to consider that the gender gap in the cyber sphere has deeper roots. Even at the educational stage, girls face stereotypes regarding the “non-feminine” nature of technical specialties, which affects their self-confidence, career choices, and further professional development.

Examples from different countries can serve as guidelines for Ukraine in implementing more inclusive cyber policies and overcoming gender inequality. Their experience convincingly demonstrates that overcoming gender imbalance in the cyber sphere requires a multi-level strategy: engaging girls in STEM education from an early age; creating organizations aimed specifically at supporting women in cybersecurity; implementing gender-sensitive legislation; and supporting systematic efforts to combat stereotypes. Through the study of effective international practices and approaches, it is possible to develop effective recommendations for creating a sustainable and gender-balanced environment. Successful examples of such reforms already demonstrate their results, for instance, in the form of mentoring programs (CyberFirst, WiCyS) and corporate and governmental initiatives (scholarships, quotas).

Therefore, against the background of global trends and international practices, the need to study the national context becomes increasingly relevant. Despite the ongoing war, Ukraine is advancing its digital transformation while navigating a unique set of obstacles.

Under such conditions, cybersecurity in Ukraine acquires exceptional strategic importance, highlighting the issue of effective mobilization of the country's entire national potential, including the gender dimension of this critical field. Russia's invasion has caused significant changes in the country, as a substantial proportion of men have been mobilized, leading to a noticeable shortage of personnel. In this situation, women have become more actively involved in the cyber sphere, filling professional niches and demonstrating their expertise. Thus, the war itself has created a complex dynamic of new "windows of opportunity" for women in this traditionally masculine field.

At the same time, women entering this sphere face numerous barriers, including cyber violence, which negatively affects their emotional well-being and professional development. Many factors create obstacles for women in the cyber sphere, such as both unconscious and explicit forms of workplace discrimination, biases regarding competence, and unequal pay. However, programs specifically aimed at supporting women demonstrate positive results in increasing their presence in the workplace and in the international labor market.

This study aims to conduct a comprehensive analysis of the current state of gender relations in the field of cybersecurity in Ukraine, with a focus on changes occurring as a result of the full-scale war. The paper consistently examines aspects of public policy and legislation, initiatives of the business environment, as well as the direct impact of wartime conditions on women's professional trajectories, existing barriers, and prospects for achieving genuine gender equality and strengthening the country's cyber resilience.

Chapter 1. Women's Access to the Cybersecurity Field Worldwide

Hessin Sofiia, Denysova Hreta, Kukurik Mariia, Larkova Yuliia, Reshetnik Anastasiia

1.1. International Experience in Engaging Women in Cybersecurity: Education and the Labor Market

1.1.1. Women in the Cyber Sphere: Historical Perspective

As of 2024, women constitute 36% of the workforce in the IT sector; however, in the field of cybersecurity their share is lower — only 24%. [1]It is expected that by 2025 this figure will increase to 30%. [2]Cybersecurity, as a modern technological specialization, is based on interdisciplinary knowledge and skills formed within STEM education (Science, Technology, Engineering, Mathematics). These fields ensure the development of critical thinking, analytical skills, and competencies necessary for participation in technologically complex spheres of the future, such as information technology, artificial intelligence, and digital security[3]. However, how did women enter the field of computer science when today this sphere is considered specifically "male"?

The active involvement of women in working with computers began as early as the 1940s.[4] Women's experience in the computer field, associated with calculation mechanisms, began to take shape in the pre-war period. Women were involved in other technical and industrial professions already during the Second World War.

Before the early 1940s, women were engaged in calculations, accounting work, and performed clerical duties, which allowed them to demonstrate themselves as effective workers who were easy to train[5]. In Britain, with the development of mechanical engineering, women became operators of these mechanisms, as they outnumbered men and due to gender stereotypes: men performed more complex work and were considered the "breadwinners" of the family. At the same time, the country's economic situation contributed to the fact that women were engaged not only in unpaid reproductive labor but also agreed to low-paid work related to machines. One of the reasons for women's low wages was the stereotype of them as temporary and auxiliary workers who would sooner or later leave their jobs for reproductive labor at home. At the beginning of the twentieth century, machine work began to be considered unprestigious and industrial; however, the intellectual labor of office workers and the

[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] Ibid., p. 21.

bureaucratic system relied precisely on its results. Despite this, women's machine work became indispensable for maintaining the viability of the government and institutions of Great Britain[6].

The shortage of male labor during the Second World War encouraged women to master new professions, and the previously "male" field of computer technologies was no exception[7]. Britain began to compile lists of women who could replace men in the most important sectors of industry, and at that time opportunities for career advancement opened for them, which had been significantly limited in the pre-war period. The main sphere to which women were directed was information processing (military information, logistics, and data analysis). While men were engaged in the army, women formed the foundation of the British information sector, held most managerial positions, and some even became part of the army and navy, thereby proving that women could be considered equal to men[8]. It is worth noting that even during wartime in Great Britain, stereotypes persisted that women were mothers and wives first, and soldiers or typists second.

After the launch in the United States of the first digital computer, the Electronic Numerical Integrator and Computer (ENIAC), men were entrusted with the prestigious and complex development of hardware, while the work of female coders and programmers who engaged in the technical programming of machines — that is, the "easier" work — remained invisible. While the U.S. Department of Defense encouraged women's work in both military and civilian spheres and generally described their contribution positively in the media, in news about such an important project as ENIAC, men received the main recognition, while the work of women who played a key role in its programming was not mentioned at all[9].

During the 1950s–1960s, computers transformed from bulky machines into more universal devices that became accessible not only to the government but also to other enterprises. While more qualified fields were reserved for men, women gained experience and developed in clerical work — programming. The reputation of computer programming as "women's work" created opportunities for their development in this field: women's success was reinforced by their reputation as fast and capable learners.

There were so many women in programming that in April 1967 Lois Mandel, in the Cosmopolitan magazine article "The Computer Girls," noted that computer programming requires patience and attention to detail, qualities possessed by women rather than men. "Women are naturally suited for computer programming," and therefore have an advantage in this field[10]. This was almost the only intellectual work where women could earn good money — about $20,000 per year at that time. Even though computer programming was initially a technically complex profession requiring a high level of typing skills and speed of analysis, the lower cost of women's labor negatively affected their status: they were considered less valuable

[6] Ibid., p. 25.
[7] Ibid., p. 26.
[8] Ibid., pp. 26-27.
[9] Light, J. S. (1999). When Computers Were Women. *Technology and Culture*. p. 473.
[10] Mandel, L. (1967, April). The computer girls. *Cosmopolitan.* p. 52.

workers who could not perform higher-level work like men. When men were unable to fully replace women as machine operators, the result was the feminization of programming — machine operator jobs had to be divided into smaller tasks to fit the "feminized" category, although women had previously performed most of the work with machines[11].

From the mid-1960s, the mass displacement of women from the programming sphere began, which acquired a distinctly masculine character — it came to be perceived as a prestigious, more technically complex, and "male" profession. The development of technologies led to the increasing complexity of industry processes — analysis, coding, planning, etc., which required the cultivation of unique skills that men developed through greater access to craft practices. Programming began to be perceived as a phenomenon incomprehensible to most of the population, understood only by a limited group of specialists[12]. In general, when the gender composition of a field changes, as happened with computer programming in the 1960s, the content of the work in the field also changes: when men dominate, the work is considered prestigious and complex, and when women dominate, it is perceived as simple and less demanding in terms of specific skills. "Masculine" programming actively increased the prestige of the profession through professional associations that did not include women: formal computer science programs, professional journals and societies, etc.[13]

As a result, by the 1970s the programming field had become overtly sexist. Professional journals contained derogatory jokes about women, their skills, and emotionality, which contributed to the spread of the idea of "programming as a masculine sphere," where emotions interfere and rationality and adaptability are required. [14]For example, in 1970 in the United States women constituted 38% of the total workforce, but only 8% among STEM workers[15]. The women's movement of the 1970s aimed to remove barriers that prevented women from becoming qualified specialists in various fields. As a result, the image of women in the computer field began to change in a more positive direction. The successes of feminism led to the fact that three major computer companies — IBM, Control Data, and Burroughs Corporation — promoted practices of gender diversity in the workplace.[16]

The 1980s failed to continue the success of the feminist movement: the financial deregulation of the U.S. economy that began in the 1970s[17] contributed to workforce reductions in many companies; increased international competition and neoliberalism reduced the investment capacity of most American companies in employee training, and therefore staff reductions primarily affected women. Many companies effectively reversed internal changes aimed at supporting gender equality initiated by the women's movement of the 1970s. Additionally, the

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

[12] Kim, H. H. (2020, 14 spring). *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*.

[17] Ibid.

release of personal computers also became one of the reasons for the low number of women in programming in the 1980s and 1990s — at a time when men dominated the professional computer sphere, the media promoted the image of the computer as a "toy for boys," thereby contributing to the gender stereotyping of work with computers as "men's work."[18]

1.1.2. Women's Education in Cybersecurity: Key Aspects

It should be noted that gender segregation originates as early as school age, when girls are less encouraged to study technical subjects. Therefore, higher education institutions (HEIs) that offer programs related to information security often have a very small number of female students — the majority of applicants are male. This demonstrates that education plays an important role in shaping a gender-balanced digital future.[19]

According to data from NCWIT (National Center for Women & Information Technology), in 2022 women constituted only 23% of bachelor's degree graduates in computer and information sciences in the United States[20]. This indicates the underrepresentation of women already at the educational stage, particularly in cybersecurity. A number of initiatives seek to change this situation. For example, the United States operates the CyberCorps: Scholarship for Service program, which is funded by the National Science Foundation (NSF) and administered by the U.S. government[21]. The program emphasizes the involvement of underrepresented groups, including women, in the national cybersecurity sector by providing scholarships to undergraduate, graduate, and postgraduate students in exchange for mandatory employment in government institutions after completing their studies.[22]At the same time, the international organization Women in CyberSecurity (WiCyS) operates actively in the United States; it was established in 2013 with the support of the National Science Foundation (NSF). It brings together female students, educators, and industry professionals, providing mentorship, career support, and networking opportunities. In particular, George Washington University has an official student chapter of WiCyS that conducts training sessions, workshops, and career events focused on women's leadership in digital security[23].

At the same time, some global companies develop their own practices to support women, particularly after career breaks. A prominent example is the IBM Tech "Re-Entry Program." This program is aimed at female technical specialists who have had a forced pause in their careers (for example, due to maternity leave) and seek to return to the IT sector (analytics, programming, cybersecurity, etc.). Participants complete paid internships, take part in practical projects, attend adaptation training sessions, and receive mentorship support. After completing

[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). CybeCorps: Scholarship for Service (SFS). *Program Solicitation*.

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

the program, most women receive permanent contracts with IBM or other job offers in the labor market. The program is actively implemented in the United States, Canada, the United Kingdom, Germany, India, and Australia and, according to its organizers, contributes not only to overcoming career gaps but also to creating a more inclusive corporate environment.[24]

Modern cybersecurity is an example of a field characterized by pronounced vertical and horizontal **gender segregation[23].** Women are not only less represented among technical personnel but also rarely occupy leadership positions. The **glass ceiling** theory, developed within feminist sociology, explains that women may be allowed to hold positions up to a certain level, but their further career advancement is often limited[25]. Men in leadership positions tend to allow women access to lower- and middle-level management but not to the highest levels of the hierarchy. These barriers have both a structural nature (embedded in internal organizational policies) and a behavioral nature (associated with gender norms, stereotypes, and expectations regarding the "appropriate" role of women[26]). This is also confirmed by the results of a Women in CyberSecurity (WiCyS) survey conducted in 2023, according to which 83% of women reported experiencing at least one incident of exclusion in the workplace[27]. The main sources of such incidents were: senior leadership (68%), direct managers (61%), and colleagues (52%).[28]

Despite these barriers, some initiatives demonstrate positive dynamics. For example, in the United Kingdom, the CyberFirst Girls Competition, organized by the National Cyber Security Centre (NCSC), annually engages schoolgirls aged 12–13 in interactive cybersecurity competitions. In 2023, more than 8,700 girls participated in the competition, which exceeds the 2022 figure by 24%, and since the initiative's launch in 2017, the total number of participants has reached 65,000[29].

1.1.3. Cybersecurity Labor Market: Civilian and Military Sectors

Despite global initiatives, women in the field of cybersecurity remain a minority. According to data from ISC2 (The International Information System Security Certification Consortium), as of March 2025 the average share of women in cybersecurity teams globally estimated to be only 22%.[30] LinkedIn analytics (see Fig. 1.1.3.1) in July 2024 provides an even more detailed picture: the highest percentage of women is observed in Italy and Singapore — 26.7% each; in Canada — 21.2%; India — 20.9%; the United States — 18.3%; the United Kingdom — 17.9%; and the

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

lowest rate is in Germany — 14.6%.[31]

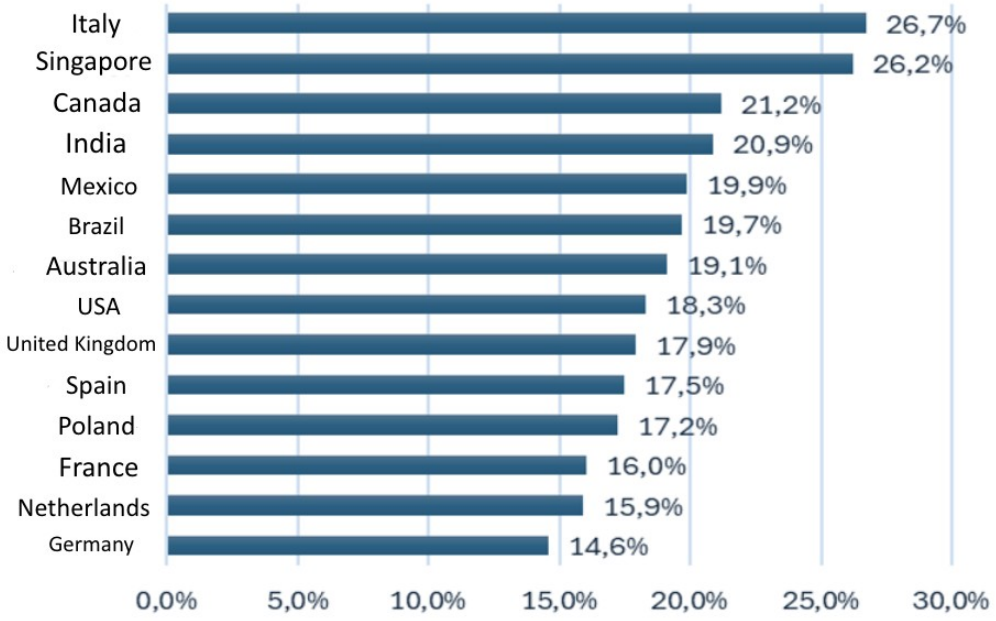


Fig. 1.1.3.1. Share of women among cybersecurity professionals in 2024, % by country
Source: *LinkedIn Economic Graph. (2024), p. 8.*

The situation is particularly challenging in Southeast Asian countries, where women constitute 5–25% of industry professionals. Social expectations, gender stereotypes, and limited leadership opportunities most often serve as the main barriers to their development[32]. In response, the Ready4Cybersecurity program was created, which plans to provide 100,000 women in Asia with education and skills in cybersecurity by 2025[33].

In 2024, women constituted a significant share of cybersecurity teams in sectors where they are represented: in cloud services and construction, the highest share of women in such teams was recorded at 27%; in the real estate sector it was 26%; and in software/hardware development and retail trade — 25%.[34]These were followed by education, healthcare, non-profit organizations, manufacturing, and financial services — 20%. The lowest shares of women in cybersecurity teams were observed in the legal and military sectors — 19% and 18% respectively. At the same time, women hold many managerial or senior positions in cybersecurity — 55%; however, only 7% belong to executive leadership positions (Chief Information Security Officer, engineering director, or Chief Technology Officer). It is worth

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

noting that women in senior and managerial positions have a strong educational background — 38% hold a bachelor's degree, predominantly in STEM fields (51% in computer science/cybersecurity and 12% in engineering), 48% of women hold a master's or specialist degree (58% in computer science/cybersecurity and 12% in engineering), and 9% hold a doctoral degree[35].

In addition to gender stereotypes, workforce reductions also affect the experience of working in cybersecurity. An ISC2 study in 2024 found that 32% of women reported being laid off from cybersecurity positions, compared to 23% of men[36]. At the same time, both direct layoffs (from an organization's cybersecurity staff) and indirect layoffs (dismissals from other parts of the organization) negatively affect job satisfaction: in 2022, 82% of women and 73% of men were satisfied with their work in cybersecurity, whereas in 2025 this figure declined to 67% and 66%, respectively. As of 2024 (see Fig. 1.1.3.2), women more often faced workplace reductions than men due to budget cuts affecting cybersecurity staff operations (40% versus 36%), delays in hiring (42% versus 37%), and delays in salary and promotion increases — 36% and 31%, respectively.

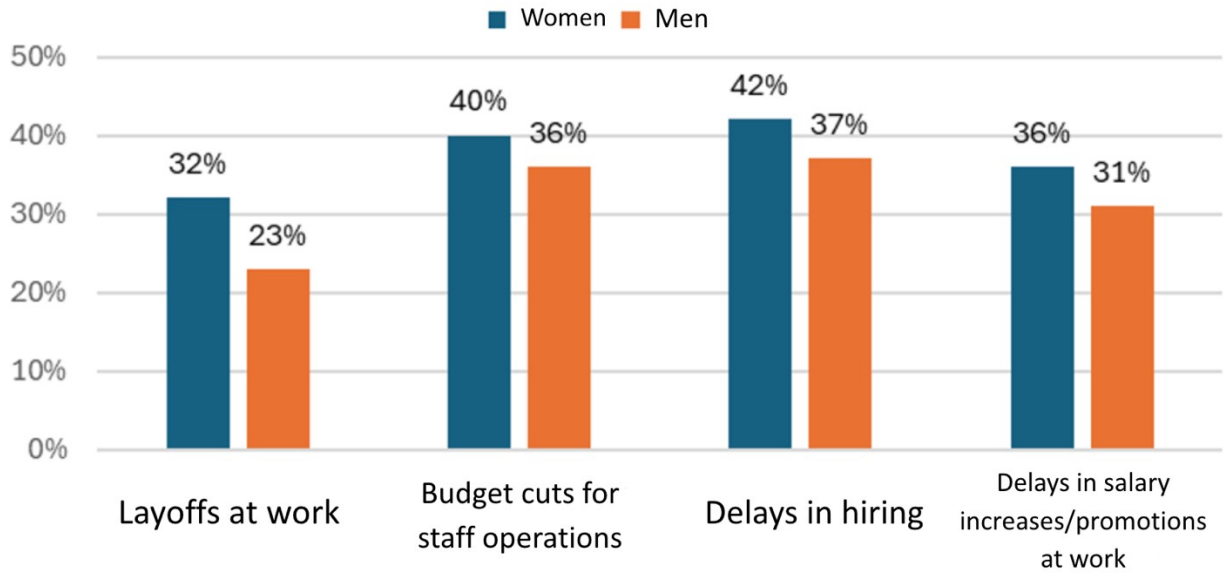


Fig. 1.1.3.2. **Results of the ISC2 survey on types of layoffs in cybersecurity in 2024, %**

Source: 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

[35] Ibid.

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

Among global sectors that most frequently faced reductions in company spending on digital security, the greatest impact was observed in cloud services (48%), telecommunications (44%), and the aerospace industry — 43%. In contrast, the legal sector (19%), non-profit organizations (24%), and the military sector (26%) were the least affected by restrictions in cybersecurity funding[37] .The aforementioned workforce reductions affect not only the lives of individuals but also the capacities of a number of industries: software/hardware development (38%), cloud services (34%), and construction (34%), while the legal sector (14%), non-profit organizations, and the military sector — 13% each — experienced the least impact from staff reductions[38]. The reduction of qualified personnel has not only significantly affected the ability of existing employees to ensure the digital security of organizations but also continues to expose them to considerable risk. The *Global Cybersecurity Outlook* in 2025 revealed that only 14% of cybersecurity companies are confident that they have sufficient staff with the necessary skills. At the same time, **the global gender gap in the cybersecurity labor market** increased from 20% in 2024 to 28% in 2025[39].

According to research by Allied Market Research, the **global military cybersecurity market** was valued at $15.7 billion in 2023 and is projected to reach $68.5 billion by 2033[40]. At the same time, spending on high-quality technical, software/hardware solutions and cybersecurity services in the United States, France, the United Kingdom, and China continues to grow, which raises the issue of new personnel capable of effectively utilizing and providing these resources. The issue of the gender gap in the military and military cybersecurity is becoming particularly relevant. The study *"2023 Demographics Profile of the Military Community,"* conducted by the United States Department of Defense, found that among the total personnel of the Department of Defense, women constitute only 19.3%, while men account for 80.7%[41]. Among them, in 2023, 17.7% of service members were women, compared to 17.5% in 2022. Compared to 2005, the share of women who joined active service in 2023 increased by 3.1%, while the corresponding share for men decreased (see Fig. 1.1.3.3).[42] In Europe, the overall share of women in the armed forces was 13% in 2023, with the highest proportion in Sweden (22%) and the lowest in Ireland (7%)[43]. The average share of women in NATO armed forces increased from 12.24% in 2020 to 12.73% in 2022[44]. Thus, women are increasingly entering traditionally male-dominated fields such as cybersecurity and the military sector, where they acquire specialized

[37] ISC2. (2024a). *Key findings.* 2024 ISC2 Cybersecurity Workforce Study.
[38] Ibid.
[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] bid., p. 21.
[43] European Organisation of Military Associations and Trade Unions. (2023). *EUROMIL survey – gender equality/women in the armed forces*. p. 5.

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

skills and occupy higher positions.

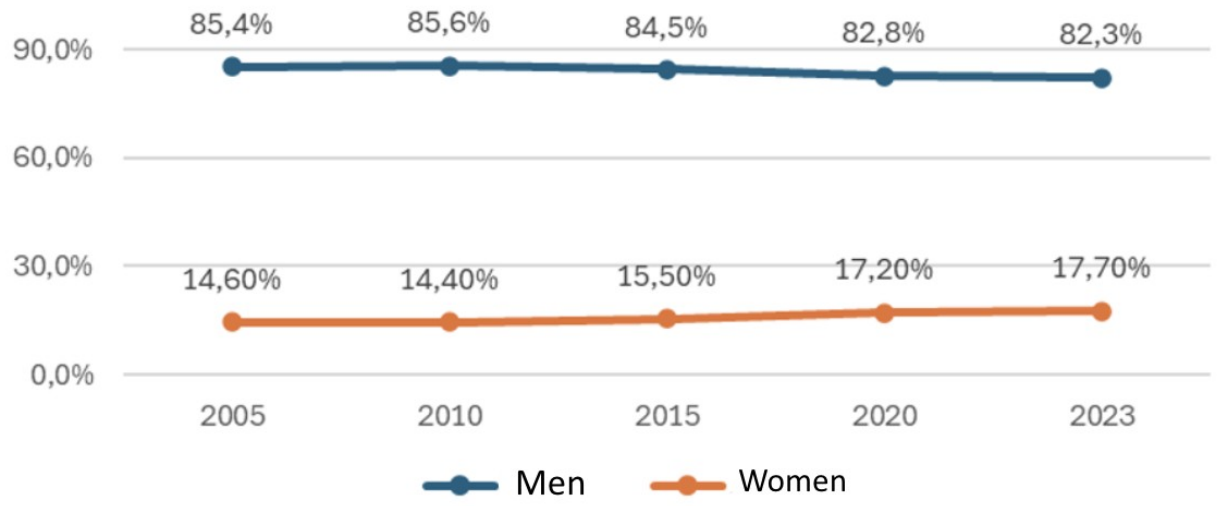


*Fig. 1.1.3.3**. Percentage of active-duty service members in the U.S. Department of Defense, 2005–2023.***

%

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

Data on the number of women in the field of military cybersecurity were not found in open sources. However, it is known that female officers account for 20.1% of the total number of U.S. active-duty officers (18.4%) in 2023[45]. Meanwhile, among NATO military personnel in 2022, women constituted 2.84% of junior officers, 1.41% of mid-level ("field") officers, and only 0.01% of senior officers or generals[46].It should be noted that many U.S. active-duty servicewomen gain experience working with technical systems and cybersecurity even without specialized education. Due to the availability of military educational programs for specialist training, women such as Julia Davila — a soldier, co-founder, and Chief Executive Officer of the cybersecurity company ZibaSec — are able to continue their professional development after completing their service[47]. One of the key programs supporting women's development in cybersecurity after military service is the Women in CyberSecurity (WiCyS) Military Affiliate branch, which provides not only mentorship programs but also networking opportunities and assistance with job placement and career development in this unique field[48].

1.2. Challenges and Achievements in Women's Participation in Cybersecurity

Cybersecurity is one of the IT fields that remains predominantly male-dominated, with low representation of women. Numerous studies and practical experience demonstrate that

[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*.

diversity in teams is an important factor for achieving high economic performance and innovative solutions; however, in cybersecurity it remains significantly limited. As of 2025, the global cybersecurity sector is experiencing a chronic workforce shortage, and therefore the recruitment and support of women may have positive consequences for the field[49].

It is well known that women's involvement in STEM has been a complex and prolonged process. To describe the long trajectory leading to women's participation in STEM, the term **STEM pipeline** was introduced. Subsequently, in response to this concept, the metaphor of the leaky pipeline emerged in academic literature, according to which women are more likely to leave STEM fields at all stages — from initial interest in school, through higher education, and even during academic careers as faculty members. This is explained by the numerous challenges that accompany women at every stage of their path in STEM[50].

The **foundations of gender imbalance** in cybersecurity are formed at the stage of education and socialization of women in STEM fields. Research shows that girls encounter stereotypes about the "unfemininity" of technical and natural sciences from an early age, which undermines their confidence in their own abilities[51]. Stereotypes and biases embedded in society and educational institutions often create the perception that computer science, IT, and cybersecurity are "male" fields where women may feel uncomfortable[52].In particular, the culture of STEM fields is often described as "masculine": computer science is stereotypically associated with social isolation, technocracy, and an innate "talent for technology" required for successful professionals. Such perceptions are incompatible with gender roles traditionally attributed to women, which may lead girls to unconsciously avoid these fields due to a feeling that they do not fit the image of a "typical" IT specialist[53]. A study of women's pathways into cybersecurity in Norway found that dominant masculine images of the IT sector — "hoodie-wearing male gamers who have been programming since childhood" — deter many potential candidates. Women do not identify with such stereotypes and often do not believe they can integrate into the IT environment. As a result, a lack of awareness of the actual range of roles in cybersecurity and narrow perceptions of the field become barriers to women's participation[54].
In addition to stereotypes, biases also occur in hiring and candidate evaluation. Managers may prefer male candidates for technical positions, doubting women's technical skills due to gender bias[55]. Studies confirm that employers sometimes perceive women as less competent in

[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] Ibid., 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] Ibid., p. 49.
[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.

cybersecurity solely based on stereotypes rather than actual skills[56]. Gender stereotypes manifest already at the stage of entry into the profession, making it more difficult for women to obtain their first job or a decent position in cybersecurity. In the workplace, these trends continue in the form of both unconscious and overt discrimination. Women in the industry often report a lack of support and mentorship. Many encounter male-dominated "networks" that are difficult to join and a shortage of female mentors in leadership positions[57]. For example, the 24/7 culture in cybersecurity — that is, the expectation of round-the-clock availability — constitutes a significant barrier for female professionals, especially those with family responsibilities[58]. Ultimately, the combination of these socio-institutional barriers makes it considerably more difficult for women not only to enter the cybersecurity field but also to remain and advance within it.

A separate challenge is the spread of gender-oriented forms of cyber violence, which negatively affect the professional development of women in technological fields. Such phenomena include, in particular, online stalking (cyberstalking), sexual and psychological online harassment, doxxing (the publication of private information), and other forms of aggression in the digital space. It should be emphasized that cyber violence against women and girls has been recognized as one of the fastest-growing forms of gender-based violence in the European Union[59].

According to the Cybersecurity Workforce Study 2021, 87% of women in the field experienced unconscious discrimination in the workplace, and 19% experienced cases of overt gender-based discrimination. Unconscious bias may manifest in small details — from who is given the floor at meetings to managers' assumptions about the professional abilities of female employees. Accumulating over time, such micro-inequalities create invisible barriers to women's career advancement. One of the consequences is the the persistence of the gender pay gap and unequal career progression. Women also reported unclear delays in career advancement (53%) and exaggerated reactions to mistakes (29%)[60].

Despite the barriers outlined above, several positive developments have been observed in the cybersecurity field over the past decade. Research shows that targeted programs can significantly change the gender profile of cybersecurity. In particular, the British "CyberFirst" program in 2023 provided women with 39% of places in its scholarship scheme and involved more than 12,500 girls in the "Girls' Competition," raising the share of female students to a

[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] Ibid., p. 47.

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

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

record 43% in the project's history[61]. In Latin America, government scholarship programs increased the share of women graduating from cybersecurity courses to 30–35%, compared to less than 20% in 2018[62].

1.3. Experience in Overcoming Barriers: Counteracting Discrimination and Gender Stereotypes in Cybersecurity

The development of women's participation in the field of cybersecurity requires a comprehensive approach that encompasses educational and career support, equality policies, and measures to counteract discrimination and gender stereotypes. One of the key solutions is the synergy of initiatives at the micro-, meso-, and macro-levels, structured according to short-, medium-, and long-term measures *(see Table 1.3.1).*[63]

Table 1.3.1 **Measures to Promote Women's Participation in Cybersecurity**

<table>
<tr><th colspan="3">LEVEL</th></tr>
<tr><th>MICRO
Individual Development</th><th>MESO
Institutional and Organization</th><th>MACRO
Systemic and Governmental</th></tr>
<tr><td>Self-development</td><td>Human Resourcers Policy</td><td rowspan="3">Educational and Informational Measures
- National STEM Olympiads and competitions for girls;
- Public awareness campaigns about cybersecurity;
- Funding for research and publications on gender equality in cybersecurity;
- Promotion of female role models in the media;
- Campaigns against gender stereotypes in cybersecurity.</td></tr>
<tr><td>- Self-education (courses, certifications) and professional qualification improvement;
- Participation in educational programs, trainings, workshops, and cybersecurity conferences;
- Increasing confidence in one's professional competencies.</td><td>- Positive discrimination (affirmative action) in hiring;
- Training to counter gender bias and discrimination;
- Transparent recruitment and promotion practices.</td></tr>
<tr><td>Professional Support</td><td>Career Development</td></tr>
<tr><td>- Mutual support among women in the professional environment;
- Networking among women</td><td>- Support for participation in professional events, conferences, and business trips;</td><td></td></tr>
</table>

[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.

in the industry and their involvement in professional communities; - Involvement of men in gender equality support programs.	- Internship and training programs for women; - Mentorship programs and professional guidance; - Return-to-work programs after maternity leave.	
Family Support	**Organizational Culture/Working Conditions**	**Economic and Political Measures**
- Encouragement and support from family and partners; - Shared household responsibilities (reduction of the double burden on women).	- Flexible working schedules; - Remote or hybrid work formats; - Workplace childcare or childcare subsidies; - Support for work–life balance.	- Government grants and scholarships for women in cybersecurity; - Tax incentives for companies supporting women in cybersecurity; - Funding of STEM education programs for girls; - Legislation to combat discrimination and ensure equal pay; - Legal regulation of flexible work arrangements and maternity leave; - Ensuring a gender-sensitive environment at the national level.

Sources: USAID Project (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).

At the individual (micro) level, several factors are considered that contribute to the professional realization and development of women in the field of cybersecurity. One of the key aspects is self-development, which includes obtaining education and improving qualifications through participation in specialized courses, certification programs, trainings, and conferences[64]. Such a continuous learning process not only provides the necessary technical

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

knowledge but also helps build confidence in one's competencies, which is essential for overcoming stereotypes and prejudices that often accompany women in this field.
An important element is also professional support, which is implemented through active interaction within professional communities and networking. These create favorable conditions for experience exchange, skill development, and increased confidence, as well as help overcome professional isolation that women often experience in technical fields[65]. Moreover, the involvement of men in gender equality support programs and cooperation with them contributes to the formation of a more inclusive environment in the cybersecurity sector, which is important for overcoming stereotypes regarding women's roles in technical fields[66].
Equally important is the factor of family support, which includes emotional support from relatives and partners that helps overcome professional challenges and stress. The equitable distribution of household responsibilities and the reduction of domestic workload for women create conditions for a better work–life balance, which in turn allows them to devote more attention to professional development and career growth[67]. Thus, at the micro level, overcoming barriers for women in cybersecurity is based on the development of personal competencies, the creation of professional support networks among women, and the provision of a supportive family environment, which together form the foundation for a successful career and active participation of women.

The organizational (meso) level encompasses institutional transformations in the field of education, professional training, and the development of career opportunities for women in cybersecurity. One of the key strategies is the expansion of STEM education, which is implemented through motivational initiatives, information campaigns, specialized courses, training sessions, and mentoring programs aimed at preparing qualified cybersecurity professionals[68]. Leading universities, such as the University of Oxford (ranked 1st among higher education institutions) and the Massachusetts Institute of Technology (ranked 2nd)[69], offer a range of programs aimed at attracting women to the field of cybersecurity. These include both university courses on the fundamentals of cybersecurity, cryptography, and network security, as well as student and extracurricular initiatives. For example, the Massachusetts Institute of Technology offers free open online courses available in multiple languages[70] and organizes the summer academic Women's Technology Program for American high school students who excel in mathematics and natural sciences[71]. The activities of the student organization Stanford Women in Computer Science (WiCS) are aimed at supporting women in the technology sector through the organization of workshops and meetings with industry experts, as well as providing mentorship and networking opportunities to support women in the technological field[72]. Such

[65] Проєкт 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] Ibid., 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*.

an approach expands access to high-quality STEM education and enables the development of both fundamental and advanced skills in the technical domain, particularly in cybersecurity.

Despite these efforts, at the stage of obtaining education there remains a problem of "pipeline leakage," whereby the level of interest among girls in cybersecurity decreases as they progress to higher levels of education. One of the initiatives introduced to address this issue is the "Cybersecurity for All" approach, which aims to promote careers in cybersecurity and create a gender-neutral environment[73]. A mandatory aspect of both education and professional practice is also the consideration of gender balance policies among leadership and teaching staff[74].

A notable example is the #NoBiasInCyber campaign by Orange Cyberdefense[75], which aims to overcome stereotypes that discourage women from entering the field. In cooperation with the Women4Cyber organization, it offers specialized training and mentorship programs to support gender and social diversity in cybersecurity.

The implementation of initiatives supporting women in cybersecurity is also carried out through the activities of non-governmental and civil society organizations, as well as corporate programs of leading companies (Google, Microsoft, IBM)[76]. These initiatives create additional opportunities for professional development and career advancement for women in the field. A number of programs, such as CyberFirst[77], Women4Cyber[78], and Cyberdefense, provide practical training and internships and subsequently assist women with employment in cybersecurity. Examples of organizations (initiatives) and the directions of their activities are presented in *Table 1.3.2.*

Table 1.3.2. **Examples of Organizations (Initiatives) and Areas of Their Activities for Overcoming Barriers in Cybersecurity**

Program/Initiative Name		Country	Areas of Activity
CyberFirst Girls Competition		United Kingdom	Government program for schoolgirls aged 11–17 that includes competitions, summer schools, scholarships, and mentoring.
Women4Cyber	**Women4Cyber**	EU	Innovative online platform providing access to

[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] Проєкт 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*.

(non-governmental organization)	**Academy**		professional training: specialized courses, training programs, and certifications.
	Mentorship Programs		Assistance for women in acquiring professional knowledge, expanding professional networks, and increasing confidence
	Women4Cyber Expert Registry		A registry of cybersecurity experts that promotes the visibility of women and their achievements, encourages participation in public events, and creates opportunities for collaboration
	Women4Cyber STARtup		Support for female entrepreneurship and startups (founded by women or with at least 50% women in the team), promotion of women's leadership.
	Publications		Raising awareness and promoting real female role models in cybersecurity (e.g., the book *"Hacking Gender Barriers: Europe's Top Cyber Women"*).
WiCyS (Women in CyberSecurity) **(**non-profit organization)		USA	Comprehensive approach: from education to professional support. Annual conference dedicated to women in cybersecurity for knowledge exchange and professional networking; mentorship programs (WiCyS Mentorship Program), training; scholarships and grants; partnerships with universities and corporations (internship and employment opportunities).
Google Women Techmakers (WTM) global initiative by Google	**Women Techmakers Story**	Global (operates in over 75 countries)	Increasing visibility and inspiration, challenging stereotypes through success stories of women technologists from different parts of the world.
	Black Women in Tech		Increasing representation of Black women in the technology sector through access to learning platforms.
	She Builds AI		Expanding opportunities through education in artificial intelligence, mentorship, community support, participation in workshops, and project-based learning.

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

The implementation of these programs has led to an increase in the number of women participating in educational and professional initiatives in cybersecurity. In 2024, a record

number of 15,000 girls registered to participate in the CyberFirst Girls Competition organized by the UK National Cyber Security Centre (NCSC), indicating growing female engagement in cybersecurity[79]; in 2023, 600[80] participants took part in the Women4Cyber mentoring program; more than 1,900 women from the United States participate annually in WiCyS conferences, with even more joining mentoring and educational programs[81], while the Girls Who Code initiative has engaged over 670,000 participants since its establishment in 2012[82].

Thus, organizational-level initiatives contribute to overcoming barriers for women in cybersecurity through skill development, the formation of professional networks, and increasing women's visibility in the field.

Despite educational initiatives, women in cybersecurity encounter career barriers and gender bias already in the workplace. In the European Union, women earn on average 13% less than men, which corresponds to approximately one and a half months of unpaid work per year in the same position. This gender pay gap is one of the main obstacles to equal participation of women in the professional sphere, including cybersecurity[83]. According to recent studies, women constitute only about 22–25% of the global cybersecurity workforce, and these figures are even lower in leadership positions[84]. Despite the efforts made, at the current pace of progress, according to the World Economic Forum, achieving full gender equality will not be possible before 2158, meaning that more than five generations (over 130 years) will still be required[85].

Accordingly, it is necessary to accelerate the elimination of systemic barriers and biases at the macro level (within industry, government, and society) through the implementation of gender equality policies that promote inclusion, eliminate discrimination, and create gender-sensitive working environments. For this purpose, as an instrument of positive discrimination, the establishment of mandatory quotas for women in job competitions has been proposed[86]. For example, France has introduced quotas for women on the boards of directors of large companies ("Women on Boards"), which contributes to increasing their representation in leadership positions[87].

Particular attention in overcoming barriers is given to counteracting discrimination and gender stereotypes in cybersecurity. To achieve this, reforms of educational programs have been

[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 Keport.* 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.

proposed to increase awareness of the importance of gender equality, particularly in cybersecurity, and to promote the early involvement of girls in STEM disciplines by challenging gender stereotypes. The European Commission encourages female entrepreneurship and educational development through its DIGITALEUROPE and Horizon Europe programs, whose main condition is ensuring gender equality[88].

The next step involves the development of state policies aimed at reintegrating women into the workforce after maternity leave, including financial support, flexible working arrangements, and opportunities for retraining[89]. Overall, the further development of cybersecurity requires a systematic approach to the formation of gender-sensitive policies and the reduction of gender imbalance in cybersecurity.

In this context, an important factor is the role of female leaders who have already achieved success in cybersecurity and actively promote the field. In particular, Katie Moussouris, a cybersecurity expert and founder of Luta Security, is one of the pioneers in the implementation of "bug bounty" programs—initiatives that encourage the identification of vulnerabilities in software. She was among the first to introduce such programs at Microsoft and co-initiated the U.S. Department of Defense project "Hack the Pentagon" [90] , which became a revolutionary step in government cybersecurity.

Another prominent example of successful women in cybersecurity is the American engineer and technologist Megan Smith, who served as the Chief Technology Officer of the United States and previously as a Vice President at Google. There, she co-founded the "Women Techmakers" initiative, which aims to support women's participation in STEM fields[91]. Her work contributes not only to increasing the visibility of women in technical domains but also to creating structural pathways for their professional development. A significant contribution to overcoming barriers is also made by Jessica Gulick, founder of Katzcy, a company specializing in cybersecurity marketing and strategy[92]. Under her leadership, mentoring and training programs are implemented to help women develop professional skills and engage in networking. She also participates in conferences and forums dedicated to gender equality in technology, where she delivers presentations and organizes panel discussions. Through the activities of such female role models, a positive image of women in cybersecurity is formed, which is an important factor in overcoming stereotypes and encourages younger generations of girls to pursue careers in cybersecurity.

[88] Ibid., p. 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.*

Chapter 2. Women's Participation in Cybersecurity in Ukraine

2.1. Statistical Information on Women in Cybersecurity: Education and the Labor Market

Hryvtsov Volodymyr, Smolenska Yuliia, Onishchenko Artur

2.1.1. Women in Higher Education Institutions in Cybersecurity Programs in Ukraine

In order to determine the characteristics of gender distribution in Ukrainian higher education institutions (HEIs), seven leading institutions across the country were selected. This was done using a self-developed index of university demand for the educational program (abbreviated as IUDP — Index of University Demand for the Program). The development of this indicator was driven by the absence of relevant analogues[93]. Although attempts to create rankings of higher education institutions already exist, they primarily focus on only one criterion, for example, the average admission score of applicants. Such a method does not consider other important indicators, such as the number of students enrolled in the selected educational program, which may be a source of systematic bias. Other similar indices attempt to calculate the quality of education provided but do not reflect the institution's popularity among applicants.[94]

In turn, the methodology proposed in this study is based on three main indicators: **the total number of enrolled students, the average External Independent Testing (EIT) score of admitted students, and the competition for one state-funded place**. These indicators combine representativeness and ease of data collection. As shown in Table 2.1.1.1, no strong correlation was found between these variables, which indicates their independence. In addition, Bartlett's test of sphericity did not show statistical significance (p = 0.233), indicating the absence of grounds for reducing the variables to a single latent factor. Thus, each variable reflects a separate aspect of university evaluation. To balance the scale of the indicators and ensure their comparability within the integrated index, min–max normalization was applied, transforming the values into the interval [0;1].

Table 2.1.1.1. **Correlation matrix for the components of University Demand Index for an Educational Program (UDI-EP), 2024 admissions[95]**

	Average	Number of enrolled	Competition

[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.UA"

		score	students	
Correlation	**Average score**	1,000	-0,072	-0,414
	Number of enrolled students	-0,072	1,000	0,025
	Competition	-0,414	0,025	1,000

As a result, the formula of UDI-EP takes the following form: $\mathrm{UDI\text{-}EP}_n$[96]

(where x_n is the average admission score of applicants to a particular university, y_n is the number of enrolled students, z_n is the competition rate, and x_{max}, y_{max}, z_{max} represent the highest values among all higher education institutions, respectively). The index is a linear variable and takes values from 0 to 3.

The number of enrolled students reflects the actual scale of education in the specialty "Cybersecurity" at higher education institutions. Competition per place serves as an indicator of applicants' demand and the attractiveness of the institution and its program. The average score of admitted students demonstrates the academic level of students and the selectivity of admission.

Within this study, the UDI-EP was calculated based on the results of the 2024 admission campaign for the specialty "Cybersecurity." The data were manually collected from the website Vstup.OSVITA.UA (n.d.).

In this case x_{max} = 168.78, y_{max} = 327, z_{max} = 18,75. As a result, a list of 15 leading higher education institutions was determined (see Table 2.1.1.2) based on data from the web resource Osvita.ua[97], which is linked to information from the state register of the Unified State Electronic Database on Education (ESEDO). The highest average admission score was recorded by Taras Shevchenko National University of Kyiv; the largest number of enrolled students was recorded by Lviv Polytechnic National University; and the highest competition per state-funded place was recorded by the National University of Kyiv-Mohyla Academy. The top three universities included Lviv Polytechnic National University, the National University of Kyiv-Mohyla Academy, and Igor Sikorsky Kyiv Polytechnic Institute.

Table 2.1.1.2. **Top 15 Higher Education Programs by the UDI-EP, 2024**

University	Average admission	Number of	Competition per state-funded	Total I UDI-EP score

[96] Формула 2.1. Розрахунок індексу ІУЗдОП.

[97] Вступ.Освіта.UA. Пошуковий запит: Кібербезпека та захист інформації; бакалавр.

	score of all admitted students	enrolled students	place	
Lviv Polytechnic National Universit	159,88	**327**	4,56	1,84
National University of Kyiv-Mohyla Academy	162,03	36	**18,75**	1,73
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”	165,97	205	4,81	1,54
State University of Information and Communication Technologies	138,9	53	15,67	1,39
State University of Trade and Economics	141,46	113	10,5	1,32
Taras Shevchenko National University of Kyiv	**168,78**	96	5,29	1,26
Ivan Franko National University of Lviv	167,41	47	7,47	1,22
State University of Information and Communication Technologies (Management	147,42	108	5,21	1,08
National Aerospace University named after N. Ye. Zhukovsky “Kharkiv Aviation Institute”	163,74	16	7,13	1,07
National University of Life and Environmental Sciences of Ukraine	140,65	58	8	1,01
Sumy State University	161,21	32	5,4	1,00
V. N. Karazin Kharkiv National University	163,07	49	3,56	0,97
Borys Grinchenko Kyiv Metropolitan University	145,54	65	5,87	0,97
Odesa Polytechnic National University	160,15	61	3,33	0,97
Kharkiv National University of Radio Electronics	164,48	42	3,4	0,95

After this, a search was conducted for data on the ZNO[98] scores of admitted applicants enrolled in bachelor’s programs at universities, as well as data on the winter examination sessions of first- to fourth-year students from open sources on the official university websites. As a result, data on ZNO results were found for the two highest-ranked universities: Lviv Polytechnic

[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).

National University and the National University of Kyiv-Mohyla Academy. These institutions differ in terms of region and size, which makes them appropriate for comparison. During the analysis of applicants, those who were admitted under quota-based admission were excluded due to the anonymization of their full names and the inability to identify their gender. At the same time, for the analysis of the gender distribution of students in universities, the results of winter examination sessions of first- to fourth-year students at the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" and the State University of Information and Communication Technologies were analyzed. The attribution of gender characteristics to individuals was performed using the language-based artificial intelligence ChatGPT, followed by manual editing. Coding, analysis, and visualization were carried out using Excel software.

There is a lack of data on women's employment in the cybersecurity sector in Ukraine. Oral requests were made to the Main Directorate of Intelligence of the Ministry of Defense of Ukraine, the Security Service of Ukraine, and the State Service of Special Communications and Information Protection of Ukraine; however, access was denied due to data confidentiality.

2.1.2. Women in the Cybersecurity Sector Worldwide

Horizontal gender segregation can be observed in the cybersecurity sector worldwide, although the percentage of female cybersecurity specialists varies depending on the country. According to estimates by the Global Cybersecurity Forum, approximately 24% of specialists in this field are women *(Figure 2.1.2.1).* By region, the Asia-Pacific region has the highest proportion (almost 25%). This can be explained by the recent acceleration in the development of STEM fields in this region. As a result, most employees obtained their education under conditions of reduced gender segregation. In contrast, Africa has the lowest share — 13.5%. In Europe, the proportion of women working in cybersecurity is 22.4%. As shown in *Figure 2.1.2.2,* as of 2022, a gender gap in the representation of women and men in the cybersecurity sector exists in all countries worldwide. Only in two countries did more than one-third of employees turn out to be women, namely Nigeria and Mexico. Since Africa is the region with the lowest share of women in cybersecurity, Nigeria may represent either an exception or a possible calculation error by researchers. At the opposite end of the list are Japan, Germany, and the United States, with values ranging from 10% to 13%.The graph also shows that among the five countries with the smallest gender gap, almost none belong to the group of the wealthiest states, while the largest gender gap is observed exclusively in affluent countries. This may indicate a lower level of horizontal gender segregation in countries with less economically advantaged populations.

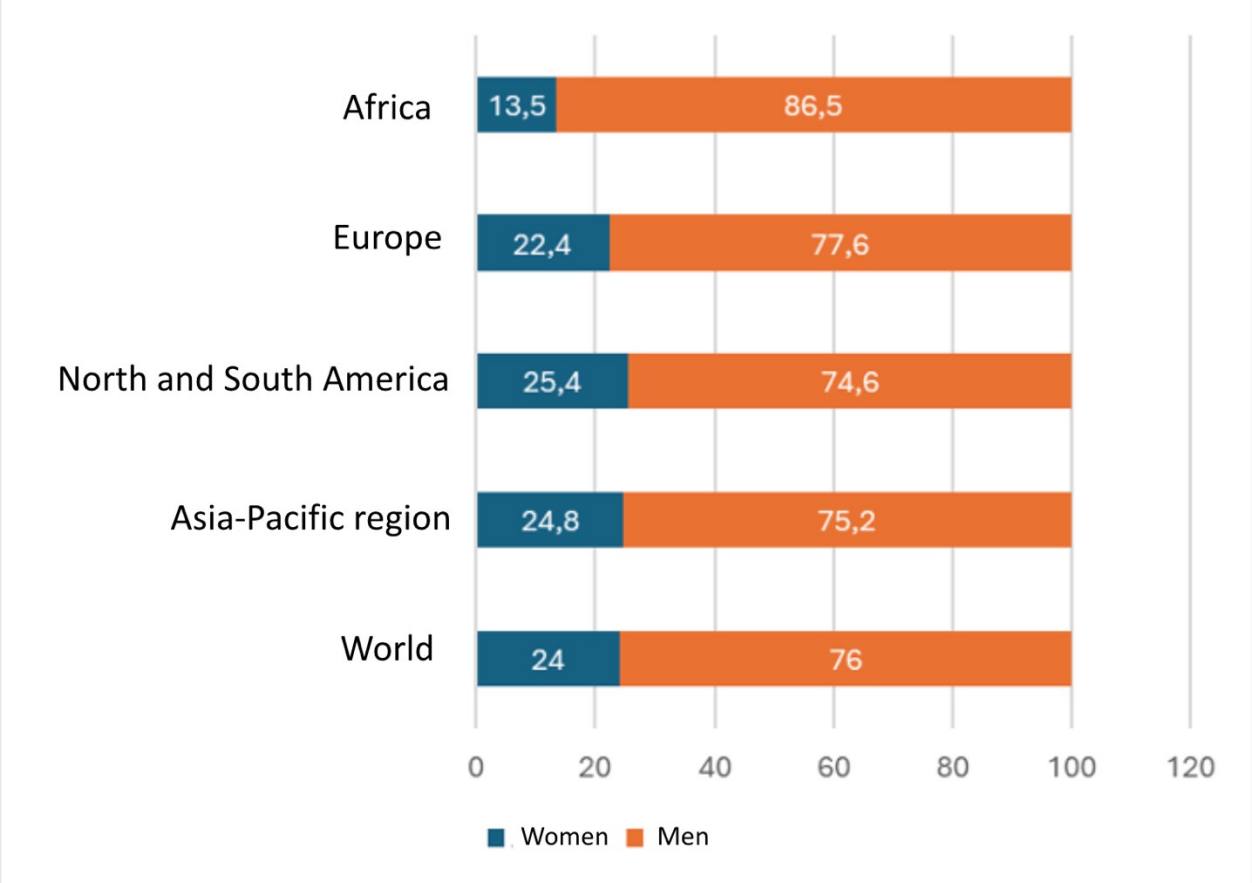


Figure 2.1.2.1. **Gender distribution in the cybersecurity sector by region in 2024 (%)**[99]

Figure 2.1.2.2. **Gender distribution in the cybersecurity sector: five countries with the highest and lowest shares of women in 2022 (%)** [100]

However, there is indirect evidence of a decrease in horizontal segregation over time. Such conclusions can be drawn from statistics on the distribution of employees in this field by gender and age, as demonstrated in *Figure 2.1.2.3*. The highest percentage of women (24%) is observed in the age category under 30, while their share decreases with increasing age. In the 30–38 age category, women account for 20%, whereas in all older categories the share remains at approximately 15%.

[99] Global Security Forum, 2024, c. 15.
[100] ISC2, 2022, c. 41.

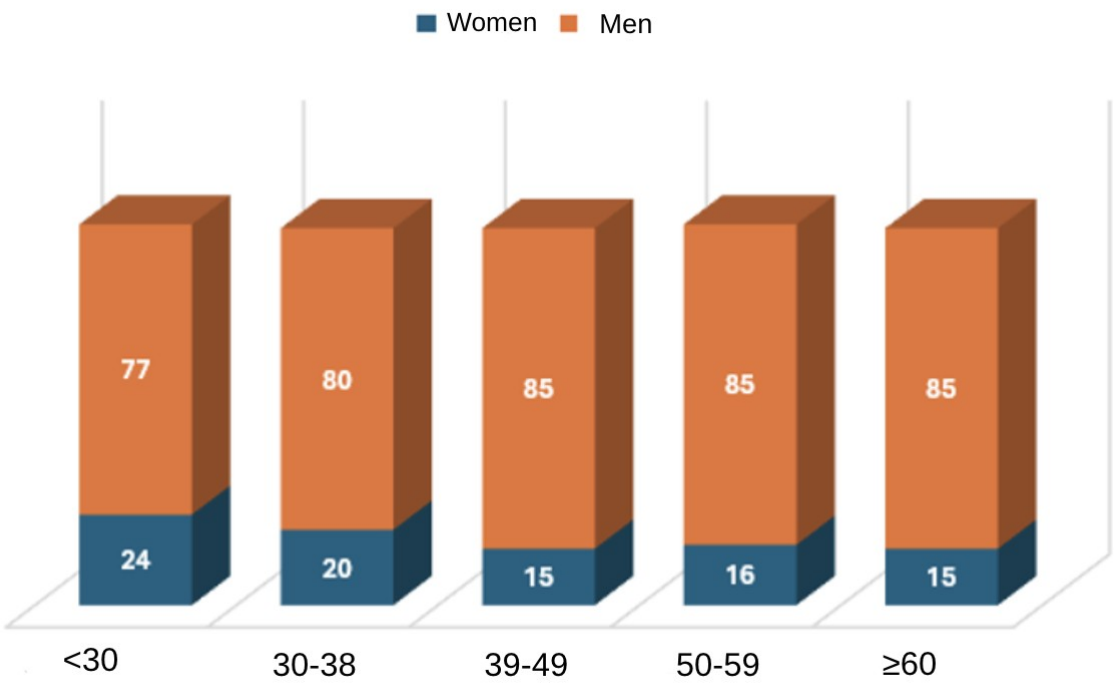
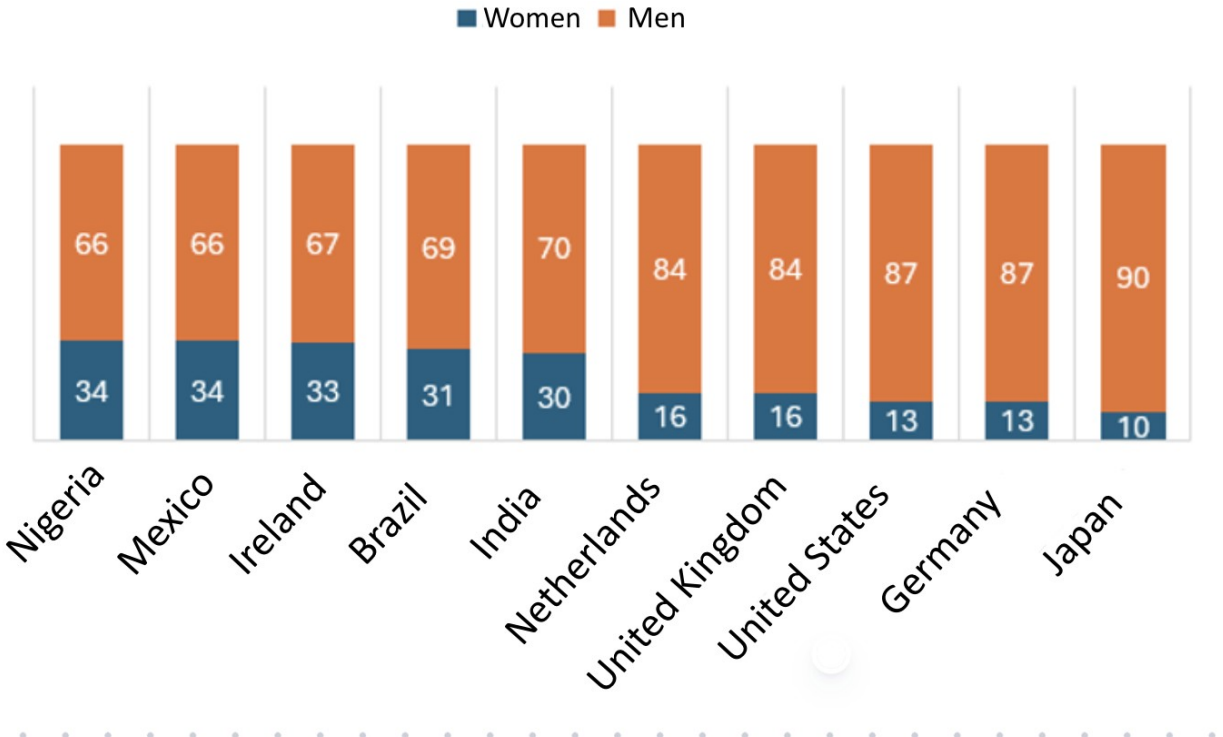


Figure 2.1.2.3. ***Gender–age distribution in the cybersecurity sector worldwide in April–May 2023 (%)***[101]



[101] ISC2, 2023, c. 39.

The data also demonstrate the phenomenon of vertical segregation in this field, as in 2024 "only 16% of all CISOs (Chief Information Security Officers) are women[102]." Thus, the glass ceiling (an invisible barrier to attaining leadership positions) in this case can hardly be considered insurmountable, as the existing indicator is only about one-third lower than the overall share of women in the cybersecurity sector, which amounts to 24%.

In addition to segregation, a gender pay gap also exists globally. As shown in the graph in *Figure 2.1.2.4*, women in cybersecurity earn on average USD 109.61 thousand per year, which is 4.9% less than men.

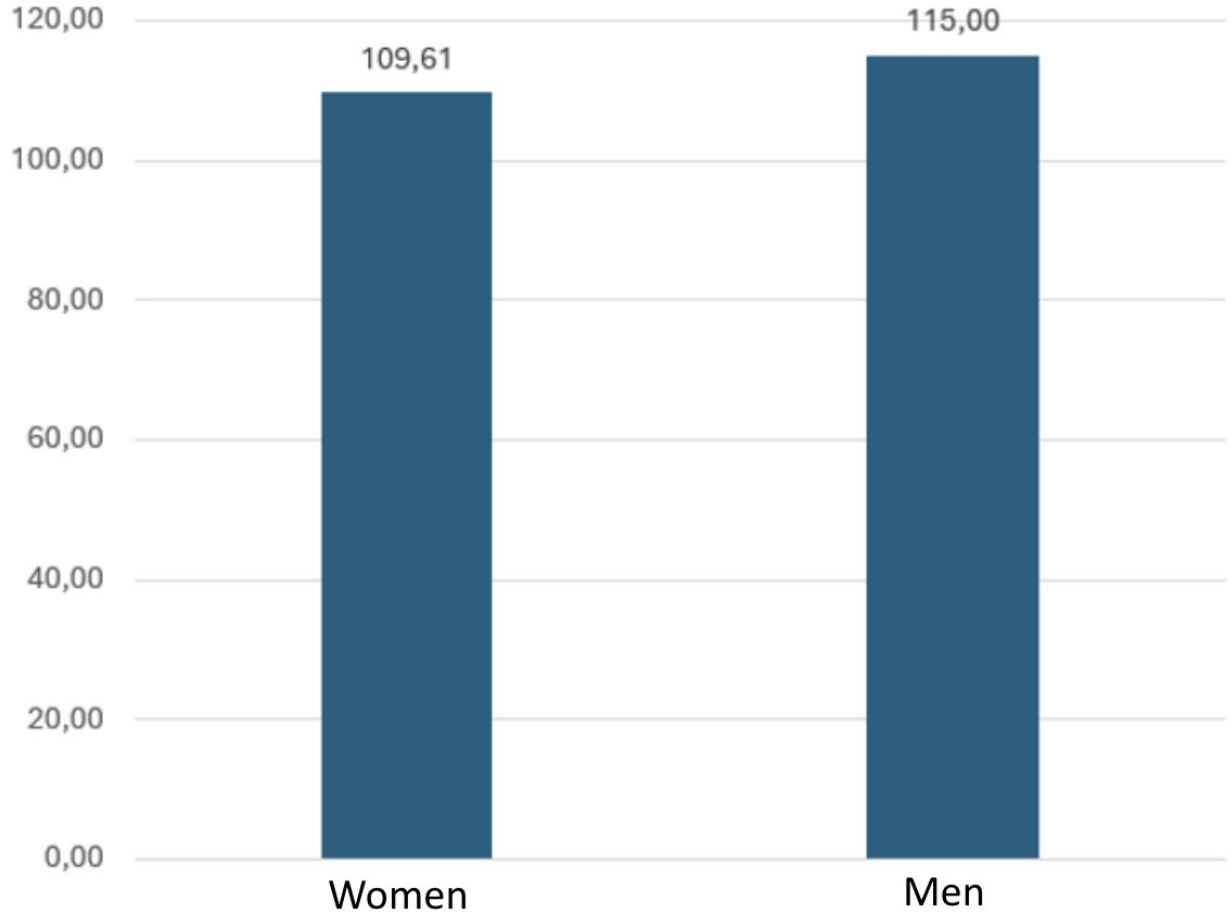


Figure 2.1.2.4. **Gender pay gap in the cybersecurity sector worldwide in April–May 2023 (thousand USD per year)**[103]

Regarding education, it has also been established globally that, on average, female cybersecurity specialists have a higher level of education than their male colleagues. As demonstrated in *Figure 2.1.2.5*, women are more likely to obtain a master's degree or higher. In

[102] Cybersecurity workforce report, 2024, c. 15.
[103] Borgeaud, 2024.

contrast, men have a slightly higher probability of working in the cybersecurity sector with general, vocational, or incomplete higher education.

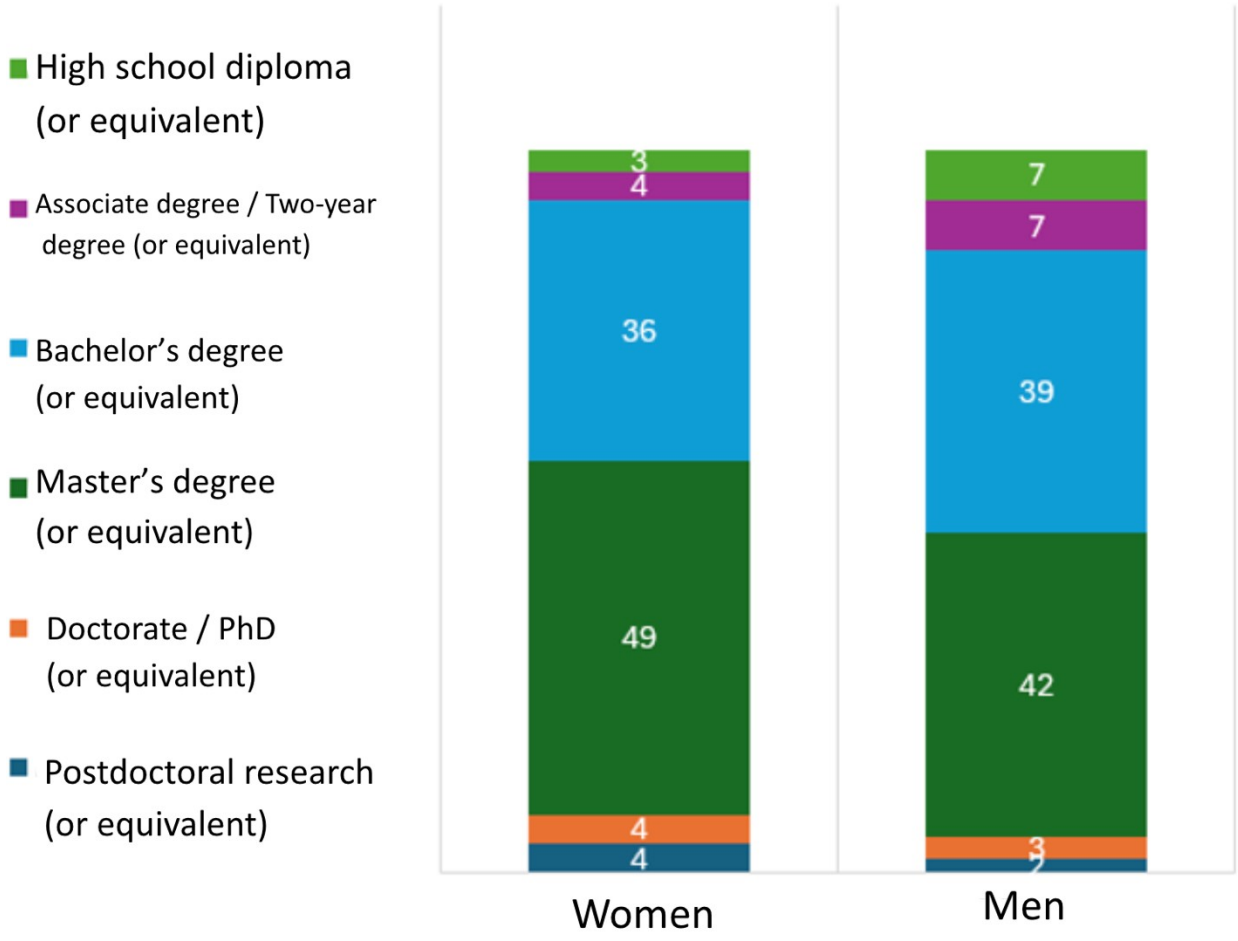


Figure 2.1.2.5. **Differences in education level by gender in the cybersecurity sector worldwide in 2022 (%).**[104]

2.1.3. Women in Cybersecurity Education in Ukraine

Gender segregation manifests itself from an early age and becomes particularly visible when choosing a field of study in higher education institutions. In the two educational programs under specialty 125 "Cybersecurity" that were most popular among applicants in 2024 (see Table 2.1.3.1), the share of women among students admitted to this specialty averaged 27.4%. At the same time, the gap between the average admission scores of men and women is insignificant (less than 4%), with women having a slight advantage in one university and men in another.

Table 2.1.3.1. **Comparative table of gender segregation among admitted students in the top two educational programs under specialty 125 in 2024.**

[104] ISC2, 2022, c. 52

	Lviv Polytechnic National University		Kyiv-Mohyla Academy	
Gender	Men	Women	Men	Women
Number of individuals*	236	82	25	10
% of total admitted students	74,20%	25,8%	71%	29%
Average admission score	159,3	**160,9**	**163,5**	159,2

Data obtained from the official websites of the National University of Kyiv-Mohyla Academy [105]and Lviv Polytechnic National University[106].

Quota-based admissions were excluded from the analysis.

The results of the winter examination sessions for years 1–4 in specialty 125 “Cybersecurity” at the State University of Information and Communication Technologies and the National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” indicate horizontal gender segregation in cybersecurity education: the average share of women is 26%. At the same time, a general trend of increasing numbers of female students in cybersecurity can be observed over time: among fourth-year students, who enrolled in 2021, the average share of women was 22%, whereas among first-year students admitted in 2024, the average share has already reached 29% (*see Figure 2.1.3.2 and Figure 2.1.3.3).*

[105] Ranked List of Applicants under the Bachelor's Educational and Professional Program in Specialty 125 for 2024. Cybersecurity and Information Protection. Admissions to NaUKMA.

[106] Ranked List of Applicants Admitted to the First Year of Full-Time Study under the Bachelor's Educational and Professional Program in Specialty 125. Cybersecurity and Information Protection at Lviv Polytechnic National University. Admissions 2024.

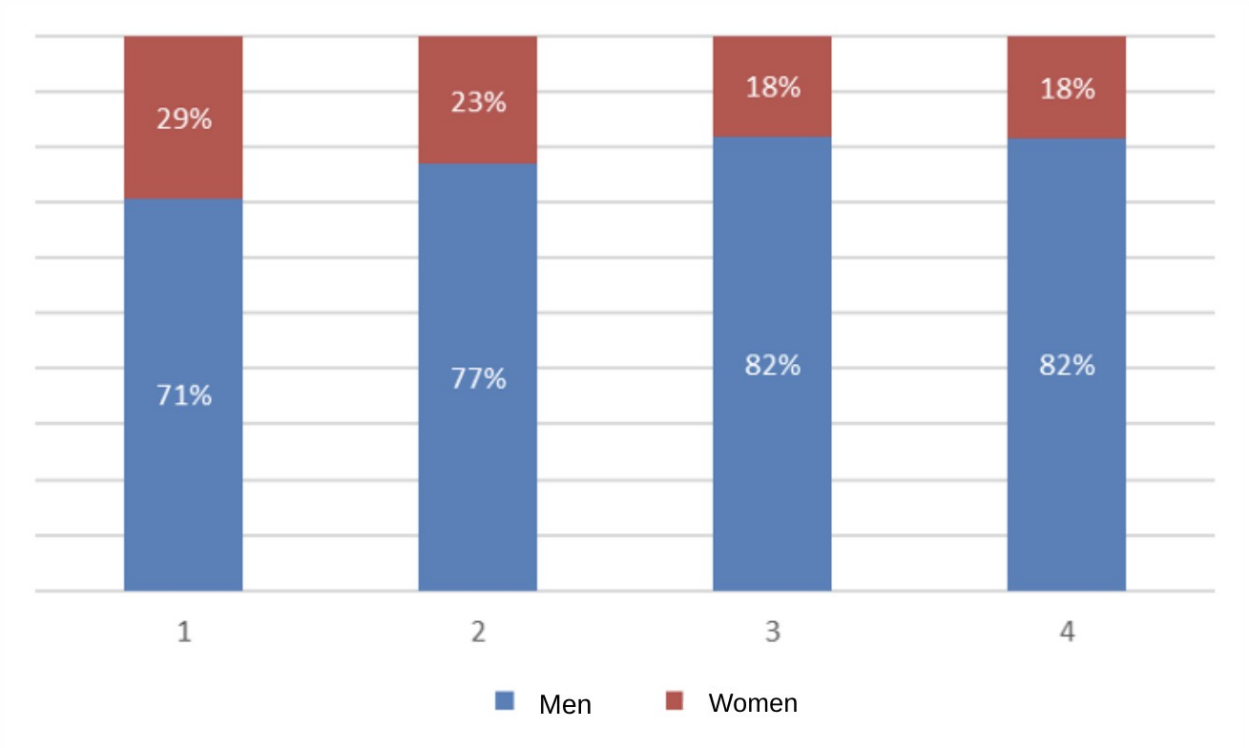


Figure. 2.1.3.2. **Gender distribution among first–fourth year students at the State University of Information and Communication Technologies in the 2024/2025 academic year[107].**

[107] Student Performance Rankings of the Educational and Research Institute of Cybersecurity and Information Protection (Autumn Semester 2024–2025 academic year). State University of Information and Communication Technologies.

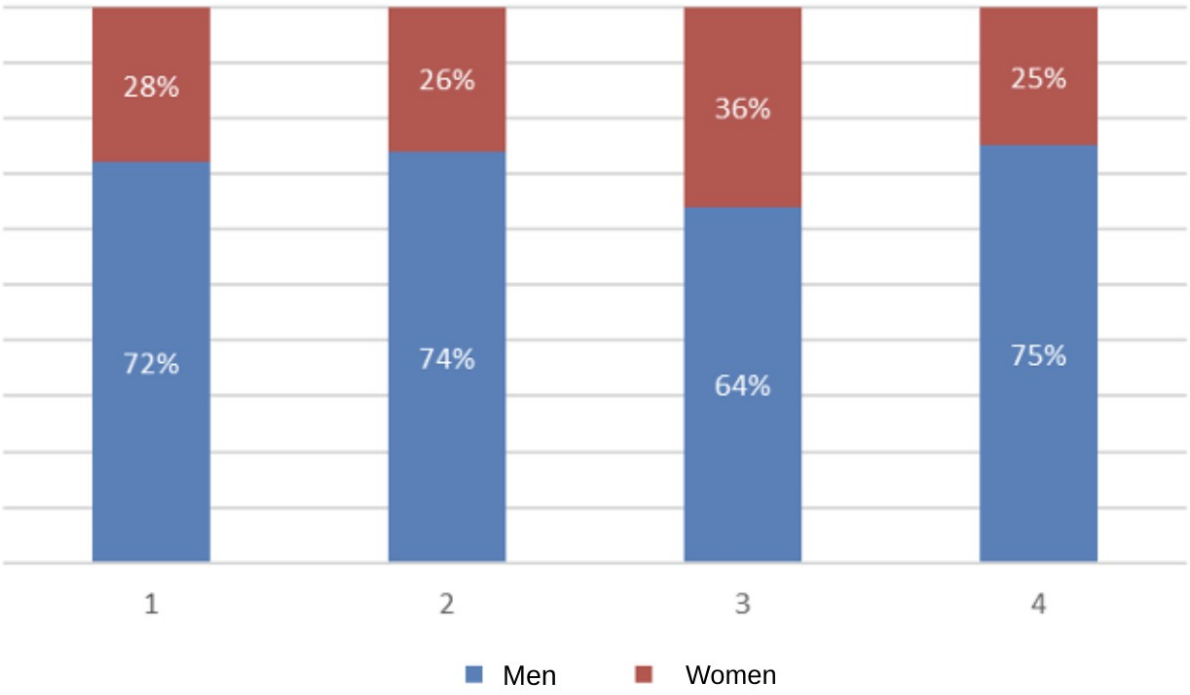


Figure 2.1.3.3. **Gender distribution among first–fourth year students at the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" in the 2024/2025 academic year.**[108]

[108] Student Performance Rankings of the Institute of Physics and Technology (IPT) based on the results of the Winter Semester Assessment 2024/2025 academic year. Department of Academic and Educational Affairs, Igor Sikorsky Kyiv Polytechnic Institute.

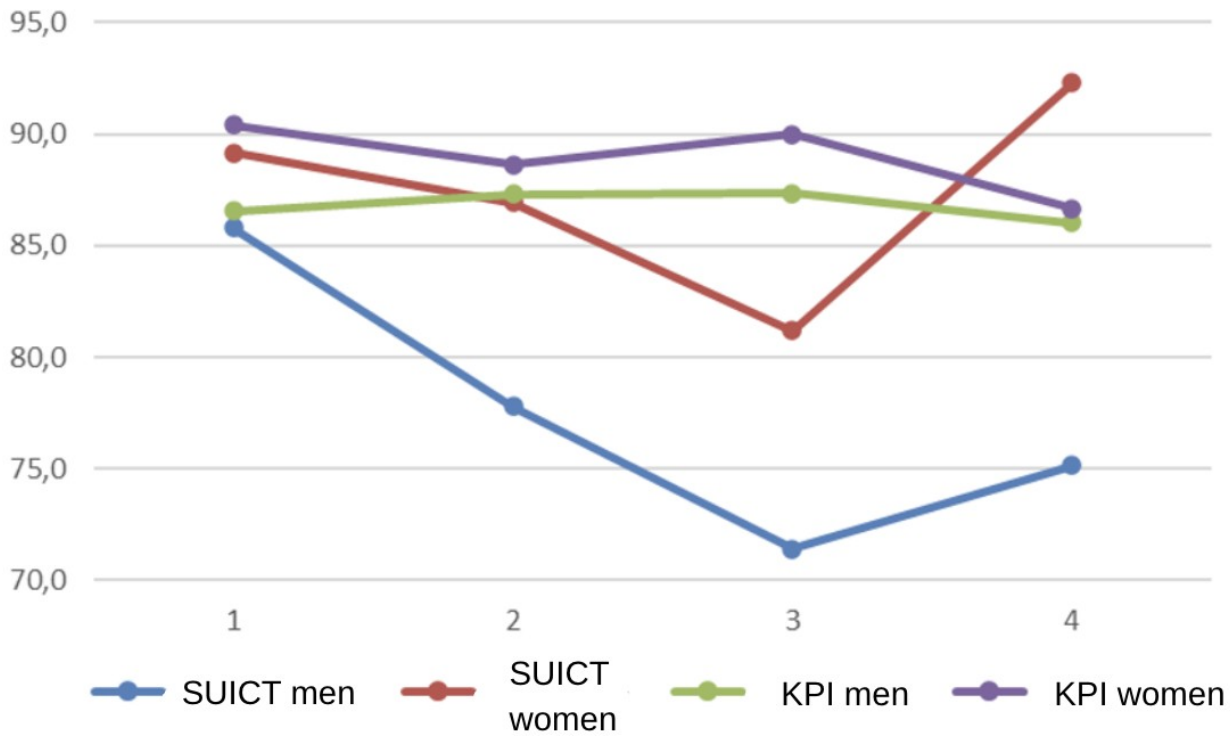


Figure 2.1.3.4. **Average ranking score of male and female students based on the winter examination session of the 2024/2025 academic year (years 1–4) at the State University of Information and Communication Technologies and the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (KPI).**

This trend may be associated with the beginning of the full-scale invasion of Ukraine in 2022 and the increased demand for cybersecurity specialists. However, it may also be explained by other factors, such as the systematic dropout of women in later years of study. Regarding academic performance, women consistently outperform men in ranking scores, with a gap ranging from 1% to 23% (see Figure 2.1.3.4).

2.2. The Situation in Ukraine and the Regulation of Gender Relations in Cybersecurity

Sydorov Rostyslav, Chorna Viktoriia, Vasylenko Polina, Kuchabska Kateryna

2.2.1. Legal Framework of Cybersecurity in Ukraine

European countries, particularly within the EU framework, are developing legal mechanisms to combat such phenomena. For example, **Directive 2011/93/EU of the European Parliament on combating the sexual exploitation of children** also covers online crimes that contain a gender dimension.[109] In addition, in December 2022 the European Commission initiated the

[109] Directive 2011/93/EU of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0093

development of a separate directive on combating gender-based violence online[110], which proposes the criminalization of digital stalking, non-consensual dissemination of intimate images, and online defamation.

To understand the specifics of the formation of gender relations in Ukrainian cybersecurity, the research should begin with a thorough analysis of current state policy and legislative acts, as they establish the regulatory framework and reflect the level of institutional support for gender equality in this strategically important sector for Ukraine.

The regulatory framework of cybersecurity in Ukraine is primarily based on a technocratic approach focused on protecting information systems, critical infrastructure, and preventing cyber threats at both the state and private sector levels. At the same time, current policies almost entirely overlook the impact of digital threats on different social groups, particularly based on gender. As a result, specific risks faced by women in the online environment (including cyber violence, harassment, and sextortion) remain outside the scope of sectoral strategies. Unlike certain international practices that recognize women's vulnerability to specific forms of digital threats, Ukrainian cybersecurity policies have so far neglected these aspects.

The central legal act in the field of cybersecurity is the **Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" of October 5, 2017, No. 2163-VIII**[111]. The document regulates the activities of state authorities, law enforcement agencies, operators of critical infrastructure, and business entities in the field of cyber protection. However, the text contains no references to gender equality, anti-discrimination measures, or support mechanisms for women in the cybersecurity sector. Instead, the law includes general provisions that may be interpreted as a potential basis for gender-sensitive interpretation. Only a general reference to the principle of non-discrimination (Article 2, paragraph 6) may be interpreted as allowing gender-sensitive interpretation, according to which "decisions, actions, and omissions of public authorities must not result in differences in rights and obligations of individuals in similar situations unless such differences are necessary and minimally sufficient to satisfy the public interest[112]." Although this provision may be applied in a broader context of equality, it does not emphasize the gender-specific nature of cyber threats nor provide mechanisms to ensure equal access for women to the cybersecurity sector.

Thus, the Law "On Cybersecurity" is gender-neutral but not gender-sensitive, which contradicts modern European security practices where digital rights, including protection from gender-based online violence, are integrated into the overall security strategy. For example, **EU Directive 2024/1385** provides for the criminalization of such forms of cyber violence as unauthorized distribution of intimate images, deepfakes, cyberstalking, doxing, and cyberflashing, and obliges member states to ensure specialized assistance for victims and

[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
[111] Закон України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII https://zakon.rada.gov.ua/laws/show/2163-19
[112] Верховна Рада України. (2017)

preventive mechanisms. The focus of this policy is the recognition of digital threats as a factor of systemic inequality that limits women's public participation, particularly in media, politics, and the security sector.

At the level of analytical institutions, such as the **European Institute for Gender Equality (EIGE, 2024)**, the need for specific measurement and policy instruments to address cyber violence, which disproportionately affects women, is also emphasized. The absence of similar provisions in Ukrainian legislation not only limits opportunities to protect vulnerable groups but also highlights the need to reconsider approaches to digital security as a multidimensional phenomenon requiring consideration of social, legal, and gender factors.

Ukrainian legislation does not contain specific provisions addressing the gender dimension of cyber threats, although research shows that women are a disproportionately vulnerable group in the digital environment. According to data from the European Institute for Gender Equality (EIGE, 2017), one in ten women in the EU has experienced cyber violence since the age of 15, including cyberstalking, sextortion, non-consensual dissemination of intimate content, blackmail, or threats on social media. These forms of violence are often combined with physical or sexual violence in real life: 77% of women who experienced cyber harassment also experienced violence from a partner[113].

In this context, the absence of similar provisions in the Ukrainian legal system indicates the need to update cybersecurity policy to account for the gender-specific nature of risks. This is particularly critical during wartime, when the level of aggressive digital communication targeting women — including female military personnel, activists, and journalists — increases.

The Ukrainian regulatory framework in this area remains fragmented. Despite the silence of the specialized cybersecurity law, several related legal acts provide a foundation for incorporating a gender dimension into digital policy. In particular, the **Law of Ukraine "On Ensuring Equal Rights and Opportunities for Women and Men"**[114] establishes the obligation of public authorities to implement gender equality in all areas of public administration, including information policy. Importantly, the law provides gender legal expertise — an effective mechanism for assessing legal acts for gender discrimination, which can (and should) be applied to regulations governing cybersecurity.

Similarly, the **Law of Ukraine "On Prevention and Combating Discrimination"** [115]formalizes the possibility of legally challenging discriminatory practices. In the context of the digital sphere, this means that barriers faced by women in accessing IT and cybersecurity professions, including structural discrimination or hidden gender biases, may be subject to legal review and correction. However, in practice, mechanisms for implementing these provisions remain

[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.
[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

ineffective due to the absence of clear administrative procedures, responsible authority, and monitoring tools.

An important document in the field of digital security is the **Implementation Plan of the Cybersecurity Strategy of Ukraine**, approved by the National Security and Defense Council on December 30, 2021, and enacted by Presidential Decree No. 37/2022[116]. This plan is designed for a five-year period; therefore, updates to both the Strategy and its implementation plan are expected in the near future. This creates a foundation for updating approaches to digital security by incorporating gender factors and integrating a gender component into state cyber policy.

The document outlines a number of goals and measures aimed at strengthening the state's capacity for cyber defense, responding to cyber incidents, developing critical information infrastructure, and harmonizing international standards. In particular, it provides for the creation of cyber forces, incident management systems, a national cyber crisis response plan, the introduction of mandatory information security audits, and the development of cyber education and research in Ukraine.

However, analysis of the document reveals the absence of a systematic gender approach: the Plan completely ignores issues of gender inequality and gender-based cyber threats. None of its priorities, including the development of human capital in cybersecurity, contain references to the need to consider the needs of women or other socially vulnerable groups. This indicates the dominance of a technocratic discourse in Ukraine's cybersecurity strategy, within which issues of inclusion, diversity, and social justice remain outside the scope of attention.

As a result, despite its potential to transform state cyber policy into an innovative and resilient system, the Strategy is implemented without integrating a gender perspective, which contradicts modern approaches to digital security that recognize the uneven impact of cyber threats on different social groups.

2.2.2. State Initiatives and Programs for Gender Inclusion in Cybersecurity

Despite the limited gender sensitivity of key legislative acts and strategic documents identified in the previous analysis, recent years in Ukraine have witnessed a gradual emergence of regulatory and policy awareness regarding the need for gender inclusion in the cybersecurity sector. Although specialized state policies aimed at integrating a gender perspective into digital security remain fragmented and largely declarative, certain institutional initiatives demonstrate progress toward recognizing the importance of women's participation in national cyber resilience. A gradual shift is taking place from a purely technocratic approach toward a more inclusive paradigm of digital security that takes into account social risk factors, including gender inequality.

[116] Про План реалізації Стратегії кібербезпеки України https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

A notable example is the increased activity of the **National Cybersecurity Coordination Center (NCCC) under the National Security and Defense Council of Ukraine**, particularly through public support for women's leadership in cybersecurity. In December 2024, the 32nd meeting of the National Cybersecurity Cluster was held, dedicated to the topic *"The Role of Women in Ensuring Ukraine's Cyber Resilience: Challenges and Prospects*[117]*."* The event, organized by the NCCC in cooperation with the NGO *Women's Leadership and Strategic Initiatives Foundation*, the U.S. Civilian Research and Development Foundation, and with support from the U.S. Department of State, became the first in a series of events aimed at institutionalizing the gender dimension in Ukraine's cybersecurity policy. During the opening of the event, Deputy Secretary of the National Security and Defense Council of Ukraine Serhii Demediuk emphasized: "The involvement of women in cybersecurity significantly enhances our ability to counter cyber threats. Women possess a unique way of thinking that complements men's approaches, creating synergy that enables the successful resolution of the most complex challenges. We must promote opportunities for more women and girls to find their place in the cyber domain, as their potential can strengthen our capabilities at all levels — from operational activities to strategic planning and decision-making."[118]

Natalia Tkachuk, Head of the Information and Cybersecurity Service of the National Security and Defense Council of Ukraine, noted: "During Russia's full-scale invasion, the involvement of women in cybersecurity is not merely an issue of equality or compliance with international standards. It is a vital necessity for strengthening national security and ensuring state resilience. Women have always played an important role in the development of our country, and today their contribution is becoming even more significant. We must create opportunities for professional growth and development at all levels — from education to leadership positions — facilitating the involvement of new talent in cybersecurity. This not only strengthens our economy and technological development but also contributes to our collective victory in the struggle for Ukraine's future."[119] An important component of the event consisted of practical sessions during which participants developed proposals for a national initiative aimed at improving gender equality in cybersecurity. These developments have the potential to form the basis for future policies to expand women's participation in digital governance, particularly in the context of regulatory development and the implementation of gender-sensitive cyber resilience standards. An important instrument for implementing these goals and fulfilling the state's international commitments is the **National Action Plan for the implementation of UN Security Council Resolution 1325 "Women, Peace, and Security."** With support from international partners, the Government of Ukraine has integrated into this National Action Plan a series of measures that not only opened access for women to specialized cybersecurity courses but also secured their right to participate in shaping national protection standards[120]. According to a 2022 report by the Kyiv City State Administration, expert groups and advisory councils on cyber defense are now required to include representatives of women's clusters,

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

whose opinions genuinely influence defense policies. In parallel, **UN Women** coordinated workshops and grant programs[121]. Without such a multisectoral approach, the genuine realization of women's potential in cybersecurity would remain merely declarative. In addition to state initiatives implemented under the auspices of the National Cybersecurity Coordination Center, Ukraine actively implements cross-sectoral programs aimed at supporting, training, and engaging women in digital security. These initiatives vary in format — from civil society platforms to state retraining programs — and play a key role in developing an inclusive workforce for the cyber sector.

In February 2025, Kyiv hosted the joint event **"Cyber Innovations and Resilience: Women4Cyber Talks,"** which brought together over 100 representatives from the public, private, and academic sectors. Its goal was to shape a national discourse on the role of women in ensuring Ukraine's cyber resilience[122]. Leading experts in digital security participated in the event, along with mentors for female students, demonstrating the growth of horizontal connections within the professional community.

The project **"Reskilling Ukraine"** is a large-scale retraining program focused on women and veterans who lost their jobs because of the war. The initiative is implemented by the Swedish non-profit organization Beredskapslyftet in partnership with the Ministry of Economy of Ukraine and with support from the Government of Sweden, private Swedish foundations, and businesses[123]. The project actively cooperates with public authorities, organizations, and businesses in promoting inclusivity and social responsibility, thereby contributing to the development of an inclusive environment and supporting women's leadership in cybersecurity[124].

The leadership program for women involved in the digitalization of public services, launched by the **United Nations Development Programme (UNDP) in Ukraine** in partnership with CDTO Campus and funded by the Government of Sweden, represents a significant example of an international-state initiative directly promoting gender inclusion in digital public governance[125]. Although the program does not focus exclusively on cybersecurity, it operates within the broader field of digital transformation, where issues of cyber protection, digital literacy, and secure information management are integral. The program focuses on preparing women leaders to implement digital tools in the public sector, particularly in the context of public services. Its training modules include both technical aspects of digital transformation (implementation of electronic services, data protection, process analytics) and the development of soft skills critical for women's advancement to leadership positions — including public speaking, negotiation, and strategic communication. Importantly, the initiative is oriented

[121] КМДА. (2022). Звіт про виконання Національного плану дій 1325.
[122] https://www.linkedin.com/posts/ncscc_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-zaluchenih-do-cifrovizaciyi-derzhposlug

toward practical support for representatives of government authorities, local self-government bodies, and digital institutions who are already involved in digitalization processes or seek greater participation in this field.

Thus, the program not only increases women's representation in key digitalization processes but also strengthens their influence on policy development, including areas related to security, risk management, data protection, and the cyber resilience of state institutions. Its example demonstrates a gradual transition from declarative calls for gender equality to the structural integration of women into the state's digital strategies. This approach not only expands opportunities for women in high-tech public administration but also ensures the sustainability and effectiveness of institutional cyber resilience through the involvement of diverse managerial potential. In this context, another important initiative should be mentioned — the **USAID project "Cybersecurity of Critical Infrastructure of Ukraine,"** serving as a mentorship program that challenged the socio-cultural construct of cybersecurity as a male-exclusive domain and fostered a more inclusive professional ecosystem. The program was conducted online during August and September 2022[126]. It also included the webinar *"Building Women's Careers in Cybersecurity: Recommendations and Advice from Successful Professionals,"* held in May 2023. The webinar targeted students and presented three different career stories of charismatic female cyber experts and examples of their professional development[127]. On October 31, 2023, the USAID project "Cybersecurity of Critical Infrastructure of Ukraine," in partnership with the Aspen Institute Kyiv, held a dialogue titled *"Gender Diversity in Cybersecurity: Realities and Opportunities for Women in Ukraine."* The purpose of the dialogue was to establish cooperation among representatives from different sectors to promote gender equality in cybersecurity in Ukraine and to develop recommendations for overcoming barriers to women's professional realization[128].

In the same direction operates the **SheCyber Hub initiative**, launched by the NGO *Women's Leadership and Strategic Initiatives Foundation* in cooperation with the **National University of Kyiv-Mohyla Academy**. The project creates a space for the development of female students and young professionals in cybersecurity by combining educational activities, meetings with industry leaders, mentorship, practical workshops, and project-based work. Particular attention is given to building a support community and providing access to role models — women who have achieved success in cybersecurity and are willing to share their experience. SheCyber Hub promotes women's integration into the professional community, the development of leadership potential, and the dismantling of gender stereotypes in the field.

All analyzed initiatives demonstrate the potential to form a new generation of female experts in cybersecurity and digital governance. At the same time, ensuring their sustainability requires targeted support from the state — not only through funding but also through regulatory

[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). "Ґендерне різноманіття в кібербезпеці: реалії та можливості для жінок в Україні": відбувся Діалог в межах програми "Діалог про кібербезпеку"

consolidation and integration of results into public policy. Given sufficient political will, such programs may become the foundation for structural gender reform in the IT sector and for strengthening Ukraine's institutional cyber resilience.

2.2.3. War as a Factor in the Intensification of the Gender Dimension in the Security Sector

The state and cross-sectoral programs discussed above, which demonstrated certain progress toward gender inclusion, have been operating under entirely new realities since February 2022. Russia's full-scale invasion in 2022 significantly transformed Ukraine's national security architecture, including cyberspace as a key component of hybrid warfare. At the same time, the war has intensified the need to reconsider the role of women in the security sector, particularly in its digital dimension. As Shopina notes, since 2014 — and especially since 2022 — there has been an increase in the number of women in the defense sector, particularly in areas such as strategic planning and information security[129]. However, the author emphasizes that the growth in women's participation has not been accompanied by a corresponding increase in their role in decision-making processes. Women remain underrepresented at managerial and analytical levels, indicating the persistence of **horizontal segregation**[130].

Changes in the nature of threats, particularly in the digital sphere, have led to an increase in forms of violence specifically targeting women. According to research by L. Soroka, wartime conditions have intensified phenomena such as cyberstalking, sextortion, mass publication of personal data without consent, discreditation campaigns, and disinformation targeting women actively engaged in public life — including journalists, military personnel, and activists[131]. Thus, the digital space becomes not only a channel of communication but also an environment of repressive control that complicates women's participation in public life.

Shopina further argues that gender policy under martial law requires a transition from purely declarative guarantees of rights toward the development of functional mechanisms for women's participation in security governance, particularly in the IT sector. The author highlights that war has a dual effect: on the one hand, it increases women's vulnerability, and on the other, it creates opportunities for their professional growth in fields where their presence had previously been marginalized[132]. Furthermore, the implementation of the National Action Plan for the execution **of UN Security Council Resolution 1325 "Women, Peace, and Security"** has contributed to formalizing approaches to women's participation in the security sector, including digital domains. Within this process, mechanisms are being introduced to enable women's participation in advisory, analytical, and expert groups within public administration bodies,

[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

particularly in areas related to cybersecurity. Such practices lay the foundation for a more inclusive and gender-balanced approach to public administration in the national security sector.

Thus, the Russian–Ukrainian War has become not only a challenge to state security but also a catalyst for changing approaches to gender inclusion in strategic sectors. In cybersecurity, this is reflected both in the growth of women's representation and in the increasing need to establish gender-sensitive policies through revisions of existing legislation, expansion of educational initiatives, and strengthening institutional capacity to respond to digital threats, including those with a gender dimension.

At the same time, an important factor driving change has been the recognition that cybersecurity, alongside military and humanitarian security, constitutes a critical component of the modern security environment. The expansion of hybrid aggression — particularly through information attacks, interference with critical infrastructure, and disinformation campaigns — has created the need to involve a broader range of specialists in the development and implementation of digital protection policies.

In this context, the National Action Plan for the implementation of UN Resolution 1325[133] serves as an instrument for the normative legitimization of women's participation in sectors previously not viewed through the lens of gender inclusion, including information and cybersecurity. The document's provisions regarding women's involvement in decision-making processes in the security sphere create a foundation for developing a comprehensive and gender-balanced cyber policy.

2.2.4. Business and Private Sector Initiatives to Ensure Gender Equality in Cybersecurity

An important aspect of creating a gender-sensitive environment in Ukraine's cybersecurity sector is the set of initiatives originating from the private sector. Compared to government institutions, which typically establish general regulatory frameworks, businesses can respond more flexibly to market needs and implement innovative approaches to attracting and supporting women. Therefore, this section analyzes the practices of leading IT companies and international organizations operating in Ukraine, focusing on their efforts to promote gender equality and overcome existing barriers.

All these initiatives are implemented against the backdrop of several systemic challenges. Despite the acute shortage of highly qualified specialists — which theoretically should create more opportunities for Ukrainian women in cybersecurity — persistent stereotypes regarding the "male" nature of the profession continue to constitute significant barriers[134]. As a result,

[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.

although the share of women in the IT sector overall has increased since 2022[135], women still remain a minority in critical technical and managerial cybersecurity roles[136].

Significant changes have occurred in the educational and professional landscape of cybersecurity: emerging complex cyber threats require professionals to continuously develop innovative protection methods and modernize response tools. At the same time, there is a general lack of public information and research describing the situation and career pathways of women in Ukraine's cybersecurity sector, particularly during wartime. Gaps in educational programs that fail to address women's needs are insufficient to meet emerging challenges. According to DOU, women constitute approximately 24% of all IT workers in Ukraine, but only 19% occupy technical positions[137]. Policies and training systems that are not adequately reformed perpetuate existing systemic gaps, thereby enabling unequal participation in career advancement and access to strategic positions. These issues may be addressed through targeted interventions such as specialized training programs, mentorship initiatives, and transparent criteria for leadership selection[138].

Despite the severe workforce shortage, cyberspace remains male-dominated, as access to strategic decision-making groups is often restricted not by qualifications but by informal networks where security-related issues are discussed. Women's candidacies are frequently questioned in matters related to state security, reinforcing their professional isolation. This implicit exclusion creates an environment of gradual marginalization: even highly capable specialists are often compelled to perform complex tasks outside their core areas of expertise, despite their willingness to assume responsibility. A similar pattern is observed across Ukraine's IT sector, where gender imbalance remains one of the most prominent indicators of structural inequality[139].

This subsection aims to identify and describe specific barriers faced by Ukrainian women cybersecurity professionals under conditions of ongoing conflict. Attention is therefore given to analyzing concrete initiatives implemented by various companies — both Ukrainian and international — operating in Ukraine. Comparing their approaches to attracting, supporting, and advancing women in cybersecurity enables the identification of the most effective models and best practices that may be scaled to address the existing gender imbalance. For a comparative analysis of the role of business in ensuring gender equality in cybersecurity, the activities of several IT companies are examined, including the Ukrainian company **ELEKS**, as well as **Sigma Software** and **Apriorit**, which have significant experience in developing technological solutions, including cybersecurity services.

---

[135] DOU. (2024). Жінки в українській IT-індустрії: як змінюється гендерний баланс та роль жінок.
[136] ISC2. (2023). Women in cybersecurity: Inclusion, advancement and pay equity.
[137] DOU. (2024). Жінки в українській IT-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 is ranked among the world's top 100 outsourcing companies and has provided expert software development and consulting services for over 30 years. The company demonstrates a public commitment to gender equality and inclusivity, positioning itself as an equal opportunity employer and incorporating diversity, equity, and inclusion into its corporate social responsibility priorities. ELEKS seeks to build inclusive and diverse IT communities with equal opportunities not only in Ukraine but also internationally[140].

In 2021, the company received recognition as one of the best family-friendly IT companies. These initiatives reflect recognition of broader social factors influencing women's careers[141]. ELEKS emphasizes employee well-being and the creation of a workplace characterized by respect, trust, and support, fostering personal growth and providing competitive salaries. According to company data, women constitute 34% of its workforce. ELEKS also participates in "Women in Tech" events[142].

Sigma Software demonstrates a proactive approach to gender equality by seeking to eliminate barriers based on bias and promoting diversity and multiculturalism[143]. The company emphasizes that its strategy has always been people-centered, focusing on employees' needs, professional growth, and realization of potential regardless of gender. Sigma Software has actively promoted gender equality since its establishment, and since 2022 it has developed this area as a separate strategic initiative. The company aims to comply with international standards and the requirements of socially responsible partners regarding **DEI (diversity, equity, and inclusion**) and gender balance. Sigma Software highlights the importance of increasing women's participation in technical fields to expand the talent pool and challenge societal stereotypes[144].

Women account for 35% of Sigma Software's workforce, exceeding the industry average of 25%. Approximately 50% of women hold leadership positions, while their share in technical and engineering departments is 19%. The company aims to eliminate pay disparities by continuously monitoring the labor market and providing fair compensation based on professional level and experience, regardless of gender or other characteristics. It guarantees gender equality in working conditions and opportunities, including compensation, working hours, work-life balance, insurance, leave policies, parental leave, and mechanisms for protection against bullying and harassment[145].

Apriorit seeks to ensure gender equality in terms of women's representation and career advancement within the organization. The company identifies key aspects of gender equality, including a neutral approach to candidate selection, gender-balanced leadership in role distribution, accessible career paths regardless of gender, and a safe and comfortable work

[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

environment[146]. Apriorit's CEO is a woman — Klavdiia Zaika — which may indicate support for gender equality at the leadership level. The company also emphasizes the importance of inclusive design in software development to ensure accessibility for users from diverse backgrounds and abilities[147].

Thus, all three companies are significant contributors to Ukraine's IT industry. They provide employment for thousands of Ukrainian IT professionals, contribute to the development of technological expertise in the country, and make a substantial contribution to Ukraine's economy through IT service exports. While Sigma Software demonstrates a clearly structured DEI policy with a high number of women in leadership positions and detailed gender equality initiatives, ELEKS focuses on global operations and employee well-being, whereas Apriorit emphasizes internal equality processes.

In addition to initiatives by individual Ukrainian companies, international organizations and their projects play an important role in engaging women in the digital economy and cybersecurity, often implemented in response to challenges caused by the war.

The UNITAR Prosperity Division launched its training program *"Enhancing Livelihoods: Digital Reskilling for Ukrainian Women Evacuees in Poland"* on October 16, 2023, at an event in Warsaw attended by government representatives, program partners, academic institutions, NGOs, and training participants. The program ran from October 2023 to March 2024, and approximately 1,000 Ukrainian women evacuated to Poland applied for participation. [148]Such reskilling programs are critically important for women whose careers were disrupted by the war, providing opportunities to enter promising technological sectors related to cybersecurity.

Additionally, the global technology corporation **Microsoft** collaborates at national and local levels to increase women's participation in cybersecurity, working with organizations such as the Kosciuszko Institute in Poland to implement training and internship programs for women, including Ukrainian refugees. The company also cooperates with more than 20 other non-profit organizations focused on preparing women for employment opportunities[149]. Partnerships between large technology corporations and local NGOs and educational institutions serve as effective mechanisms for scaling training programs and adapting them to the needs of specific groups of women, particularly those affected by the war.

In summary, the analysis of business and private sector initiatives demonstrates their growing contribution to promoting gender equality in Ukraine's IT sector and related fields such as cybersecurity. Companies increasingly implement DEI policies, seek to ensure equal opportunities, and aim to eliminate pay gaps. International organizations and corporations also launch targeted reskilling and training programs, particularly for women affected by the war.

[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)

However, despite these positive developments, challenges remain, including horizontal segregation (lower representation of women in purely technical cybersecurity roles), overcoming deeply rooted stereotypes, and ensuring genuine advancement of women to senior technical and leadership positions in cyber defense. The effectiveness of these initiatives will largely depend on their systemic nature, long-term sustainability, and ability to adapt to the specific needs of women in wartime and post-war recovery conditions.

2.2.5. The Impact of the Full-Scale War on Gender Aspects of Cybersecurity in Ukraine

Russia's full-scale invasion has triggered significant transformations in Ukraine's cybersecurity labor market. The mobilization of a large share of male specialists and the sharp increase in demand for cybersecurity professionals created a unique "window of opportunity" for women[150]. Women began to enter the field more actively, filling workforce gaps, demonstrating high professional competence, and introducing new approaches[151]. This contributed to a partial transformation of perceptions regarding women's agency and role within the cyber community. Cyberspace has become a visible arena for women's professional self-realization. However, this process unfolds against a paradoxical challenge: the militarization of public discourse and the perception of cyber defense as part of military action may have reinforced traditional gender stereotypes about the "male" nature of the security sector[152], creating additional pressure on women entering this traditionally masculinized domain.

In many professional environments in Ukraine, defense and security are still perceived as strictly male-dominant spheres, while women are more readily imagined at the stove or beside a child's cradle. Similar perceptions also affect the technology sector: it is often suggested that algorithmic work or network analysis should be performed by people with a "warrior's character," implicitly referring to a "male" way of thinking. Even the boldest attempts by women to join penetration testing teams may be met with skepticism, framed in terms of insufficient "restraint" or "cold calculation." [153]The archetype of the hacker as a lone individual further strengthens this barrier, emphasizing that entry into the "great digital war" should be granted only to those who fit the image of a strong man[154]. In this context, Russia's war against Ukraine may have intensified certain gender stereotypes: within a militarized paradigm, cyber defense appears as an extension of combat, increasingly reinforcing the perception of the field as traditionally "male." At the same time, the acute shortage of qualified personnel forces organizations to abandon prejudices and opens doors for talented women. Nevertheless, there is evidence that decentralized Russian-speaking cyber groups occasionally express doubts about the adequacy of "female hackers[155]," as the archetype of aggressive masculinity remains

[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.

dominant. As military tasks shift into the digital domain, women often end up in peripheral positions, performing secondary defensive roles.

Regarding career advancement, women in the technology sector face structural barriers that restrict their professional progression. Globally, the **"glass ceiling"** [156]effect is observed on the path toward top management positions, but in cybersecurity these difficulties become particularly acute: genuine opportunities to lead strategic projects are undermined, while mentorship initiatives may reproduce patterns of horizontal and vertical gender segregation. [157]Although equal access to expert or working groups is formally declared, in practice influential informal networks and decision-making centers often remain closed to women[158], limiting their representation to a narrow circle. Although women's share in the IT sector increased by 4% after 2022, in cyber defense they remain a minority in critical technical and managerial roles[159]. These factors may contribute to the so-called "sticky floor" effect, where women struggle to move beyond entry-level or mid-level positions, especially under the highly competitive and stressful conditions of wartime.

The existing gender pay gap characterizes both the global cybersecurity sector (approximately 20%) [160]and Ukraine's economy overall (18.6% up to 2021, with a projected decrease to 13.6% by 2030 [161]under the national campaign), yet shows no clear tendency toward reduction. Under conditions of economic downturn and heightened vulnerability of women in the labor market, there is a risk of further exacerbation[162]. Even among highly qualified IT professionals, where the share of Ukrainian women has already reached double-digit percentages, **"salary pauses"** in favor of men persist, reflecting the inertia of entrenched assumptions about role and reward within the profession[163]. This indicates that achieving genuine gender equality requires not only skills and knowledge but also clear and transparent mechanisms for correcting internal pay policies. According to DOU (2024), women account for about 24% of all IT professionals in Ukraine, but only 19% of them work in technical roles. As a result, this contributes to indirect discrimination, which is difficult to detect statistically yet negatively affects women's career advancement[164].

Despite the severity of these challenges, the period of martial law has also stimulated the expansion of initiatives aimed at developing technical competencies and supporting women's

[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 IT-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 IT-спеціаліста 2022*.
[164] DOU. (2024, March 7). *Як змінювалася кількість і роль жінок в українському IT за останнє десятиліття*.

leadership. This includes discussions within the National Cybersecurity Cluster, increased visibility of women in informal cyber-volunteer movements, and the activities of female hacktivists. This activity, alongside other efforts, illustrates the potential to overcome existing barriers, provided transparent selection mechanisms are ensured. However, under extreme conditions where speed and flexibility are paramount, the desperate search for specialists may break down fragments of certain barriers, yet without systemic initiatives aimed at transforming gender norms and perceptions of women's professional roles, such "glimpses" of integration risk remaining accidental flashes rather than a foundation for sustainable change.

To achieve long-term impact, it is necessary to implement clear career development roadmaps, ensure equal access to specialized training tracks, create dedicated courses and mentorship programs oriented toward women, and introduce transparent mechanisms for selection into leadership positions that take gender-specific factors into account. It is also important to emphasize the overall lack of public gender-disaggregated statistics and research that would comprehensively describe the specific situation and career pathways of women in Ukraine's cyber defense sector during wartime, which substantially complicates the design and monitoring of effective policies and programs.

Chapter 3. Women in Ukrainian Cybersecurity: Voices of Those Who Have Overcome Barriers

3.1. Results of In-Depth Interviews with Women in Cybersecurity on Their Successful and Challenging Experiences in the Field

Semernikova Iuliianiia, Simanska Zoia, Korobkova Mariia, Dudka Olha, Krasnopolska Tetiana, Hunda Dana, Hlazkova Viktoriia, Nataliia Ditchuk, Pohorila Yelyzaveta, Kolisnyk Sofiia.

> *" "If you are afraid of something, it does not mean that it is not meant for you. On the contrary, it means that it is meant for you. It means that you want to do it and want to do it well. Therefore, doubt and fear are normal. You should not be afraid of fear."*
> *(Respondent 3)*

3.1.1. Research Methodology on Women's Access to the Cybersecurity Sector in Ukraine

This study examines women's access to Ukraine's cybersecurity sector through an interpretive paradigm, recognizing social reality as both constructed and multidimensional.
The interpretative approach makes it possible to examine the subjective experiences of women working in cybersecurity, uncover their stories of overcoming barriers, and better understand the social mechanisms of inclusion and exclusion within this professional field. The

interpretative paradigm gives voice to women themselves, allowing their personal experiences and perceptions to be explored[165].

The study relies on primary data collected through semi-structured in-depth interviews with women working in the cybersecurity sector in Ukraine. The semi-structured format provides flexibility: respondents may expand their answers and offer unexpected insights, which is valuable for understanding the social context of their career paths.

The research adheres to ethical principles of qualitative sociology. An informed consent form was developed, and prior to the interviews respondents were provided with detailed information about the study. Participants' names and other personally identifiable data were anonymized: each respondent is referred to in the text by a conditional numerical designation (e.g., Respondent 1, Respondent 2, etc.). Respondents were free to interrupt the interview at any time or refuse to answer specific questions, and the collected data were used exclusively for research purposes.

The sample was formed using the snowball sampling method. This method operates through recommendations: women who had already participated in interviews suggested colleagues from their professional community who could also share their experiences. Snowball sampling is particularly useful for studying closed or insufficiently explored fields where direct access to respondents is difficult[166]. The snowball process began with the "SheCyber Hub" event held in mid-February. During the event, the researchers met women working in cybersecurity and invited them to participate in interviews. At the end of each interview, participants were asked to recommend other women from the cybersecurity field who could be invited to take part in the study. Communication was also maintained with the Deputy Dean of the Faculty of Informatics at the National University of Kyiv-Mohyla Academy, Trokhym Babych, who provided contacts of women working in cybersecurity known to him.

To ensure a broad range of perspectives and enable the identification of patterns in the challenges and opportunities faced by women in this field, the sample included 11 participants. The primary inclusion criteria were professional experience in the cybersecurity field and female gender. A summary of information about the respondents is presented in Table 3.1.1.1.

*Table 3.1.1.1**. Respondents in the Study on the Status of Women in Cybersecurity***

Respondent	**Company / Sector**	**Position**	**Experience**
Respondent №1	IT company	SOC analyst	Six months

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

[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.

Respondent №2	Consulting company	Security Analyst	More than 1 year
Respondent №3	Bank	Administrative position (confidential)	1 year
Respondent №4	IT company	-	3 years
Respondent №5	Public institution	Analyst	5 years
Respondent №6	IT company	Lead Security Engineer, Director	5 years
Respondent №7	Cybersecurity company	Infrastructure security, DevSecOps, mentor in Women in Tech community	Approximately 1 year
Respondent №8	Consulting company	GRC Specialist (Governance, Risk, and Compliance)	More than 1 year
Respondent №9	Bank	Lead engineer of the incident response department	Six months

Respondent №10	Cybersecurity company	Security engineer	5 years
Respondent №11	IT company	PR Manager with strong knowledge of the cybersecurity field	3 years

The fieldwork phase lasted from mid-February to early May 2025. A total of 20 invitations to participate were sent. The sample size was determined by the sensitivity of the research topic and the high workload of potential respondents, which affected the number of individuals who agreed to participate.

The study is based on the following research questions that define its focus:

1. What challenges do women face in the cybersecurity field and how do they cope with them?
2. How do women evaluate their professional experience and the perceptions of colleagues and society toward them?
3. What conditions, according to respondents, facilitate or hinder their professional development?

The interview guide, presented in Appendix A, follows a semi-structured format that allows respondents to express themselves freely. It consists of five sections. The introductory section includes an explanation of the research purpose, informed consent, and an overview of the interview format. The first section covers career pathways, including education, initial experience, and sources of support. The second section focuses on work experience, including working conditions, equality within the company, and professional communities. The third section addresses barriers, including gender bias, discrimination, and their impact on career development. The fourth section explores societal perceptions of women in technical fields and existing stereotypes. In the final section, respondents share observations, provide recommendations, propose changes within the industry, and may add their own reflections. Overall, each section helps reveal the central issue corresponding to its theme.

Data analysis was conducted using Microsoft Word and was based on thematic analysis. This method was selected due to its flexibility and compatibility with the theoretical framework of the study. Additionally, thematic analysis allows respondents' perspectives to be represented without researcher bias. The choice of this method was also influenced by the size of the research group — formal coding was considered inappropriate as it would have been significantly influenced by the researchers' positionality. Data analysis followed a deductive

approach, moving from general to specific. After transcription, interview texts underwent an initial stage during which key themes common to all transcripts were identified. Several main themes were distinguished: barriers, achievements, attitudes (of surrounding people, family members, colleagues, and the industry), and recommendations for improving the position of women in cybersecurity. Subsequently, individual meaningful text fragments were highlighted and marked with corresponding colors and labels according to each theme. At the final stage, interpretation of the results was conducted, allowing for the identification of general patterns and specific characteristics of women's experiences in cybersecurity[167].

3.1.2. Social Perceptions of Women in Cybersecurity

> *"This is more of a general myth that girls go into IT to find a wealthy boyfriend or husband." (Respondent 7)*

At the beginning and throughout their work in cybersecurity, respondents encountered various attitudes toward their career choice from their environment, family members, and colleagues. These attitudes may influence the willingness to continue working in cybersecurity both negatively and positively. Therefore, attitudes represent an important aspect that must be examined in the context of women's experiences in cybersecurity. To explore this aspect, a block of questions was developed in the interview guide (Appendix A).

Respondents noted that women face **objectification** and **inappropriate offers** that may completely devalue their professional activity and expertise. They may be offered ways of earning money that involve filming or displaying their fully or partially nude bodies, which is presented as "easy work with good earnings."

> *"One day, my classmate texted me, asking how I was doing and everything. I said: 'Everything is good, I got a job in my field, at a bank.' He replied: 'Oh, cool! Don't you want to try this app where you dance and people donate? You can dance in a swimsuit and earn money.'" (Respondent 3)*

> *"Or even when I said I was already working, they told me: 'Maybe OnlyFans would still be better?'" (Respondent 3)*

In addition, respondents frequently mentioned that their environment sometimes attributed women's choice of cybersecurity careers to the **desire to find** a husband and live at his expense. Such perceptions may be explained by several factors: 1)a woman working in a stereotypically

[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

"male" field may be perceived as an exception, and her motivations are therefore questioned and interpreted through the lens of more "traditional female goals," such as finding a partner; 2)such claims may reflect a lack of understanding or even deliberate devaluation of women's professional interests and abilities.

> *"Every answer you give is analyzed through the lens of stereotypes that women enter this profession to find an IT boyfriend and live off his income." (Respondent 4)*

> *"There was one girl who was completely convinced that I chose a technical major to find a good suitor." (Respondent 8)*

Stereotypical perceptions regarding women's reasons for choosing the IT field are also widespread among family members. Respondents noted that relatives sometimes attributed their motivation to external factors such as financial gain ("quick money") or the desire to find a partner in a predominantly male environment, ignoring professional interest.

> *"People mostly say: 'Oh, you probably chose this field because there's a lot of money, or maybe because there are many guys there?'" (Respondent 9)*

Additionally, among respondents' relatives — particularly older generations (grandparents, parents) — cybersecurity is often perceived as "not a woman's profession." Even in the absence of open family conflict, women frequently reported long-term misunderstanding and a certain distance from relatives regarding their work. Positive changes in attitudes (from negative to neutral or positive) were mainly driven by economic factors and visible professional success.

> *"She [my mother] didn't understand why I sat for eight hours and where my money came from." (Respondent 8)*

> *"My friends already understand… they are simply happy that the job is safe and paid." (Respondent 2)*

Several respondents also noted that despite the increasing number of women in cybersecurity, **gender stereotypes** persist among colleagues and management. Women continue to be **perceived as less competent in technical matters**, and their knowledge is often questioned.

> *"In my first company, I saw that girls were treated more condescendingly… if a woman said she didn't know something, the reaction was: 'Well, I knew it — you're a woman, women don't know.'" (Respondent 4)*

“If my female friends said they worked as developers, people would react like: ‘You’re not that great a developer… you’re an IT specialist, but only halfway, because you’re a woman.’” (Respondent 4)

The consequences of gender stereotypes systematically complicate women’s career paths in cybersecurity. This manifests in implicit workplace biases — such as different levels of trust and differing “rights to ignorance” for men and women — as well as in general environmental pressure. **Double standards** exist: women must exert greater effort to prove competence, whereas men may enter the field simply because of its prestige.

“If a man says he doesn’t know something, people react normally because everyone lacks knowledge sometimes. But when I said I didn’t know something, the reaction was: ‘Well, you’re a woman, I expected that.’” (Respondent 4)

“Guys come here just because cybersecurity sounds cool. Girls have to push through pressure even at university because they are judged based on old stereotypes.” (Respondent 6)

One respondent also highlighted **biased attitudes among older colleagues**, particularly in the public sector, where **ageism** and **sexism** intersect.

“In the public sector, the situation is worse. Men over 50 working in government institutions do not take young specialists seriously, let alone women.” (Respondent 6)

“Men aged 40+ often ask me: ‘Are you sure you understand this? Do you really know what we’re talking about?’” (Respondent 4)

Women also faced **gender stereotypes** from colleagues occupying lower positions, with their competence questioned on both **gender** and **age** grounds.

“I heard things like ‘Isn’t this too difficult for a girl?’ or ‘Do you know what the internet is?’ or ‘Do you know what an API is?’” (Respondent 5)

“People were not always friendly — they would say: ‘Oh my God, this young specialist doesn’t know anything, who is she, where did she come from?’” (Respondent 9)

It should also be noted that the respondents encountered stereotypical attitudes regarding their choice of profession and their presence in certain positions. The experience described by one of the respondents goes beyond purely **professional discrimination** and includes instances of **humiliation** based solely on gender. This highlights the deeply rooted nature of sexist biases within the workplace environment.

> *"There was also something else — once I was taking off my sweater, literally like this: first you take your arms out of the sleeves and then just pull it over your head. That is, without anything suggestive, not like in music videos or anything like that… [A colleague said]: 'Oh, XXX is putting on a striptease.'" (Respondent 3)*

Gender stereotypes also hindered respondents' professional self-development and even affected salaries. One respondent noted that some women were denied salary increases because they had partners who could support them financially.

> *"During a salary review, my colleague was told: 'Why do you need more money? You already have a boyfriend.'" (Respondent 6)*

Respondents also reported **differences in how clients treat male and female professionals** in consulting and auditing roles.

> *"When communicating with external clients, comments are sometimes clearly different from what they would be if I were a man… everyone leaves, and then a client says the work was terrible and a waste of time, even though earlier everyone seemed satisfied." (Respondent 6)*

Gender bias also manifests in public online spaces.

> *"On Dou.ua, terrible comments often appear under posts about women in IT, and they are barely moderated." (Respondent 6)*

In summary, women working in cybersecurity face gender-stereotypical attitudes, including doubts about their competence, professionalism, and motivation. These attitudes originate both within the industry and from the broader social environment — friends, family, colleagues, and management — illustrating how deeply rooted sexist biases remain regarding women's work in this field.

3.1.3. Barriers Faced by Women in the Cybersecurity Profession

"You still have to prove that you are capable of something." (Respondent 8)

During employment and work in the cybersecurity field, situations may arise that hinder women in their professional activities — certain barriers. These may include comments or specific actions from colleagues, management, or clients that question women's professionalism, mock them, or simply fail to take them seriously. This can not only prevent women from entering the IT or cybersecurity field but also discourage them from continuing to work in the industry. Such obstacles to career development include, for example, the **glass ceiling** and **glass walls**.

At the stage of initial job interviews, some respondents faced heightened requirements regarding their technical knowledge, which may create an initial sense of personal incompetence. Entry into the technical field for some women is accompanied by intensive self-learning and, at times, informational isolation, when basic concepts are not explained but are instead assumed to be common knowledge by default.

> *"I also went to interviews. They gave me a whole list of things I had to know. I just wrote everything down. And after some time, I realized that some things were so new to me that I had written them down incorrectly."* (Respondent 3)

In addition to high expectations regarding technical preparation, interview participants identified unprofessional behavior by interviewers as a significant barrier, which may indicate **gender bias** regarding women's professionalism in cybersecurity.

> *"But there were cases when interviewers behaved unprofessionally during interviews. For example, the guys would lounge in their chairs, spread their legs, and start the conversation with 'how are you?'"* (Respondent 6)

Some respondents expressed confidence that their gender itself was a factor in being denied employment. This experience is recurrent: repeated rejections create the belief of distrust of professional competence among women, which is widespread in the field. One respondent emphasized that **discrimination** is sometimes informal but evident to the participant herself.

> *"But actually, during my job search there were cases when I clearly felt that they did not want to hire me simply because I was a woman."* (Respondent 7)

> *"It was the moment when you just join a call, you see the person, they say literally two words to you, and you already understand that no matter what you do, you have failed — you can close the call. That happened, probably, twice in my entire life."* (Respondent 7)

At the same time, a softer but no less problematic form of gender differentiation is also observed — **paternalistic**, "lenient" **treatment**. Such treatment reduces women's agency and reinforces perceptions of their less competent or less serious role in the professional field. Instead of full participation in technical dialogue, women often find themselves in the position of someone who needs to be supported or pitied, which does not correspond to their status as equal professionals.

> *"Actually, as strange as it may sound, most men, when they see a girl entering cybersecurity or any technical specialty, treat her more leniently. That's how it seemed to me."* (Respondent 8)

After employment, women are often forced to prove their competence much more thoroughly than their male colleagues. This indicates an unequal distribution of trust within teams, where men are perceived as more competent a priori.

> *"I would say that they simply did not believe me. For example, they constantly checked my work. I was very afraid to say anything so that they would just believe me and not check every word I said twenty times. They did not check men like that."* (Respondent 4)

Attitudes toward women in leadership or mentoring positions are particularly problematic. Age and gender may become grounds for denying authority regardless of objective professional qualifications.

> *"It was the moment when I was supervising interns. And one intern asked to be reassigned because he did not consider me a professional, a specialist he would listen to. First of all, I was younger, and secondly, I was a woman."* (Respondent 4)

> *"And some still believe that women cannot work in serious positions, especially if it is a leadership role, something related to management."* (Respondent 8)

Moreover, the **discrediting of women's achievements** takes the form of men appropriating the results of women's work. Such experiences marginalize women's contributions to professional outcomes and deprive them of recognition. This mechanism often remains invisible, as formally the actions of male colleagues appear as "editing" or "collaboration."

> *"So, I wrote a really good policy, and then my boss came, criticized it, basically destroyed it. Although he did not change much — it was mostly spelling — the body of the policy remained the same, but later he told everyone that he had written the policy, not me."* (R4)

Women in cybersecurity also face forms of **latent sexism** disguised as friendliness but reinforcing perceptions of them as non-professional subjects. Such remarks devalue professional achievements and shift attention to gender rather than knowledge.

> *"At one of my previous jobs, they often told me 'good girl,' which was somewhat irritating. They never said that to my colleague Oleksii."* (Respondent 6)

Some respondents encountered **gender-stereotypical attitudes** that later affected their self-esteem and professional orientation. For example, Respondent 4 describes her unsuccessful experience in her first Ukrainian company, where her work was devalued.

> *"After I left that first Ukrainian company, I was completely broken; I was very afraid to go to any job interviews."* (Respondent 4)

Although she had prior experience at another company, her supervisor strictly controlled her work. The company consisted of 70% men who typically worked on projects and presented them, while the respondent remained in the background. She was treated as interchangeable with other employees, which contributed to professional burnout. The respondent also reported a **gender pay gap** in her company, as she noticed that her male friend's salary was higher than hers. After this, she was afraid to search for another job, as she felt insecure and feared similar treatment.

> *"Even until recently it was quite difficult for me to restore that confidence in myself, because it was hard for me to believe that at my second job they simply were not picking on me. That they simply trusted me and that for someone I was a specialist. It was difficult to regain that feeling. Now it's normal, I'm confident in myself, but yes — that first job was quite traumatic for me."* (Respondent 4)

However, she was fortunate with her next place of employment — a company where she was treated equally with others, which helped restore her self-confidence. A similar impact of fear and distrust was also experienced by Respondent 6. At the beginning of her career, she doubted her ability to master a technical profession. Constant devaluation intensified internal doubts and developed a fear of making mistakes at work, which can significantly hinder professional development.

> *"At the beginning of my career, I even thought about becoming a software tester or a business analyst because of fear of the difficulties."* (Respondent 6)

Respondent 6, working in a team engaged in audits and consulting, notes that she often remembers the names of those who write **sexist comments** and checks where they work. If their companies later approach her team with proposals, she refuses cooperation, quoting statements made by their employees. Respondent 6 emphasizes the lack of corporate response to **sexism**, which contributes to its further spread, as no one holds employees accountable for their words.

> *"For the most part, companies do not react to this — at most they warn their employees, but do not take serious measures."* (Respondent 6)

It is therefore appropriate to conclude that a systematic **pattern of biased behavior** toward women in cybersecurity can be observed, manifested in doubts about professionalism, distrust, additional control, appropriation of results, and hidden condescension. This may significantly affect women's confidence, self-realization, and career trajectories in the cybersecurity field and confirms the need to highlight this issue, conduct educational initiatives on **gender discrimination** in the workplace, and promote **anti-discrimination policies** within companies.

3.1.4. Personal Achievements of Women in Cybersecurity

> *That is now when many women and men of any age are simply used to working with women, and they constantly see that quite many women are professionals."* (Respondent 4)

Personal achievements are important for the professional development of women in the IT field. Respondents noted that their achievements resulted both from personal determination and from support provided by mentors. Many respondents emphasized the importance of overcoming their fears and doubts, which became key to their success. For example, one respondent recalled how at the beginning of her career she felt afraid during job interviews and even during her internship, but she did not allow fear to stop her.

> *"When they invite me to a job, I say no, I'm scared, I've never been there, but I still go. Then again, no, I'm scared, there is an internship, I'm afraid, but I still go."* (Respondent 1)

In addition, respondents emphasize the importance of continuous learning and striving for technical mastery. For instance, one respondent noted that to transition into cybersecurity, she clearly planned her career path and was prepared for changes.

> *"I planned my career path and simply waited for the moment when I would become technically strong enough to move into cybersecurity."* (Respondent 6)

For some respondents, obtaining certifications and additional courses has become an important step. For example, Respondent 2 actively completed courses from Google and IBM, which helped her acquire the necessary technical skills.

> *"I took courses on Coursera related to cybersecurity from Google. I also completed several courses from IBM that were freely available. Also, leaked courses, which included preparing courses for the CompTIA Security Plus certification and other similar certificates."* (Respondent 2)

Thus, the personal experience of overcoming obstacles among women involves not only solving professional problems but also continuously struggling with self-doubt and developing their own skills.

3.1.5. Positive Developments in Practices of Attracting and Supporting Women in Cybersecurity in Ukraine

> *"Although there are still fewer technical specialists among women than non-technical ones, their number is increasing, and that is encouraging."* (Respondent 6)

At the same time, despite the above-mentioned challenges and difficulties that women have faced and continue to face while working in cybersecurity, some respondents noted that certain **positive changes** have recently become noticeable. There has been a reduction in discrimination, gender-stereotypical attitudes, misunderstanding, and conversely — increased visibility of women in the field, greater support, and broader acceptance.

> *"It's already easier, much easier in Ukraine now. It seems to me that there is no longer the kind of discrimination that existed before. In IT, it seems that employers perceive women the same way as men."* (Respondent 2)

One important trend is also the increasing number of women in educational groups and workplaces. According to respondents, many study groups have already demonstrated a balanced gender ratio.

> *"For us it's the same — fifty-fifty. I mean… and we… we have girls… our top groups are probably only girls."* (Respondent 1) (regarding the gender balance in a study group).

> *"Now young people deliberately choose cybersecurity, whereas before they entered the field accidentally through interest and self-education."* (Respondent 6)

According to some respondents, improved attitudes toward women in this field may also be related to the **shortage of personnel** in the industry. Due to the war in Ukraine, some men join the military, which leads to free vacancies in companies. These positions are increasingly filled by women, which contributes to changing perceptions regarding women's professionalism in the field.

> *"At the moment circumstances are developing positively in this regard, because many men go to the front lines, many are mobilized, and this is discussed at every conference I attended […], that more women should be brought into this field because women, in principle, understand cybersecurity very well if they are immersed in it."* (Respondent 1)

Women are increasingly integrating into the field, particularly through educational programs, which positively affects their professional status. In addition, more companies start to hire women, expanding opportunities for career growth.

> *"Yes, I really notice positive changes in attitudes toward women in cybersecurity. Every year more companies open their doors for female specialists. More support, fewer stereotypes, and greater trust in professionalism regardless of gender."* (Respondent 5)

Another important change is the reduction of gender discrimination in some companies. Respondents note that organizations show **decreasing stereotypical attitudes** toward women, and women feel more equal to men in terms of professional opportunities.

> *"…now many women in cybersecurity are valued, and there is some kind of uplifting effort to smooth out these gaps in the hiring practices."* (Respondent 1)

> *"I had interviews, also in banks and other organizations, and there was no special attitude toward me as a woman."* (Respondent 1)

This is also confirmed by colleagues' attitudes toward women, as most respondents do not feel discrimination or disrespect because of their gender and even report greater loyalty among women professionals.

> *"No, I would probably say that it is even a bit easier for me to communicate, for example, with clients. Because most of these communications were with managers or responsible personnel. There were more women there. So, they seemed more loyal to me than to my male colleague."* (Respondent 2)

It should also be noted that women's teams in companies and study groups are becoming increasingly visible, which positively influences the motivation of other women to join the profession. Overall, changes in the field indicate improved equal opportunities for women and men in cybersecurity.

> *"Thanks to the efforts of our government, senior leaders, and local managers, the promotion of women in cybersecurity is being advanced."* (Respondent 9)

> *"I also see this in my company: now we receive many resumes from women."* (Respondent 6)

Thus, the positive developments in cybersecurity regarding women's position in the field include an increase in the number of women in the profession, a reduction in stereotypes about their role, and expanded opportunities for career development and support from organizations and colleagues.

3.2 Results of Expert Interviews on the Successes and Challenges of Involving Women in Cybersecurity During the Russian-Ukrainian War

Kviat Sofia, Hres Anna, Selianinova Yevheniia, Vysoven Karina, Stashko Veronika, Balabash Anastasiia, Ovsiuchenko Oleksandr, Pimenov Stanislav, Khlivna Yelyzaveta, Vasiutynska Anastasiia.

3.2.1 Methodological Foundations of the Survey on the Successes and Challenges of Women's Access to the Cybersecurity Field in Ukraine

To study the successes and challenges of women's access to the cybersecurity field, the interpretative paradigm was used. The choice of this approach is determined by its ability to identify the essence of social phenomena, which enables further formulation of hypotheses[168]. Accordingly, this enables a deeper understanding of the phenomenon in the future.

According to E. Maccoby (1954), [169]an interview is defined as *"a face-to-face verbal exchange in which one person, the interviewer, attempts to obtain information, expressions of opinions, or*

[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/gs_ok.pdf

[169] Maccoby, E. E., & Maccoby, N. (1954). The Interview: A Tool of Social Science. In G. Lindzey (Ed.), *Handbook of Social Psychology* (Vol. 1, pp. 499). Reading, MA: Addison-Wesley.

beliefs from another person or persons." The primary sociological data of this qualitative research consists of semi-structured expert interviews. They make it possible to obtain a comprehensive understanding of the problem that goes beyond the individual competence of the researcher. The study applied research (analytical) triangulation, which involves engaging several analysts in processing the same data[170]. This made it possible to minimize subjectivity in the interpretation of the collected data. At the same time, it increased the validity of the results, the reliability of conclusions, and enabled a deeper analysis of the studied phenomenon through the inclusion of different perspectives and expert evaluations[171].

The search for respondents was conducted using Google search engine as well as social networks such as Instagram, Facebook, and LinkedIn. The snowball sampling method was also applied after collecting and processing recommendations from previously interviewed experts. Invitations to participate were sent to 24 respondents.

The final research sample consisted of 14 respondents (5 men and 9 women) involved in the cybersecurity field in Ukraine who agreed to participate in the interviews. The average length of professional experience in cybersecurity among all experts was 8.4 years. The formal selection criterion was at least one year of work experience in cybersecurity (in either the public or private sector). Only 5 out of 9 female respondents have higher education in the specialty "Cybersecurity," while none of the male respondents have higher education in this field. Respondents who had not studied this specialty acquired particular knowledge while studying related fields (computer science, engineering, law), through specialized courses, or directly in the workplace.

The criterion of expertise included knowledge in the field of equal rights and opportunities, involvement of women in cybersecurity, work aimed at strengthening women's capacity in cybersecurity, and related areas. The average duration of interviews was one hour. The interviews were conducted between March 21 and April 1, 2025. The general characteristics of respondents are presented in Table 3.2.1.1.

Table 3.2.1.1. General characteristics of experts regarding the successes and challenges of involving women in cybersecurity during the Russian-Ukrainian war.

№	Gender	Workplace	Professional Experience (years)	Expert Knowledge on Women's Access to Cybersecurity

[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

Respondent №1	Female	Non-governmental organization	6	Deep technical understanding of security processes and active participation in women's IT communities
Respondent №2	Female	IT company	7	Practical experience in IT and civic engagement, particularly in equality initiatives
Respondent №3	Male	Private IT company in the field of data protection	3,5	Related experience in IT without a specific focus on gender equality or women's participation
Respondent №4	Male	Private IT company	1,5	General understanding of the topic and potential involvement in gender-sensitive initiatives
Respondent №5	Male	IT developer	5	Experience relevant for

				cross-sectoral cooperation
Respondent №6	Female	Cybersecurity educator in Ukraine; co-founder and project coordinator of an NGO supporting women in cybersecurity	25	Leader of strategic initiatives promoting women's leadership, including in the digital sphere
Respondent №7	Male	Cybersecurity educator in Ukraine	15	General understanding of the topic and potential involvement in gender-sensitive initiatives
Respondent №8	Female	Analytical company	20	Comprehensive strategic vision aimed at strengthening women's roles through analytics and communication
Respondent №9	Female	Government institution	3,5	General understanding of the topic and potential involvement in gender-sensitive initiatives

Respondent №10	Male	Government institution	10	General understanding of the topic and potential involvement in gender-sensitive initiatives
Respondent №11	Female	Founder of a consulting company and cybersecurity projects/initiatives	8	Lawyer and cybersecurity expert developing policies and training programs
Respondent №12	Female	Administrator of the information security department	9 months in the current position	General understanding of the topic and potential involvement in gender-sensitive initiatives
Respondent №13	Female	Co-founder of an NGO in women's leadership	3	Leader of strategic initiatives promoting women's leadership, including in the digital sphere
Respondent №14	Female	IT company	7	Expertise in managing technical projects with the

				capacity to influence women's participation in IT

This number of respondents can be considered sufficient for analysis. The responses of participants were repetitive; therefore, the information can be considered to have reached the saturation point.

Before the interviews began, consent to record the conversation was obtained. Respondents were informed about the consent process, which included the purpose of the study, confidentiality conditions, and their right to withdraw from participation at any time. For ethical reasons, the data obtained during the research was depersonalized.

The interview guide was constructed based on previously predefined thematic sections, which ensured the structured nature of the research, consistency of data collection, and the possibility of comparing responses by each interviewer (Appendix B).

The first section was devoted to acquaintance with the expert to clarify previously collected information about their position, experience in cybersecurity, and education. Information regarding motivation to work in the field was also collected.

The second section explored experts' opinions regarding the representation of women in cybersecurity in Ukraine. Respondents were asked about gender disproportions in the field, women's representation in the workplace, and how this was affected by the beginning of the full-scale Russian invasion.

The third section of the guide was devoted to the challenges faced by women in cybersecurity in Ukraine. The questions focused on identifying vertical or horizontal gender segregation, whether women experience gender bias, discrimination, or sexual harassment in the workplace.

The fourth section addressed the successes of women's access to the cybersecurity field in Ukraine. It focused on support for women at organizational and state levels. In addition, experts were asked whether they were aware of female role models and their achievements in cybersecurity.

The purpose of the fifth and final section was to gather recommendations from specialists on attracting more women to cybersecurity in Ukraine.

The AI transcription tool Restream was used for interview transcription. After transcription, interviewers reviewed the transcripts to ensure accurate reproduction of information and to check for errors.

To process the data obtained from semi-structured expert interviews, the method of thematic analysis was used. This method was chosen due to its ability to focus both on broad patterns in the data and on the analysis[172] of individual aspects, including explicit and latent meanings in respondents' statements. At the stage of primary coding, respondents' opinions corresponding to the content of interview questions were identified and then grouped thematically. After that, the coded text was reviewed, and quotations were distributed according to relevant themes. This made it possible to identify and structure key themes from respondents' answers.

Thus, after completing all stages of data collection and processing, the successes and challenges of involving women in cybersecurity during the Russian-Ukrainian war were identified.

According to the results of the analysis, among the challenges of women's access to cybersecurity in Ukraine, respondents mentioned several critical issues, including manifestations of horizontal and vertical gender segregation, gender stereotypes and biases toward women, lack of initiatives and support from the state and society, and manifestations of sexual harassment.

3.2.2 Challenges in Women's Access to the Cybersecurity Field in Ukraine: Gender Stereotypes and Biases

> *"Yes, I noticed it, and I pointed out that sexism is undesirable or unacceptable, so I tried to stop it."* (Respondent 10)

An important challenge to women's accessibility to the cybersecurity field is gender stereotypes and biases. They maintain gender polarization and the belief that men and women are homogeneous within groups[173]. In the fields of education and employment, they shape the perception of cybersecurity as a "male" domain, reduce the self-esteem and confidence of potential female specialists, and influence employers' decisions regarding hiring and career advancement. Not all respondents encountered manifestations of sexism in their teams; however, most have such experience or are aware of such cases. For example, Respondent 8 stated that *"women need to prove their competence,"* which indicates a condescending and/or non-serious attitude toward women's capabilities in the workplace. In addition, women emphasized that the number of biases is greater in the public sector compared to the private sector:

---

[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 соціогуманітарних спеціальностей* (3 видання, випр. і доп.). К.: Критика. (С. 44)

> *"When I communicated with state authorities, I very often heard the phrase: 'Oh, you're a girl, what could you possibly… What can you tell us here?' … Or: 'She is a woman, why should she work on defense facilities or critical infrastructure objects?'"* (Respondent 11)

It should be noted that respondents reported having to *"work very hard (overtime) so that their competence would be believed in, in order to prove their knowledge in a male environment."* (Respondent 13). Respondents also mentioned the widespread traditional perception of cybersecurity as a masculine field and/or the psychological tension caused by this perception:

> *"At the Ministry of Defense, I actually had a case where I cried for the first time in my life because I was organizing an event with the military. I saw direct disrespect. If I came with my supervisor, they talked to the supervisor; when I sat at the negotiation table and expressed my opinion on how to improve something, the men demonstratively pretended that I did not exist, as if they did not listen, and spoke only to my supervisor."* (Respondent 13)

Among male respondents, only 2 out of 5 reported cases of sexism toward women in their workplace. This indicates a low level of awareness, understanding, and/or recognition of the problem of sexism among men, even when such cases occur:

> *"Yes. It's classic patriarchal nonsense. Especially when, you know, they emphasize their gender. Like, she's smart, and she's also a girl. And such ways of phrasing things slowly drive me crazy. Especially when that person five minutes earlier said 'I'm not sexist.' You see, 'Here, for example, XXX — she's smart and she's also a girl,' and then you think, 'Well, you're not sexist at all.' It's unconscious. It's not something particularly deliberate — it's just everyday sexism."* (Respondent 7)

Sexism focuses attention on the physical, intellectual, creative, and other advantages of one group of people (men) over others (women). [174]Respondents' answers indicate the prevalence of this phenomenon and the persistence of traditional stereotypical gender role division in education and employment into feminine and masculine roles. It should also be noted that such manifestations exist within the cybersecurity field itself.

3.2.3. Challenges in Women's Access to the Cybersecurity Field in Ukraine: Horizontal Gender Segregation

> *"Throughout all her years working in cybersecurity, she has never had a female colleague."* (Respondent 1)

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

Manifestations of **horizontal gender segregation** concern the disproportional ratio of women and men in the cybersecurity field in Ukraine. According to DOU, in 2022 women accounted for 23.4% of employees in the IT sector, which is a significant improvement compared to 8% more than a decade earlier[175]. Almost all female respondents agreed that there are significantly more men than women in the field. Women are also perceived rather as an exception than as a normal part of the workforce composition in the sector. Some respondents had not worked with women at all:

> *"I see the number of women, girls, who come to our events. I jokingly call it 'a men's rain.' When you come to any event related to cybersecurity, there are very few women there and mostly men… Women are more like an exception than some normal situation…"* (Respondent 13)

> *"Gender disproportion is very noticeable. It's very funny… Well, funny… hysterically, ironically funny, that when they organize gender meetings about women's rights (in cybersecurity), there are about 70–80% men there…"* (Respondent 7)

Women and men are often employed in different areas of work, and even when working in the same domain they frequently perform different tasks, occupy different positions, have different levels of pay, and experience different rates of career advancement[176]. Respondents also emphasized that gender segregation in cybersecurity is higher than in other areas within the broader IT sector. This indicates gender-stereotypical perceptions and the division of work domains into traditionally "feminine" and "masculine":

> *"Parents come, for example, to an Open Day at Mohyla Academy and they say: 'Oh, well cybersecurity is not really a women's thing, better become a programmer'… There is an idea that programming is okay for women, but cybersecurity is not. Well, cyber comes from information security, from KGB people, etc., etc., it grew out of that… And therefore… I don't want to be ageist, but people of a more elegant age than mine have a certain notion that this definitely should be done by a man with a beard."* (Respondent 7)

> *"I recently found a pretty good analogy. I compare cybersecurity to our army. There are women there. That's a fact. However, there are very few of them, and in some areas, there are none... Yes, in cybersecurity there are pentesters, where I have almost not seen women at all. And in the army, for example, in combat positions, there are very few."* (Respondent 2)

[175] Paliychuk, U. (2023, August 9). *Women in technology: Insights from Ukraine, Bulgaria, and Poland*. Beetroot.
[176] Маєрчик, М. (2017). *Гендер для медій: підручник із гендерної теорії для журналістики та інших соціогуманітарних спеціальностей* (3 видання, випр. і доп.). К.: Критика. (С. 79)

Socio-demographic characteristics also influence women's access to and representation in traditionally masculinized domains of work, including cybersecurity. Respondents mentioned such characteristics as: young age, not having a family, higher education, leadership qualities, and a sense of being "different from other women." For example, Kimmel refers to career changes associated with having a child as the "mommy track," which slows professional growth and development. Alternatively, due to established gender norms, perceptions, and expectations, demands placed on young female specialists will differ from those applied to women with children[177]. However, nearly half of the respondents could not answer this question because they do not believe personal characteristics influence women's access to the cybersecurity field. This is related to the fact that horizontal gender segregation in the field is caused not by a lack of competence among women, but by the influence of established socio-cultural perceptions that shape professional orientations already at the stage of education and socialization:

> *"This is not related to what kind of women come into cybersecurity. This is related to how people choose their profession in general."* (Respondent 10)

An important challenge of the field is not only the low representation of women, but also the reasons for their leaving the sector and/or the barriers to their career advancement. Respondents pointed to a lack of shared language with the team, low salary, the complexity of the work, and military service and its specific conditions as reasons why women leave the field. Respondents also mentioned such reasons as marriage and starting a family. This indicates the reproduction of traditional gender roles among representatives of the cybersecurity community:

> *"Gender stereotypes existed. This mostly came from older people, because they were used to the fact that they work, and their wives sit and look after the children."* (Respondent 6)

Respondents also noted that it is difficult to determine reasons why women leave, since many reasons are common for everyone. One of the respondents stated that these common reasons are likely hyperbolized for women. This indicates somewhat blurred perceptions of women's reasons for leaving, particularly in cybersecurity within the context of military service:

> *"For some it's personal reasons. Because, for example, the husband moved somewhere. And for the family to be together, the wife also transferred. For some it's better working conditions. Still, even things like this are possible: when there is a slightly more promising job, slightly higher pay, a person transfers to another unit, another organization. Probably these two are the main ones, but again, in the environment I am in now, it is specific."* (Respondent 10)

[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.

Among the challenges for women in cybersecurity is also the lack of state and civic support to support women in the cybersecurity field. This refers to the absence and/or low number of high-quality and effective initiatives such as trainings, quotas, mentoring, and similar measures:

> *"Initiatives mostly come from the civic sector; the state sometimes picks up or joins already existing NGO initiatives. There is no centralized state program to support women."* (Respondent 11)

> *"…this is better than nothing. Of course, such initiatives actually need further improvement… Yes, we talk about it, but unfortunately we still talk about it insufficiently, because this topic should penetrate all layers of cybersecurity provision, starting from the upper levels related to organizing regulators' work, and ending with the people responsible for cybersecurity at enterprises in the regions—small towns, settlements."* (Respondent 2)

This indicates that horizontal gender segregation in Ukraine's cybersecurity field is largely driven by the absence of a systematic state policy aimed at supporting and integrating women into this sector. Challenges arise, in particular, due to low public awareness of state initiatives and reforms. Female respondents emphasize that initiatives to address gender imbalance largely remain at the level of NGOs, while the state does not form an integrated approach that would cover all levels—from developing a regulatory framework to implementing practical solutions locally. This points to the fragmented nature of efforts and insufficient institutional support, which, in turn, reinforces gender segregation in technical fields, including cybersecurity.

3.2.4. Challenges in Women's Access to the Cybersecurity Field in Ukraine: Vertical Gender Segregation

> *"I am probably one of the few women who runs a company. There are fewer women in managerial positions and leadership roles."* (Respondent 11)

Respondents' answers also indicate the presence of vertical gender segregation. First of all, they pointed to the insufficient representation of women in leadership positions or in roles directly tied to the technical component:

> *"In my work team, women most often hold positions such as Product or Project managers, marketing, sales managers, Customer Success, Pre-sales, or less often engineering roles."* (Respondent 3)

> *"So far we do not have a single woman who would hold the position of head of department, head of directorate, deputy director, or director. In other divisions of our service there are women who serve as heads of directorates, heads of departments, and there are even women deputy directors of a department. There is one woman who is a department director."* (Respondent 10)

In Ukraine, gender statistics on leadership-position distribution exist only for the civil service and do not cover the entire labor market. Although there are no formal prohibitions preventing women from holding leadership positions, in practice their career advancement is often complicated and/or halted due to invisible barriers[178]. Women predominantly occupy supportive, administrative, or client-oriented roles (management, marketing, support), while positions related to governance or technical expertise remain predominantly male. This points not only to structural inequality but also to gender barriers connected to professional socialization, biased perceptions of leadership, and insufficient institutional support for women on the path to leadership or expert positions. It should be noted that this narrows women's opportunities and limits the development potential of the field itself due to restricted diversity of viewpoints and experiences in decision-making processes.

In addition, female respondents noted that even when women are present in leadership positions, there are formal barriers indicating manifestations of the "glass ceiling." The glass ceiling is a phenomenon that generalizes a set of barriers arising from individual and societal biases and preventing women from advancing up the career ladder within their organization and from occupying managerial-level positions[179]. This hierarchy is not formally fixed; however, it is maintained through gender stereotypes that keep women at a "middle" management level, while strategic, resource-related, and technically complex positions remain under male control. This reproduces structural gender inequality, including cybersecurity:

> *"There is an important point that there is a hierarchy on paper, and there is a real one. They differ oftentimes, even men among themselves cannot distribute it, and it often really differs. Even if women are on paper in the hierarchy, it does not mean that in fact they are in this hierarchy."* (Respondent 2)

One reason is the perception of the field as "technical-male," since respondents indicated that women are present in segments with a less pronounced technical component of cybersecurity (for example, system administrators, client communications, accounting, audit). At the same time, in positions closer to the core directions of cybersecurity development (engineers, CISOs, developers), their shortage is evident.

---

[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.

Respondents' answers also revealed a tendency toward a gender pay gap, although the level of awareness and evaluation varied. The gender pay gap is one of the most common forms of labor-market discrimination, whereby men, depending on the country, earn on average 10–40% more than women[180]. However, respondents noted that they do not have specific figures or did not observe such a gap throughout their professional growth, particularly in the public sector where salaries are usually fixed:

> *"The pay gap exists everywhere; cybersecurity is probably not an exception." (Respondent 7)*

> *"As strange as it may sound, discrimination is lower in the public sector than in the private sector. And in the private sector it may not even be discrimination because someone is a woman, but maybe because a woman simply fights less for her salary level." (Respondent 8)*

Some responses also included examples of reverse discrimination, which are rather linked to women's willingness to demand equal pay in the private sector:

> *"One of my friends works in cybersecurity, and she had a higher salary, so the gap exists, but there are some individual cases where it goes the other way, but I think this is more of a unique case; overall there are still tendencies toward a gap in the direction that women have less than men."* (Respondent 5)

The gender pay gap is an unacceptable phenomenon that effectively violates women's rights, because human rights are conceptually associated with the idea of gender equality. In addition, the pay gap is a manifestation of discrimination referenced in the UN Convention. Under it, discrimination is defined as: *"…any distinction, exclusion, or restriction… of women's human rights and fundamental freedoms in the political, economic, social, cultural, civil, or any other field, irrespective of marital status…"* [181]Considering this, vertical gender segregation in the cybersecurity field indicates persistent institutional and cultural barriers that restrict women's professional advancement, reproducing gender inequality in access to resources, power, and influence in the sector.

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

3.2.5. Challenges in Women's Access to the Cybersecurity Field in Ukraine: Sexual Harassment and Violence

> *"I have not seen explicit bias or harassment, and that is definitely a good thing."*
> (Respondent 3)

Several female respondents reported experiences of **sexual harassment**. However, none of the male respondents had witnessed sexual harassment targeting women. Women note that sexual harassment is often perceived as a norm and manifests at different levels: at the institutional level—through abuse of power by representatives of law enforcement and security structures; at the interpersonal level—in the form of sexualized messages; and at the cultural level—through the objectification of women and entrenched gender stereotypes that normalize such behavior.

> *"I had a case when I came to an event wearing a knee-length skirt, heels, and a blouse, met a man from the security and defense sector, and at night I started receiving vulgar messages with calls for sex—messages like 'you have such nice legs' or something like that. People simply allow themselves to do this openly."* (Respondent 13)

Importantly, the normalization of such behavior is also related to manifestations of "special treatment" from lecturers and/or male colleagues, which can also constitute one of the forms of harassment—i.e., at the horizontal level of relations. Although the Law of Ukraine "On Ensuring Equal Rights and Opportunities for Women and Men" focuses primarily on the vertical level, the law defines actions that humiliate or insult individuals as sexual harassment[182]. Thus, manifestations of "special treatment" can be considered sexual harassment. However, such and similar formulations often include the word "unwanted," which complicates the legal and social definition of such acts, since the emphasis on "unwantedness" may reduce the perceived seriousness of the problem and create obstacles to effective response and accountability. It narrows the understanding of sexual harassment only to overt violations. For example, not all female respondents and their female colleagues consider this a problem, and sometimes they even see it as an advantage:

> *"Despite the fact that it did not affect her negatively, she felt uncomfortable receiving offers of additional help with studying from male lecturers or invitations to meet outside of class."* (Respondent 9)

> *"To be honest, maybe most administrators treat me a little more gently because I'm a girl, and they maybe somehow are afraid to offend me. Because, for example, if you need to go and ask for something at work, everyone is usually like: 'Let you do it!' I have no problem doing that."* (Respondent 12)

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

In addition, female respondents emphasize that manifestations of sexism are influenced by authority and power, because a woman's high or equal-to-men position contributes to men treating her better. In such cases, men often do not allow themselves any sexist jokes or prejudices toward a woman:

> *"I was talking about a story involving sexism with a woman who holds a leadership position in the security and defense sector. That is, she constantly moved up the career ladder to that position, and she told me that she does not see any gender bias in this field. I realized the following: when you have a high position and you manage people from above, especially men, they cannot allow themselves any sexist jokes toward you and so on (ed.: it was about harassment etc.), because they can lose their position."*
> (Respondent 13)

Acts of sexual harassment and violence breach ethical and professional standards, cause trauma, and grave violations of human rights. In addition, they create barriers to the development of women's career potential in the field, contributing to their marginalization. Overcoming these problems requires a comprehensive approach, including changes in organizational structures, strengthening legislative norms—particularly through conceptual clarification of terms—and the development of a corporate culture that supports inclusiveness, equality, and the creation of a safe, gender-sensitive environment.

3.2.6. Successes in Women's Access to the Field in Ukraine: Overcoming Horizontal Gender Segregation

"…discrimination has moved into the 'second' place."
(Respondent 10)

In addition to challenges, respondents also mentioned successes of various types regarding women's access to and visibility in the cybersecurity field. This indicates that, despite existing challenges, respondents noted positive shifts in opportunities, direct involvement of women, and women's visibility in the professional community. These successes include various processes of overcoming horizontal and vertical gender segregation. That is, they relate to the conditions for women's entry into the cybersecurity field and to the limitations in career advancement already within the field.

First of all, the onset of the full-scale war had a positive impact on women's access to and representation in the field. Respondents noted that the number of women in cybersecurity at different levels increased with the beginning of the full-scale invasion. This is linked to the popularization of women's involvement and integration into cybersecurity as a STEM discipline among businesses and officials. For example, the Ministry of Education and Science of Ukraine is implementing the concept of STEM education with an emphasis on the importance of

abandoning the division of education and labor into male and female spheres[183]. The number of vacancies also increased due to the need for workers to anticipate and fix problems arising from cyber threats and attacks. In view of this and the mobilization processes, there is also a large number of open positions:

> *"Overall, the war… It accelerated the integration of women into technical teams, demand for personnel increased, and discrimination against the background of qualifications moved into the second place. Many men are at the front, and this also creates a necessity, a need to fill positions, and thus, forced or not, we are still moving toward reducing the disproportion, which is good…"* (Respondent 3)

This indicates a reduction in horizontal gender segregation in Ukraine's cybersecurity field, which is certainly a successful change. However, these processes often occur not due to active reforms and/or a conscious approach to counteracting discrimination.

Another success on the path to overcoming horizontal gender segregation is the lower tendency among young people in Ukraine to resort to gender bias. Research by various international organizations shows that young people are less likely than older generations to agree that there are professions suitable exclusively for men or exclusively for women. [184]Therefore, it can be concluded that in contemporary Ukraine a social environment is being formed in which women can more easily choose professions that are gender-marked as "male." Manifestations of this phenomenon are noticeable both in education and in the labor market.

> *"The younger generation is more loyal, and it doesn't pay attention whether you are a girl or a boy. For them you are a professional first of all, and then we'll see."* (Respondent 7)

And although prejudice against women and gender stereotypes is still present among Ukrainian youth, one can observe a shift in perceptions of gender roles and greater attention to workers' qualifications rather than to their sex.

Among the successes, it is also worth noting the development of mentoring programs and trainings for women, especially in relation to counteracting discrimination and sexism. This format of support is aimed at attracting women into cybersecurity and developing skills at early stages of entering the profession.

> *"Initiatives to involve women often exist only at the very top of the professional pyramid, in large organizations and central bodies. Meanwhile, they do not cover regional levels, where cybersecurity measures are implemented locally."* (Respondent 2)

---

[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

[184] UNFPA Ukraine. (2021.). Презентація програми "Трамплін до рівності". https://ukraine.unfpa.org/sites/default/files/pub-pdf/prezetation_tramplin_ukr_1.pdf

This indicates that gender equality and programs on this topic are being introduced, which is a significant advantage. However, they are still often treated as optional and/or symbolic rather than as a systemic requirement for the entire sector.

In addition, initiatives and reforms to support women in cybersecurity are actively being introduced at the state level. Most often, this concerns ensuring conditions for broader access of women to the field in general. Women are systematically included in developing programs in the form of trainings, participation in delegations, and leadership programs. This indicates real examples of implementing an inclusive policy in the professional environment. That is the practice whereby women not only enter the field but also gain access to opportunities for professional growth is at the stage of formation:

> *"…judging by what we have in the department, well, me and my female colleagues are much more often directed specifically toward various training programs, leadership programs. That is, constantly, if some kind of delegation — even just a few people — is sent for training, there must always be at least one woman in that delegation. "* (Respondent 2)

All-Ukrainian and regional initiatives aimed at engaging women to overcome gender inequality are also interesting and effective; they received support at the state level, in particular from officials and high-level leadership of state structures. The effectiveness of regional development and regional policy largely depends on the ability to align the interests of the state with the needs of society, including in local communities[185]. For example, the initiative and subsequent decision of the National Cybersecurity Coordination Center (NCCC) and international forums:

> *"By a decision of the NCCC, the launch of an initiative to involve women in cybersecurity for gender equality was approved. That is, it is the first legislative case regarding gender equality in the cybersecurity field."* (Respondent 13)

> *"This month, for the second time, the Kyiv International Cyber Resilience Forum was held. And during this event, cyber competitions traditionally took place. For the first time in Ukraine, a national women's team participated in them. These were representatives of the Armed Forces of Ukraine, the Security Service of Ukraine, the Ministry of Defense, the State Service of Special Communications and Information Protection—an exclusively women's team. And it showed great results."* (Respondent 13)

The importance of this decision lies in the fact that this initiative was among the first to raise the issue of gender equality and the active involvement of women in the field at the state level. In addition to the initiative, educational and mentoring programs are being implemented. Programs such as SheCyber Hub, implemented with the support of the Women's Leadership and Strategic Initiatives Foundation (WLSIF) and the National University of "Kyiv-Mohyla

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

Academy," have demonstrated high effectiveness and public engagement. The goal is to teach female students technical skills combined with the development of women's leadership:

> *"What else do we do for women? We have a lot planned. And trainings—not just to teach some technical skills, but specifically leadership ones: about building a career, professional etiquette, personal development specifically as professional women. We also launched the initiative SheCyber Hub—here we approach it from another side. We give girl students and boy students as well access to women leaders who work in cybersecurity."* (Respondent 7)

> *"Our trainings are not just to teach technical specialties, but specifically leadership ones: about building a career, professional etiquette, about developing women precisely as professionals in their field."* (Respondent 13)

Such initiatives and reforms play an important role in supporting gender equality in the cybersecurity field. They contribute to the formation of a community of women leaders who not only overcome entrenched gender stereotypes but also act as role models for other women. Importantly, they also serve as role models for men, since more men support women's development and capacity in cybersecurity. Direct dialogue and engagement with women who have achieved success in the field allows other women not only to receive useful advice but also to feel support within their professional community.

3.2.7. Successes in Women's Access to the Field in Ukraine: Overcoming Vertical Gender Segregation

> *"Women who enter cybersecurity have a strong education (focused on exact sciences and facts) and are ready for intellectual challenges."* (Respondent 8)

Among the successes in women's access to the cybersecurity field in Ukraine is the opportunity for women to work in positions across different specializations and levels. Particularly important is women's career advancement to leading and/or managerial positions:

> *"There are senior engineers, there are principal engineers — we simply have a grading system. For example, I have grade 14, and the higher the grade, accordingly, the higher the position. There are grades 17 and 18. These are already quite significant managerial positions."* (Respondent 7)

In particular, women's representation in such positions in the public sector can be highlighted. One respondent noted:

> *"In Ukraine, women hold leadership positions in key institutions responsible for the country's development and security."* (Respondent 13)

Among the greatest achievements of women, respondents highlighted that the Head of the National Cybersecurity Coordination Center is Nataliia Tkachuk, who was mentioned earlier. It is also important to note Kateryna Chernohorenko, who, in her position as Deputy Minister of Defense of Ukraine, is responsible, among other things, for the development of cybersecurity within the Ministry of Defense system. In addition, Yevheniia Volivnyk served as a head of the government incident response team during the full-scale invasion.

The analysis of respondents' answers demonstrates the presence of positive shifts toward the formation of a gender-sensitive environment in Ukraine's cybersecurity sector. This concerns not only the formal increase in women's presence in the field but also real opportunities for their professional growth, expansion of social connections, mentoring support, and institutionalization of gender-sensitive initiatives. This indicates an orientation toward implementing a gender-sensitive approach aimed at increasing women's qualifications, visibility, and engagement in the cybersecurity field.

A significant success in overcoming vertical gender segregation in Ukraine's cybersecurity sector is the existence of female role models and awareness about them. These role models are usually associated with successful women in senior and/or leading positions, which helps break the "glass ceiling." It is equally important that respondents also mentioned to have their female colleagues among role models, which indicates the formation of a support network among women:

> *"I am pleased that through my work I periodically communicate with Nataliia Andriivna Tkachuk, who takes a very active position and serves as Secretary of the National Cybersecurity Coordination Center under the National Security and Defense Council of Ukraine."* (Respondent 10)

Twelve out of fourteen respondents named the name and specialization of at least one woman whom they consider a role model. Some have named three or more. As a result, it can be assumed that such knowledge depends rather on the level of interest and awareness of each individual. Most frequently mentioned by respondents were Nataliia Tkachuk, Head of the Information Security and Cybersecurity Service of the National Security and Defense Council of Ukraine; Anastasiia Ostrovska, co-founder and CEO of the Women's Leadership and Strategic Initiatives Foundation; and Olha Nasibulina, co-founder of the cybersecurity job search platform CyberPeople. Respondents also mentioned Hanna Martyniuk and Yevheniia Nakonechna.

3.3. Ukrainian Media on Women in Cybersecurity

Boiko Diana, Petrovets Marharyta, Mykhailiv Vitalii, Virych Anna, Kostiuk Olena, Davydenko Viktor

3.3.1. Methodology of Media Message Analysis

The study was conducted within the interpretative approach using qualitative thematic analysis of media materials. Thematic analysis is a method that allows the structuring and interpretation of qualitative data by identifying recurring semantic elements related to the research question. [186]This analysis is not tied to a specific theoretical paradigm and therefore can be applied in both deductive and inductive approaches.

The initial stage of data collection was carried out using the Shukach Pro[187] service — a Ukrainian specialized platform for automated search of media content in the Ukrainian online space. It is an information and analytical software product developed by the group of companies "NOKs fishes," which specializes in media monitoring and analysis of the information space in economic, political, and social spheres. Thanks to the director of the company "NOKs fishes" and senior lecturer at the Department of Public Relations at the National University of Kyiv-Mohyla Academy, Oleh Kononenko, access to this platform was provided, which significantly facilitated the work with media materials. A set of key search queries was formed, including: "women in cybersecurity," "female cybersecurity specialists," "gender equality in the digital sphere," and "women in IT." As a result of the search, 710 publications were identified that potentially corresponded to the research topic (*Table 3.3.1.1).*

Table 3.3.1.1. Multi-stage Sampling Design of the Study of the Representation of Women in the Cybersecurity Field in Ukrainian Media, April 2025

Sampling Stage	Stage Description	Inclusion Criteria	Number of Units
1	Search for materials via *Shukach Pro* using keywords	Thematic relevance to search queries	710 publications
2	Removal of news items without analytical content, duplicates, fragmented or promotional	interview, feature story, analytical content; presence of experience description	124 publications

[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/

	materials		
3	Manual cleaning of the sample	Content richness, professional narratives, institutional engagement	71 publications
4	Final structuring	Thematic richness, absence of duplicates, analytical depth	44 44 publications

At the second stage, selection was carried out based on the criteria of content richness and thematic relevance. From the total number of materials, duplicates, advertising content, fragmentary publications, and texts lacking substantive analytical components were removed. As a result, only those publications that contained personal stories, interviews, expert commentary, descriptions of women's professional trajectories in the IT field, and/or reflections on gender equality in the technological environment remained.

At the third stage, manual review and initial cleaning of the sample were conducted. The sample was supplemented with materials from analytical platforms, blogs, and websites of non-governmental organizations operating at the intersection of digital rights, cybersecurity, information hygiene, and women's leadership in technology. This approach ensured thematic diversity and enabled coverage of a wide range of information intermediaries.

At the fourth stage, the final structuring of the sample was carried out — 44 publications were included in the final analysis. They were selected according to the following criteria:

1. belonging to the format of analytical material, an interview, or a personal story;
2. content richness (including descriptions of experience, challenges, social context, etc.).

This form of material presentation made it possible to examine not only the formal presence of women in the media but also the depth, tone, and focus of this representation. The selected publications cover the time period from 2017 to 2025 (see Appendix C).

During the analysis of the materials, predefined thematic categories were used: women in IT and cybersecurity in the labor market, educational programs for women in cybersecurity, women in military cybersecurity and defense, and women as cybersecurity experts.

During the process of analyzing media texts, two analytical approaches were applied — gender-sensitive and gender-neutral — which were used to interpret the content of the selected materials.

The gender-sensitive approach involves identifying and interpreting how women's experiences are represented in media discourse, and whether issues of structural inequality, discrimination, or challenges faced by women in the cybersecurity field are articulated[188]. In contrast, the gender-neutral approach implies that the gender of the character or subject does not play a significant role in the structure of the material. In such publications, women are portrayed exclusively through the lens of professionalism, without reference to the specifics of their experience as representatives of a minority within the field.[189]

3.3.2. Women in IT and Cybersecurity in the Labor Market: Inclusion and Gender (In)equality

Within the gender-sensitive approach to covering the topic of women in cybersecurity, a number of the analyzed publications mentioned the promotion of gender equality in the cybersecurity labor market and the overcoming of stereotypes related to this issue. In one publication, a quote from the Deputy Secretary General of NATO was cited, stating that the exclusion of women from the cybersecurity field is unacceptable:

> *"Cybersecurity is a team sport, and we are leaving half of our players on the bench… NATO seeks the same level of gender equality in cyber defense as in all other aspects of security that we maintain. This is not only right but also necessary for our collective defense." (Material No. 37, 2017).*

Men also commented on the issue of gender inequality within the broader field of information technology, which includes cybersecurity. According to Serhii Tokarev, an IT entrepreneur, gender stereotypes and biases prevent women from entering and developing in the IT sector:

> *"Many Ukrainian women still approach this industry with caution, despite their desire to study and work in IT. Usually this is due to gender bias… And it begins at school. Let us trace the path of an average girl planning to enter the IT field. At school, she diligently studies mathematics, physics, and other sciences and becomes interested in programming. However, already at this stage she encounters the myth that most girls are 'humanities-oriented,' while boys are 'technical specialists.'" (Material No. 27, 2022).*

[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.

Women already engaged in the IT field also agreed with this thesis:

> *"After a series of discussions with researchers in this field, we concluded that stereotypes are the main reason why women choose technical programs less frequently than men." (Material No. 44, 2021).*

At the same time, the media presented the views of girls and women who oppose such stereotypical thinking, emphasizing the meaninglessness of dividing professions by gender. This contributes to greater objectivity in addressing women's involvement in cybersecurity within the information space, challenges established norms and opens space for public discussion on gender roles. Such a media approach may also stimulate the reconsideration of policies and practices that reproduce inequality in this and related fields.

> *"Anna understands that there is no point in dividing professions according to gender: 'Of course! I believe it is inappropriate to divide specialties into those for "girls" and those for "boys," because intellectual abilities are not determined by gender. More important are qualities such as intelligence, perseverance, logical and critical thinking, and determination. If a girl possesses these qualities, why not?'" (Material No. 12, 2023).*

Personal narratives reveal illustrative examples of women's inclusion in the cybersecurity field. For example, one publication described a case of positive discrimination, in which a company deliberately preferred a female candidate to reduce gender imbalance in the IT sector. Such an approach does not deny the candidate's professional qualifications but rather acknowledges that structural inequality requires active intervention to be overcome. At the same time, this highlights that women in technical fields may gain opportunities not only because of exceptional ability but also due to institutional support and changes in corporate culture. This indicates a gradual shift toward an egalitarian model, in which conditions are created for women's genuine inclusion in traditionally "male" fields.

> *"Incidentally, it was precisely because I am a woman that I was able to enter the IT field faster than expected. It turned out that when I interviewed for a Drupal school, there were two strong candidates for the final position: myself and a man. The competitor was even somewhat stronger — he already had experience working with Drupal and had worked with PHP for more than two months, unlike me. However, the company had a goal: to increase the presence of women in the IT sector. Therefore, they chose me, for which I am very grateful." (Material No. 6, 2021).*

At the same time, in a number of analyzed publications that addressed the promotion of gender parity in cybersecurity, women in this field were still implicitly positioned in a secondary role:

> *"The inclusion of women in cybersecurity significantly enhances our ability to counter cyber threats. Women possess a unique way of thinking that complements the approaches of men." (Material No. 22, 2024).*

Ultimately, the media emphasized the importance of an egalitarian approach by employers when publishing job vacancies in cybersecurity, highlighting the need to avoid gender-biased wording that may unconsciously discourage female candidates, and instead to use inclusive language that promotes an open and diverse professional environment:

> *"Cybersecurity job advertisements should be written in such a way that women professionals feel welcome and valued in this field." (Material No. 32, 2021).*

Moreover, according to Article 17 of the Law of Ukraine "On Ensuring Equal Rights and Opportunities for Women and Men[190]" of September 8, 2005, except in specific cases, it is prohibited to indicate the desired gender of a future employee in job vacancies: "Employers are prohibited in job advertisements (vacancies) from offering employment exclusively to women or exclusively to men, except in cases of specific work that may be performed solely by persons of a certain sex; from setting different requirements that give preference to one sex; and from requesting information from job applicants regarding their personal life or plans concerning childbirth."

3.3.3. Educational Programs for Women in the Field of Cybersecurity

A gender-neutral approach in materials about women's training and professional development in cybersecurity is manifested through an emphasis on professional competencies and motivation rather than gender. Gender is presented as a neutral variable — what matters more are ambition, knowledge, and skills. For example, the "Women in Cyber" program is positioned as one that does not require prior experience, but supports those women who have the desire to learn and develop:

> *"This program is aimed at women who want to take their first steps in cybersecurity or deepen their knowledge in this field. The program will provide participants with an opportunity to master the basics of cybersecurity and receive support from successful women leaders in the industry… Who can participate? Women with motivation and a desire to grow in cybersecurity (no prior experience is required)." (Material No. 11, 2025).*

Another example is a webinar emphasizing that professional growth depends on internal determination and the ability to set ambitious career goals:

[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

> *"The USAID project 'Cybersecurity of Critical Infrastructure of Ukraine' decided to organize a webinar for female students to share three stories of charismatic cyber experts… Girls, we invite you specifically to join… We are confident that our speakers will inspire you to set aside your fears (if you have faced them) and to set ambitious goals on the map of your career path." (Material No. 9, 2023).*

Further evidence of the gender-neutral approach is the positioning of cybersecurity as a field open to all people who demonstrate strong logical thinking and an interest in technology. In particular, one competition for teenagers emphasized that the key selection criteria are analytical abilities and coding skills rather than participants' gender:

> *"Girls aged 13–15 will take part in tests on logic and coding, network creation, and cryptography… The UK intelligence agency Government Communications Headquarters believes that teenage girls who spend a lot of time on the internet and social media may become the intelligence officers of the future." (Material No. 13, 2017).*

The use of a gender-neutral approach is also reflected in highlighting the primacy of interests and skills, rather than gender bias, when choosing cybersecurity as a specialization at a higher education institution. For instance, a female student of this program at the State University of Information and Communication Technologies noted:

> *"I believe it is inappropriate to divide specialties into those for 'girls' and those for 'boys,' because intellectual abilities are not determined by gender. More important are qualities such as intelligence, perseverance, logical and critical thinking, and determination. And if a girl has these qualities, why not?" (Material No. 12, 2023).*

The absence of gender bias or special criteria for girls in selection for educational programs is also visible in materials dedicated to the launch of enrollment of girls at the Ivan Bohun Kyiv Military Lyceum, which trains, among others, future specialists in cybersecurity:

> *"This year we plan to enroll from 10 to 30 girls. The first year we requested the minimum number. If it is a successful year, we will justify proposals to the leadership and increase the number," Hordiichuk emphasized. According to him, girls could very professionally support information and psychological operations, cybersecurity, special radio communications, etc. Responding to a question about any special requirements for female applicants, Hordiichuk stressed: "We have gender equality, so the requirements for boys and girls are the same." (Material No. 30, 2019).*

Positioning cybersecurity as a field in which successful professional realization is possible regardless of gender is also found in a publication of the Volyn Regional Employment Center:

> *"We do not divide work into men's or women's," "…three people received a voucher to study a new profession, and one of them mastered the specialty 'Cybersecurity.'" (Material No. 25, 2023).*

In addition, several materials recorded a gender-sensitive approach to describing educational initiatives aimed at supporting women in IT and cybersecurity. These measures are not limited to knowledge transfer alone but also consider the social context and structural barriers women face. They provide specialized support that includes emotional reinforcement, mentoring, preparation for the real labor market, and reducing anxiety before entering a masculinized field.

Participants are given access not only to lectures and practical sessions but also to consultations on career development, psychological resilience, and leadership:

> *"The event convinced 95% of attendees that IT is a business for women.*
> *The event covered topics of effective leadership in a changing reality, cybersecurity, ESG resilience, and lecturers also spoke about career development, mental health, and well-being.*
> *As a sign of solidarity with Ukrainian women, part of the 'Women's Career Day in IT' event was dedicated to workshops conducted by Ukrainian women for Ukrainian women. Mentors and experts from Ukraine shared advice on choosing a profession, finding well-paid work, and preparing for interviews." (Material No. 41, 2022).*

Another example of an educational initiative that contributed to the development of female students in cybersecurity was the mentoring program for women, "Cybersecurity of Critical Infrastructure of Ukraine." The mentors were women with experience in building successful careers in this field. Such initiatives contribute not only to the development of professional skills but also to sharing experience in overcoming barriers faced by professionals in traditionally "male" occupations:

> *"The USAID project 'Cybersecurity of Critical Infrastructure of Ukraine' breaks stereotypes about exclusively 'male' professions and supports women in the cybersecurity industry. The selected participants, together with experienced women professionals, will work on creating their own map of professional development." (Material No. 10, 2022).*

The materials also emphasize the importance of creating professional women's communities that function as professional support and as a means of resisting systemic bias in cybersecurity. They facilitate experience exchange, the development of mentoring practices, and the overall strengthening of women's presence in high-tech sectors:

> *"This event is intended to talk about opportunities to join professional associations of women working in cybersecurity and to introduce some European and Ukrainian women's cyber associations.*

Our speakers from Women4Cyber, EUGAIN, Kharkiv ACM-W Chapter, and ISCA will share their own experience of creating their associations and women's cyber communities. You will also learn about the associations' visions, membership conditions in professional cyber communities, their mentoring programs, and professional development events that will help you build connections within the cyber community." (Material No. 7, 2023).

Another example of a gender-sensitive approach in implementing educational initiatives in cybersecurity is the program "Cybersecurity for Girls: Opportunities and Profession." It provides not only technical knowledge but also the opportunity to learn from successful women professionals in the field:

"In December 2024, a new educational initiative by STEM is FEM will start for girls aged 16–21. The program 'Cybersecurity for Girls: Opportunities and Profession' will help participants master basic digital protection skills and explore career prospects in cybersecurity. In addition to technical knowledge, participants will learn about career opportunities in cybersecurity, success stories of women in the field, and educational resources for professional development." (Material No. 42, 2024).

Special attention is also paid to career guidance initiatives for girls aged 12–16. Such initiatives aim to overcome the gender stereotype of IT as a "male" sphere and to open opportunities before the moment of career choice. Organizers emphasize the importance of positive female examples as lecturers, mentors, and protagonists of success stories. During classes, girls can try themselves in different areas such as data analytics, web programming, or machine learning:

"It is necessary to show young girls that IT is a great field for development, that it is not scary, and that there are examples to follow.
Often girls do not go into IT because they do not see potential like-minded peers nearby. Therefore, to solve this problem, it is necessary to create thematic clubs and communities so that each participant can ask for advice or support from her peers. That is exactly the task we set for ourselves when we created the public organization STEM is FEM." (Material No. 27, 2022).

Another example of efforts to overcome gender bias in schoolgirls' career choices is excursions to technological and research companies:

"On October 8, 2019, the National Girls in ICT Day took place simultaneously in all regions of Ukraine. On that day, about 50 technology companies and research centers opened their doors to schoolgirls in grades 8–10 and female students to awaken their interest in science, technology, engineering, and mathematics (STEM) and to break their stereotypical perceptions of professions… The company 'EY' prepared an engaging two-hour program for young female scientists to involve them in STEM professions. They were surprised to learn that girls can successfully work in cybersecurity and IT consulting at the 'Big Four' company 'EY,' in particular developing IT strategy and conducting IT audits." (Material No. 15, 2019).

A gender-sensitive approach is also evident in the creation of educational opportunities for women's development in cybersecurity at all levels. In addition to horizontal labor market segregation, women professionals often face vertical segregation, which limits their access to leadership positions. Therefore, it is important to implement appropriate programs not only for entering a new field but also at later stages of career development. This is also mentioned by the Head of the Information Security and Cybersecurity Service of the National Security and Defense Council (NSDC) of Ukraine, Secretary of the National Cybersecurity Coordination Center, Nataliia Tkachuk:

> *"We must create opportunities for professional growth and development at all levels — from obtaining education to leadership positions — facilitating the engagement of new talents in the cybersecurity field." (Material No. 31, 2020).*

Another example of a program that supports women's career development in cybersecurity at different levels is a national initiative for developing women's leadership in cybersecurity:

> *"This project will contribute to expanding Ukraine's human resources potential and innovative capacity by ensuring gender equality and involving women in strategic and operational cybersecurity tasks. The initiative not only complies with principles of social justice and human rights but is also a strategic necessity for Ukraine in wartime and will strengthen Ukraine's position as an international leader in cybersecurity." (Material No. 1, 2024).*

3.3.4. Women in Military Cybersecurity and Defense

Direct manifestations of a gender-neutral approach—one that seeks to minimize the significance of gender and universalize the role of a soldier or cybersecurity specialist—are practically absent in the analyzed publications. None of them contain statements such as "cybersecurity has no gender" or similar formulations that would completely ignore gender as a category.

Even in quotations that may imply equality (such as "equal opportunities" in Material No. 18, 2025), the emphasis still falls on women who demonstrate this equality or make use of these opportunities. In other words, gender is not "erased"; on the contrary, it is highlighted as a factor that previously could have caused inequality.

This indicates that at the current stage of development of Ukrainian society and media discourse (after 2014, especially in the context of the war), the presence of women in military and security structures—including cybersecurity structures—remains a relatively new and still insufficiently widespread phenomenon. For this reason, media outlets tend not to ignore the gender aspect; instead, they focus on increasing the visibility of women.

One example of applying a gender-sensitive approach in media materials is the emphasis on women's participation in the military sphere through the presentation of statistical data:

> *"The active participation of women in the defense of the country underscores equal opportunities in the Defense Forces. They effectively occupy both staff and combat positions, including in the fields of medicine and UAVs. Communications and cybersecurity — 6% [regarding the percentage of women in the Defense Forces]." (Material No. 18, 2025).*

This quotation shows that the media not only mention women but also provide concrete statistics of their presence in the relevant field. The phrase "active participation of women" itself is a marker of gender sensitivity because it highlights women's involvement. The figure "6%" is an important empirical indicator that illustrates—although still small—a documented share of women in this sector, making their presence tangible.

A similar example appears in Material No. 3 (2020), dedicated to the Heroes of Kruty Military Institute of Telecommunications and Informatization. It mentions "more than ten percent of girls" among cadets and the fact of enrolling "girls into command specialties." This directly points to an increase in the number of women in military education, including technical specialties such as cyber defense, and makes this trend visible to the audience.

> *"We also have girls studying here, who mostly choose specialties in computer science and cyber defense. For example, if a girl masters the specialty 'cybersecurity,' she will be a hacker and will be able to fight remotely through networks — this will benefit the state. Such women deserve applause! In the case when a female communications specialist becomes the head of a radio-relay station, which includes a vehicle with a heavy antenna-mast device, they may physically not cope with the duties. It is necessary to clearly understand where and in which positions girls will be able to serve and to take this into account. Although it is worth adding that last year, for the first time, girls were enrolled in command specialties. Overall, among cadets there are more than ten percent girls." (Material No. 3, 2020).*

Some media emphasize that women themselves demonstrate interest in acquiring knowledge and skills in cybersecurity:

> *"Educational institutions record a trend of increasing numbers of those who wish to obtain military education in engineering-technical and intelligence profiles. Women in the military wish to study computer science and issues of cybersecurity." (Material No. 36, 2020).*

This reflects recognition of women's agency and their conscious choice to master specialties that were previously perceived as "male."

> *"girls who mostly choose specialties in computer science and cyber defense… a girl will master the specialty 'cybersecurity,' will be a hacker and will be able to fight remotely through networks." (Material No. 3, 2020).*

Here, the choice is not merely stated; it is supplemented by a potential role ("will be a hacker") and its value for the state ("will be able to fight remotely"). This makes the role of a woman cybersecurity specialist more concrete and more significant in the discourse.

A substantial portion of media messages focuses on problems associated with gender stereotypes and inequality and emphasizes the need to overcome them:

> *"It is necessary to abandon stereotypes regarding the role of women in cybersecurity… Supporting gender equality… must become a priority." (Material No. 8).*

This quotation exemplifies a critical stance toward existing barriers (stereotypes that "hinder development") and, at the same time, a call to action in pursuit of equal opportunities. Such a discourse is defining a gender-sensitive approach, which does not conceal problems but instead brings them into public discussion.

This statement, although it concerns NATO, also relays an important message about inequality:

> *"half of our players on the bench… only almost one in ten people working in the field of cyber defense is a woman." (Material No. 37, 2017).*

These phrases—metaphorically and statistically—demonstrate the problem of women's underrepresentation, which is a fundamental inequality that a gender-sensitive approach seeks to reveal and correct.

Although the media do not directly delve into specific gender-conditioned challenges in cybersecurity (such as cyber harassment, sexism in the digital environment, etc.), Material No. 3 (2020), focused on military education and career prospects, raises the issue of women's physiological characteristics. For instance, statements appear such as "physically not cope with the duties" or "it is necessary to clearly understand where and in which positions girls will be able to serve." Such expressions may represent a stereotypical approach to women's ability to perform military functions, even in areas where physical load is not decisive, such as cybersecurity. At the same time, such discussions may also serve as an example of gender sensitivity—acknowledging that women and men may have different needs that should be considered when organizing service. Although this concerns physical aspects, the very principle of "taking gender differences into account for effectiveness and comfort" is universal for a

gender-sensitive approach and can be applied to any aspects of service, including ensuring appropriate working conditions for women cybersecurity professionals.

The Secretary of the National Cybersecurity Coordination Center (NCCC), Nataliia Tkachuk, stated at a meeting of the National Cybersecurity Cluster on the topic "The Role of Women in Ensuring Ukraine's Cyber Resilience: Challenges and Prospects":

> *"During the full-scale invasion of the Russian Federation, involving women in cybersecurity is not merely a matter of equality or compliance with international standards. It is a vital necessity for strengthening national security and ensuring the resilience of the state. Women have always played an important role in the development of our country, and today their contribution becomes even more significant. We must create opportunities for professional growth and development at all levels — from obtaining education to leadership positions — facilitating the engagement of new talents in the field of cybersecurity." (Material No. 22, 2024).*

This excerpt clearly demonstrates a shift from a gender-neutral to a gender-sensitive approach. The state recognizes not only women's presence but also the necessity of their active involvement in security policy. In this context, what matters is not only equal representation but also the understanding that women play an indispensable role in shaping the state's cyber resilience. This is further reinforced by a quote from the Deputy Secretary of the National Security and Defense Council of Ukraine, Serhii Demediuk:

> *"Women have unique thinking that complements men's approaches, creating synergy that allows the successful resolution of the most complex tasks. We must encourage more women and girls to find their place in the cyber sphere, because their potential can strengthen our capacity at all levels — from operational actions to strategic planning and making key decisions." (Material No. 22, 2024).*

This statement emphasizes the value of gender diversity as a resource in decision-making. Women do not simply join an existing hierarchy—they change its structure by bringing a different type of thinking, which is critically important in the context of the Russian-Ukrainian war.

It is important to note that even before the beginning of Russia's full-scale invasion of Ukraine, in 2021, active work on developing cyber defense began, including with the goal of creating cyber forces. As N. Tkachuk stated:

> *"The Ministry of Defense of Ukraine faces a very important and necessary task of building cyber forces."*

"The activities of cyber forces can become our asymmetric response to the aggressor." (Material No. 24, 2021).

These steps formed the basis for establishing relevant structures and training personnel, including women, who ensured reliable protection of national cyber infrastructure during wartime. Women's contribution to the creation and functioning of cyber forces may be decisive in the context of strategically strengthening Ukraine's defense capability during the war.

3.3.5. Women as Cybersecurity Experts

In the analyzed publications, media tended to portray women experts in IT, including cybersecurity, as role models meant to inspire others—especially girls—to enter the field. In other words, the focus was on stories of success and overcoming barriers:

"Zoia Rashevska, a developer at ELEKS, initially worked as an economist and, five years ago, after maternity leave, transitioned into the IT sector. She told us about how difficult her path in IT was, about the biggest challenge, and about everyday work in a field where most colleagues are men." (Material No. 6, 2021).

The importance of successful women experts in cybersecurity as examples was also emphasized in the following statement:

"Many young women… fear an industry that is traditionally considered male… However, today many successful women work in cybersecurity and can share their own inspiration…" (Material No. 7, 2023).

Thus, in such media materials, women experts do not appear as background participants but rather as full-fledged and necessary agents of cyber defense, whose participation is not merely desirable but strategically important.

The depiction of women in responsible positions in security and cybersecurity (as in Material No. 23 (2021), which mentions "…the head of the Information Security and Cybersecurity Service of the Apparatus of the National Security and Defense Council of Ukraine, Nataliia Tkachuk") is an important component of a gender-sensitive approach. The very fact of mentioning a woman in such a high and responsible position within a key state body dealing with security and cybersecurity issues is unquestionably positive in terms of increasing women's visibility in the field. It demonstrates that women reach high levels of expertise and hold significant positions, sending an important signal for overcoming stereotypes about women's limited opportunities in traditionally "male" industries.

At the same time, full gender sensitivity implies not only substantive representation but also attentiveness to linguistic form. The use of the masculine form **“керівник”** (“head”) instead of the feminine form **“керівниця”** (“female head/leader”) may indicate the influence of traditional language norms or inconsistency in media usage, since the use of feminatives is a technical marker of sensitivity that is present in other materials—for example, the words **“лідерка”** (“female leader”) (Material No. 11, 2025) or **“президентка”** (“female president”) (Material No. 34, 2025). Thus, mentioning a woman in the position is substantively gender-sensitive, while the linguistic form is less consistent. This indicates the need for deeper integration of a gender-sensitive approach not only in content but also in the form of media representation.

Conclusions

Historical analysis shows that since the 20th century, women have played an important role in the development of computer science and information technology, although their contributions have often been undervalued or rendered invisible due to dominant gender stereotypes. According to current data, women remain underrepresented in cybersecurity, accounting for approximately 24–30% of IT professionals worldwide. The root causes emerge already at the educational stage, where girls are less encouraged to study STEM subjects, which leads to their lower representation in technical university programs. International programs such as **CyberCorps: Scholarship for Service** in the United States and initiatives by organizations such as **Women in CyberSecurity (WiCyS)** have proven effective in providing scholarships, mentorship, and career support for women, thereby facilitating their engagement in the cybersecurity field. Additionally, corporate programs such as IBM's **Tech Re-Entry** support women's reintegration after career breaks by providing opportunities for further professional development. These efforts collectively emphasize the importance of continuous multi-level measures—from early education to career development—to overcome gender imbalance in the cybersecurity labor market.

Cybersecurity, as a male-dominated field, continues to demonstrate significant gender imbalance due to a number of sociocultural, educational, and institutional barriers, including stereotypes, bias in hiring, and insufficient support for women in professional environments. These factors, reinforced by the phenomenon of the "leaky pipeline," limit both the recruitment and retention of women in the field, which is particularly critical given the shortage of cybersecurity professionals. Taking gender diversity into account and increasing women's representation is strategically important for improving the effectiveness of cyber defense and fostering innovation in the face of modern cyber threats. This confirms the need for systematic implementation of gender-sensitive policies in cybersecurity.

Successful strategies for overcoming barriers in cybersecurity are based on a combination of micro-, meso-, and macro-level mechanisms: from individual support and role models to institutional transformations in education (university programs and specialized courses such as CyberFirst, Women4Cyber, etc.), corporate initiatives (Google, Microsoft, IBM), and government policies (quotas, flexible schedules, reintegration after maternity leave) aimed at creating a gender-sensitive environment and eliminating structural discrimination. At the same time, combating deeply rooted gender stereotypes regarding women's roles in technological fields remains a key issue. These stereotypes, which define cybersecurity as a "male" field, create structural barriers to women's entry and career advancement and reinforce gender segregation within the industry.

The study of statistical data on women in cybersecurity employment and education revealed common trends both internationally and within Ukrainian education. The main trend is clear horizontal gender segregation, with women comprising on average less than 30% of the field. Internationally, North and South America demonstrate the highest proportion of women in

cybersecurity, while Africa has the lowest. At the same time, in some countries, such as Nigeria and Mexico, women may constitute up to one-third of cybersecurity professionals. In Ukrainian higher education institutions selected for analysis, the average proportion of women studying in specialty 125 “Cybersecurity” remained a minority, averaging 26%.

At the same time, there is a growing trend in women’s participation in cybersecurity. At the global level, this is confirmed by gender-age structures: women under the age of 30 constitute 24% of the workforce, which is 9% higher than the share of women aged 40 and older. Similar changes can be observed in Ukrainian higher education institutions, where the proportion of women in first-year cohorts is higher than in senior years. However, this trend is not universal and may have different explanations, including objective factors such as Russia’s full-scale invasion of Ukraine in 2022, as well as internal institutional processes such as systematic attrition of female students in later years.

Currently, women in cybersecurity worldwide, on average, have higher levels of education than men. Data from Ukrainian universities also indicate higher academic performance among women compared to men. However, women globally still receive lower wages than men in the same positions and occupy only 16% of leadership roles, highlighting the need for additional measures to overcome both horizontal and vertical segregation.

One possible solution may be to promote women’s participation in programs that provide initial educational qualifications necessary for careers in cybersecurity, such as associate degrees or basic higher education. This would allow women to occupy positions in subfields where they are currently underrepresented. Unlike increasing the share of women with master’s or doctoral degrees—often underutilized in professional practice—such a strategy may contribute to a real reduction in gender imbalance.

Thus, despite positive trends in recent years toward increased interest and participation of women, a significant gender gap persists in cybersecurity. This indicates the need for continued active measures to achieve full gender equality.

Despite growing recognition of the importance of women’s integration, this process remains somewhat contradictory, though it demonstrates significant progress. The current legal framework in Ukraine contains progressive elements: the Law of Ukraine “On Ensuring Equal Rights and Opportunities for Women and Men” establishes the obligation of state bodies to implement gender equality and provides mechanisms for gender legal expertise, while the Law “On Preventing and Combating Discrimination” formalizes the possibility of legally challenging discriminatory practices. These provisions are complemented by the general principle of non-discrimination embedded in the Law “On the Basic Principles of Ensuring Cybersecurity of Ukraine.” Significant progress has also been made through initiatives supporting women led by the state, civil society, and business. For example, the National Cybersecurity Coordination Center has strengthened support for women’s leadership, and the inclusion of gender aspects in the National Action Plan for implementing UN Security Council Resolution 1325 has provided women with access to specialized training and participation in policymaking. Platforms such as

SheCyber Hub, Women4Cyber Ukraine, and CDTO Campus are developing, while retraining programs similar to “Reskilling Ukraine” and leadership and mentorship programs from international partners are being implemented. IT companies also demonstrate commitment to DEI policies, and international corporations launch educational projects for women, including those affected by the war, thereby creating more favorable conditions for professional growth.

Despite these achievements, the path toward gender integration in Ukrainian cybersecurity is complicated by systemic problems. Key legal acts often demonstrate insufficient gender sensitivity: they frequently declare neutrality but overlook specific digital threats faced by women, such as cyber violence, sextortion, and online harassment. Existing mechanisms for implementing anti-discrimination legislation show low effectiveness due to a lack of clear procedures and adequate institutional support. Strategic documents, including the Cybersecurity Strategy Implementation Plan, largely ignore the gender dimension, reflecting the dominance of a technocratic rather than an inclusive approach. Deeply rooted structural barriers also remain significant obstacles, including persistent stereotypes about the “non-feminine” nature of the profession, the dominance of informal male professional networks, and the “glass ceiling” effect limiting women’s career advancement, especially in technical and leadership positions. These issues are compounded by pronounced horizontal and vertical gender segregation and a persistent gender pay gap. The education sector also faces challenges, including a lack of specialized technical training programs for women and a shortage of formalized mentorship networks. Finally, a critical problem is the lack of systematic gender-disaggregated data and comprehensive research on the situation of women in Ukraine’s cybersecurity sector, particularly in wartime conditions, which significantly complicates evidence-based policymaking and monitoring.

These systemic challenges and achievements become particularly dynamic in the context of Russia’s full-scale war against Ukraine, which has acted as a catalyst for contradictory transformations. On the one hand, extreme conditions and workforce shortages have created certain “windows of opportunity” for women, increasing their presence and visibility in the cybersecurity sector. On the other hand, the militarization of public discourse and economic instability risk reinforcing existing vulnerabilities and strengthening traditional gender stereotypes, further complicating progress toward equality. In these conditions, achieving sustainable gender equality and effectively utilizing the potential of all professionals to strengthen national cyber resilience requires a comprehensive and strategically balanced approach. This includes not only continued support programs but also systematic integration of gender perspectives into legislation, educational standards, inclusive corporate cultures, and—most importantly—the establishment of systematic collection and analysis of gender-disaggregated data.

Overall, this study demonstrated that women in cybersecurity in Ukraine may face a complex set of structural and symbolic barriers that begin at entry into the profession and persist throughout their careers. While some respondents reported no personal experience of discrimination and noted workplace support, these positive examples may represent exceptions rather than the norm. The most common barriers identified included doubts about professional

competence, devaluation of knowledge, gender stereotypes during job interviews, and lack of organizational response to discriminatory behavior.

At the same time, respondents also noted gradual positive changes. The number of women in educational programs and companies is increasing, more educational and mentorship initiatives are emerging, and examples of support from colleagues and leadership are becoming more common. Some respondents reported the formation of equal working environments in certain organizations, which may indicate potential positive transformations.

Thus, creating an inclusive and comfortable environment in cybersecurity requires a comprehensive approach—from institutional changes to women's personal confidence and active participation. All proposed recommendations aim to overcome structural barriers, reduce the impact of gender stereotypes, and support women's professional growth. However, alongside external changes, internal resilience and self-confidence remain extremely important.

Based on the analysis of expert interviews regarding the successes and challenges of women's participation in cybersecurity during the Russian-Ukrainian war, both challenges and achievements in access, representation, and support were identified. Among the key challenges were horizontal and vertical segregation; psychological pressure and increased responsibility associated with gender stereotypes; the gender pay gap; sexual harassment, often in the form of "special treatment" in workplaces, particularly in public institutions; and lack of awareness or inefficiency in implementing initiatives and reforms, especially at the state level.

Key successes include improved accessibility and representation of women in cybersecurity; an increase in the number of women in leadership positions; the presence of positive female role models and greater awareness of them; the development of mentorship programs and training for women; the implementation of initiatives and reforms supporting women in cybersecurity at the state level; and a decrease in gender bias among younger generations in Ukraine.

The main recommendations proposed by respondents included the creation and implementation of mentorship programs; information campaigns at all levels of education; the development of professional and inclusive communities; encouraging women's participation in various events and projects; providing scholarships and grants for female students; and supporting female role models.

The application of qualitative thematic analysis within an interpretative approach enabled a deep understanding of how Ukrainian media represent women's participation in cybersecurity. As a flexible tool for analyzing qualitative data, thematic analysis allowed not only the structuring of a large volume of information but also the identification of key content patterns focused on gender equality, professional identity, and social recognition of women in the high-tech sector.

The sample was multi-stage: the selection of analysis units was conducted in four stages, resulting in a representative dataset. Out of 710 initially identified media units, 44 materials

(published between 2017 and 2025) were included in the final sample. Their analysis, conducted through thematic coding, identified key themes: (1) Women in IT and cybersecurity in the labor market: participation and gender inequality; (2) Educational programs for women in cybersecurity; (3) Women in military cybersecurity and defense; (4) Women as cybersecurity experts. The combination of automated search via the Shukach Pro platform and subsequent manual sample refinement enabled the formation of a relevant and high-quality data source. Clearly defined sampling stages helped avoid the inclusion of non-representative or superficial materials and ensured comprehensive thematic coverage.

The study adopted an egalitarian approach to analyzing representations of women in cybersecurity, as no media materials demonstrating explicit gender inequality or stereotypical portrayals of women were identified. Instead, the analyzed publications mainly focused on support, empowerment of women, promotion of educational initiatives, and overcoming barriers to participation, which generally aligns with principles of gender equality and inclusion.

The qualitative thematic analysis of media revealed two main tendencies: a gender-sensitive approach (emphasizing inequality, women's experiences, and structural barriers) and a gender-neutral approach (focusing on professional qualities without emphasizing gender).

Media address the issue of women's underrepresentation in cybersecurity, particularly in the military sphere (where their share reaches only 6%), and highlight initiatives supporting them, such as mentorship programs, quotas, and educational courses. These include mentorship initiatives such as USAID projects for cybersecurity students, positive discrimination practices in IT companies, legislative prohibition of specifying gender in job vacancies under Ukrainian law (2005), educational webinars for female students (Material No. 9, 2023), and events such as the National Girls in Technology Day. However, some publications still portray women as a "complement" to men or ignore gender-inclusive language.

An important step toward equality is the elimination of gender stereotypes at the educational level, career guidance for girls, and the creation of conditions for their career advancement. A positive trend is the growing number of materials presenting women as cybersecurity experts and leaders, contributing to the formation of new social norms.

During the study, media demonstrated their role not only as a reflection of social processes but also as agents of social change. They play a significant role in transforming perceptions of women's professional opportunities in strategically important sectors, particularly in the context of full-scale war, where cybersecurity plays a critical role.

Recommendations

Recommendations for Improving the Situation of Women in Cybersecurity

As a result of the interviews, recommendations were identified for companies and for women in the cybersecurity field. Recommendations for companies concerned creating a supportive working environment for women, while recommendations for women focused on personal growth in cybersecurity.

One mechanism companies can apply to improve the situation of their female employees is equal treatment of women and men in the workplace, which includes the absence of gender-based requirements or expectations, as well as equal pay.

> *"I am simply saying that the best attitude toward women is the same attitude as toward men—equal treatment for everyone. There should not be 'woman' and 'man'; there should simply be a specialist." (Respondent 2)*

> *"I know there are companies that underpay women. Honestly, it is quite strange to underpay women in our field. There should simply be equal value placed on a person." (Respondent 8)*

Respondents also advised increasing the number of women in companies as one way to overcome gender stereotypes about women's alleged lack of professionalism in cybersecurity. Direct interaction with women in teams allows colleagues to form a more objective understanding of their competence. In addition, more active involvement of women in the field increases their overall visibility in society, which contributes to rethinking cybersecurity as an exclusively "male sphere."

> *"In general, I think the more women work in a company, the less sexism there is. Because men directly see a woman working in this profession, and everything is great. She is not breaking anything; she did not come to ruin everyone's life." (Respondent 4)*

Increasing women's presence in cybersecurity is possible through implementing measures that motivate women to work in this field. First, companies can disseminate information about learning and employment opportunities in cybersecurity among schoolgirls. Girls may not consider cybersecurity as a potential career due to gender stereotypes that associate it with being "male." Accordingly, educational events and other programs can help girls learn about the advantages of working in this field and foster interest in it.

"Awareness. Cybersecurity is a very broad field where people with very diverse skills are needed, as I said at the beginning. And I would raise awareness in this regard among girls who are choosing where to study. Because it is not only a popular and relevant field —it is also very interesting and very useful for society overall. So, I would probably organize some career-guidance events." (Respondent 3)

Second, companies can motivate and support female cybersecurity students by organizing conferences that allow women to demonstrate their professional skills and achievements, as well as by introducing grant programs (Respondent 1). In addition, some respondents emphasized the importance of mentors in their professional development. Therefore, implementing mentorship programs in companies can be an effective mechanism of support and adaptation for female employees.

"If I had the opportunity to change something, I would probably focus attention on developing a mentoring culture and support. Often women in this field simply lack examples of support or confidence. Creating communities, open platforms for exchanging experience, and internal corporate mentoring programs could significantly influence the development of equal opportunities." (Respondent 5)

Beyond attracting more women to cybersecurity, respondents emphasized the importance of developing clear strategies for building a supportive working environment. In particular, this includes creating training plans for employees and effective mechanisms for responding to cases of discrimination.

"I would advise companies to pay attention not only to gender diversity, but also to creating real conditions for balance: flexible schedules, development programs, a safe and respectful environment, and also clear mechanisms for responding to discrimination." (Respondent 5)

Respondents also provided advice directly for women working in cybersecurity, regardless of their professional experience. One of the key points was the need to reduce fear of new challenges and to be willing to demonstrate one's abilities. It was noted that women often hesitate to participate in competitions and events such as CTFs or bug bounties due to lack of confidence. Therefore, it is important to support women and encourage their active participation in such events to strengthen confidence in their abilities.

"Strongly encourage women to show themselves and prove themselves in competitions, at CTFs, in bug bounties, because it is very useful, and many women are afraid of CTFs and bug bounties precisely because of this feeling that they are not enough, that they do not know enough." (Respondent 1)

It was also emphasized that women should not be afraid of failure, since failures are part of the learning and development process. Respondents underlined that discouragement and fear are normal emotions on the path to success. Fear should not stop a person; on the contrary, it should motivate overcoming obstacles.

> *"…not to be afraid. Because fear is always the first thing that stops you. If I had been afraid, I would not have gone to the interview, I would not have gotten into Kyiv-Mohyla Academy, I would not have passed the National Multi-Subject Test." (Respondent 1)*

> *"If you are afraid of something, it does not mean it is not for you. It actually means it is for you. And that you want to do it. And you want to do it well. So, discouragement and fear are normal. And you do not need to be afraid of fear." (Respondent 3)*

Respondents stressed persistence, self-confidence, and continuous development as key factors for achieving success in cybersecurity. Persistence in performing professional tasks and confidence in one's own abilities help overcome obstacles that often arise due to fear of the unknown or new challenges.

> *"Be as persistent as possible and do not be afraid of failures. You should not give up after a few unsuccessful interviews." (Respondent 6)*

In addition, respondents emphasized the importance of lifelong learning and developing professional skills. They advise continuously seeking new opportunities to improve qualifications and maintaining connections with the professional community through participation in trainings, conferences, and other events.

> *"Always look for something new for yourself, learn, communicate with people, be an active participant, attend various forums, take part in conferences." (Respondent 9)*

Recommendations for Companies:

- Ensure equal treatment of women and men in the workplace, including equal pay for equal work.
- Increase the number of women employed in cybersecurity companies to overcome gender stereotypes and enhance women's visibility in society.
- Disseminate information about educational and career opportunities in cybersecurity among schoolgirls to reduce stereotypes and biased perceptions of the profession.
- Organize conferences, educational initiatives, and grant programs aimed at motivating and supporting women in cybersecurity.

- Develop clear strategies for creating a supportive work environment, including training programs, flexible working arrangements, and effective mechanisms for responding to discrimination.

Recommendations for Mentors:

- Implement structured mentorship programs within companies to support and facilitate the professional adaptation of women in cybersecurity.
- Establish professional communities and platforms for experience-sharing and peer support among women in the field.

Recommendations for Women Planning to Enter the Cybersecurity Field:

- Actively participate in professional events to strengthen self-confidence and foster professional development.
- Embrace new challenges and engage in competitions and professional initiatives as a means of personal and career growth.
- Demonstrate persistence and readiness to face challenges, which contributes to overcoming fear of failure and supports long-term professional advancement.

Recommendations Regarding Women's Access to Cybersecurity in Ukraine: Educational Factors

The experts also shared recommendations concerning women's access to the cybersecurity sector in Ukraine. Three primary categories of recommendations were identified: (1) reforms in education at the secondary, higher, and supplementary levels; (2) increased awareness of cybersecurity as a professional field, particularly among girls and women; and (3) the formation and support of professional communities to facilitate interaction and development of women in this domain.

> *"I think certain narratives should be changed already in kindergarten and school, because when you see math problems in textbooks like: 'Vasyl assembled a clock, and Masha picked apples in the garden,' it starts from early childhood—these stereotypes and prejudices are embedded from a young age." (Respondent 5)*

The results of the expert interviews indicate that the educational dimension occupies a central place among the recommendations for improving women's access to cybersecurity in Ukraine. A key direction involves transforming approaches to shaping perceptions of gender roles and professional opportunities from an early age. Within secondary education, it is essential to combat stereotypes by revising educational materials and implementing awareness campaigns that present technological careers as equally accessible to girls. Respondents emphasized that

introducing students to cybersecurity career pathways during their school years would foster interest and promote a gender-neutral perception of the field.

> *"Perhaps at school, during IT classes, they could explain that such a field even exists." (Respondent 2)*

Regarding higher education, respondents stressed the need to intensify curriculum modernization processes, including the integration of contemporary practices and the direct involvement of cybersecurity professionals in teaching. Particular importance was attributed to the development and implementation of grant programs and targeted scholarships for women, which could serve as additional incentives for women to enter and further specialize in this field. At the same time, respondents highlighted the necessity of structural reforms within higher education, including modernization of teaching approaches and strengthening lecturers' engagement in preparing highly qualified professionals.

> *"The second [innovation at the state level] is to change the educational system. And this is not only a problem of attracting girls, but of the entire educational system. What we currently have is outdated conditions and lecturers who are often not interested in investing effort into teaching students. In reality, there are only a few universities that truly prepare strong professionals and invest in their students." (Respondent 13)*

Postgraduate education and professional training are identified as important instruments for the further career development of women in cybersecurity. Respondents highlighted mentorship as a key component of professional growth. They recommended the active implementation of mentoring programs that would help women overcome career-related and psychological barriers and strengthen their self-confidence. One respondent shared her personal experience, describing how her mentor helped her reconsider her career trajectory and the challenges she faced:

> *"My mentor was the former CEO of Microsoft Ukraine. It is valuable because you can look at your career differently, reconsider the challenges you face, ask for advice in various areas, and understand that it is normal for people to encounter such challenges at certain stages of their lives or careers." (Respondent 11)*

Thus, respondents emphasized the decisive role of educational institutions in supporting women in cybersecurity and in advancing the field more broadly, proposing ways in which increased participation of women can contribute to the overall development of the sector.

Recommendations Regarding Women's Access to Cybersecurity in Ukraine: Awareness of the Field and Women's Opportunities

"The more opportunities you see, the more you will pursue them." (Respondent 11)

Respondents' recommendations for increasing awareness of cybersecurity and improving women's access to the field in Ukraine encompass several key directions. At a general level, they proposed intensifying information campaigns aimed at dismantling gender stereotypes and promoting cybersecurity as an accessible field for women. Respondents emphasized the importance of developing specialized professional media that would provide high-quality and accessible information about the field for both professionals and the public.

Additionally, organizing open conferences and forums targeted at young people may contribute to community building and reduce informational barriers to entering the field. One respondent highlighted the necessity of transforming societal attitudes toward women, noting that such attitudes influence all aspects of women's experiences:

> *"First, public opinion must change so that there are no prejudices toward women, and legislative instruments are secondary mechanisms that reinforce this shift." (Respondent 5)*

Respondents particularly emphasized initiatives and reforms aimed at raising awareness among school pupils and university students. Suggested measures included the creation of dedicated scholarship programs and the involvement of girls in cybersecurity competitions. One respondent also stressed the importance of engaging parents in girls' career orientation, as parental perceptions such as *"Cybersecurity is not really a female profession; it is better to become a programmer"* (Respondent 7) remain prevalent.

The active implementation of mentoring and coaching programs was also identified as an important mechanism for supporting young women during their studies and early career stages.

Regarding direct measures to encourage women specialists, respondents recommended expanding internship opportunities in public and private institutions, organizing regular hackathons and Capture-the-Flag (CTF) competitions with dedicated participation of women's teams, and increasing women's involvement in international projects to facilitate experience exchange and practical skill development. State support—particularly funding educational programs and introducing tax incentives for companies that actively recruit women—was highlighted as an effective motivating factor:

> *"These include tax incentives for companies that hire women in the cyber sphere, state funding for beginner cybersecurity courses, and educational mentoring programs, among other initiatives." (Respondent 3)*

Many respondents also emphasized the importance of female role models in the public information space. They highlighted the need for greater visibility of successful women in cybersecurity and targeted information campaigns showcasing women's achievements and

active participation in the field. According to respondents, this would help overcome societal myths and stereotypes and increase women's visibility in cybersecurity. One respondent shared her personal reflections on the importance of drawing attention to women in the field:

> *"We need to highlight role models—successful women. I would like journalists to seek comments specifically from women, to show that they exist in our field, to celebrate their achievements rather than treating their presence as something marginal or insignificant." (Respondent 13)*

Recommendations Regarding Women's Access to Cybersecurity in Ukraine: Community and Support for Women

> *"Honestly, what I currently lack most in Ukraine is a professional community." (Respondent 11)*

Respondents also emphasized the importance of establishing and supporting professional communities for women in cybersecurity, stressing the need to create a favorable environment for interaction and professional development. They highlighted the importance of developing infrastructure that would enable women professionals to collaborate and exchange knowledge and experience.

One recommendation involved the regular organization of open forums and conferences accessible to early-career specialists. Additionally, respondents proposed creating a dedicated web portal containing informational resources to facilitate the integration of new participants—especially women—into the professional community. They also emphasized the importance of encouraging women to join existing female professional networks and participate in state-level initiatives:

> *"At the state level, attention should be paid to building networking opportunities specifically for women in cybersecurity. Usually, when hackathons or IT competitions are organized, participants are mostly men." (Respondent 6)*

Respondents further highlighted the importance of supporting women within the professional community itself. In addition to the already mentioned mentoring and coaching practices, they emphasized the need to establish flexible working conditions, promote women to leadership positions, organize initiatives aimed at combating gender-based violence, and ensure transparent working conditions, including salary transparency. Overall, respondents stressed the importance of acknowledging women's experiences, challenges, and achievements within the professional community. One respondent noted that such strategies could help prevent cases of discrimination and biased attitudes toward women:

“Perhaps we should listen to women when they report incidents at work that occurred related to their gender, so that management takes this into account and prevents such situations from occurring in the future.” (Respondent 12)

List of References

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). “Ґендерне 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/usaid-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. 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.
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
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 IT-сектор. https://uacrisis.org/uk/zhinok-zaklykayut-aktyvnish-e-jty-v-it-sektor
35. Яблоновська, Т. (2020, 5 жовтня). Рейтинг вишів для IT-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.pgitl.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-prodbc0f-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/ncscc_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.orangecyberdefense.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.orangecyberdefense.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., AlShaalan, M. B. H. (2022, sep). Empowering women to work in cybersecurity: Is a win-win. Boston Consulting Group. https://api.gcforum.org/api/files/public/upload/70f628b0-7cd5-42c0-9280-f64bfcb8ad1d_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

Appendices

Appendix A. Guide for Conducting a Semi-Structured Interview in the Study "Women in Ukrainian Cybersecurity: Voices of Those Who Have Overcome Barriers"

Informed Consent

Hello! My name is (name), and I am a third-year student of Sociology at the National University of Kyiv-Mohyla Academy. I am conducting a research study titled *"Women in Ukrainian Cybersecurity: Voices of Those Who Have Overcome Barriers"* as part of the course *Gender Studies* under the supervision of Tamara Martsenyuk, PhD in Sociology and Associate Professor at the Department of Sociology.

Thank you for agreeing to participate in my research. The interview will take the form of a conversation during which you will be asked several questions. Our discussion will last approximately one hour. Any information you provide will be used separately from your personal data; your name or any other identifying information will not be disclosed.

During the interview, there are no right or wrong answers. Please try to respond openly and honestly. You also have the right to refuse to answer any question or withdraw from participation at any time. Please note that the conversation will be recorded solely for internal analytical purposes in an aggregated form. However, you also have the right to refuse the recording.

If you have any questions regarding the interview, you may contact me by phone (…) or by email (…).

Do you agree to participate in the interview under these conditions?

Block 1. Introduction: Background, Education, Career Path, and Professional Experience (20 minutes)

- Please tell us a little about yourself and the position you currently hold.
- Do you have a university degree in cybersecurity, or did you acquire your knowledge through other resources (including online/offline courses)?
- What motivated you to choose the field of cybersecurity?
- What were the main factors that motivated you to develop in this field? *(For the interviewer: ask the respondent to name, for example, three main factors.)*
- Did you have a mentor who helped you with employment or professional development in this field?
- What are your current responsibilities in your company/organization in your position?
- How long have you been working in this field?

- In your opinion, how does management treat you?

Block 2. Barriers and Challenges in Employment and Career Development (20 minutes)

- What is the ratio of men to women in your team?
- How did you feel at the beginning? Did you notice any difficulties in communication or networking?
- Did you notice that because of your gender you could not become a full member of the team?
- Did you experience increased competition during employment?

If the answer to the previous question is “yes”:

- Did you notice that you were treated differently as a candidate because of your gender?
- Did you experience discrimination or bias in the professional environment?

If the answer to the previous question is “yes”:

- How did these barriers affect your career and personal development? Which barrier had the greatest impact on you?
- Were there situations when you felt that your success was attributed to “luck” or “chance” rather than your knowledge and efforts?
- Did you have to make additional efforts to prove your competence due to gender stereotypes?
- Were there moments when you considered changing your career because of these barriers?

Block 3. Perception by Society (10 minutes)

- In your opinion, how does society perceive women in technical fields?
- Have you encountered judgment or misunderstanding from others regarding your profession or field of interest?
- Have people’s attitudes toward your career choice changed over time?
- Have you encountered the view that “women are not suited for cybersecurity”?
- What inappropriate questions about your profession have you heard?
- How do your family and friends perceive your work? Do they understand what exactly you do?

Block 4. Final Section (5 minutes)

- Have you observed changes in attitudes toward women in this field during your career?
- If you had the opportunity to change something in the cybersecurity field (for example, culture, approaches, or attitudes toward women), what would you change and why?
- What advice would you give to companies seeking to create a more supportive environment for women in cybersecurity?
  (Clarifying question: What practical steps could contribute to this?)

- What advice would you give to women who are just beginning their path in cybersecurity? What could help them overcome potential challenges and develop in this field?
- Is there anything you would like to discuss that has not been covered during our interview?

Appendix B. Guide for Conducting a Semi-Structured Expert Interview in the Study "Women's Access to the Cybersecurity Sector in Ukraine"

Hello, (name). Thank you for agreeing to participate in this interview.

My name is (name), and I am a student at the National University of Kyiv-Mohyla Academy. As part of the course *"Introduction to Gender Studies"*, my team and I are conducting research on women's access to the cybersecurity sector in Ukraine. The results of this interview will be used for the academic study titled *"Women's Access to the Cybersecurity Sector in Ukraine."* We have decided to approach you as an expert respondent.

The purpose of this research is to identify the achievements and challenges related to women's access to cybersecurity in Ukraine.

I will record our conversation to accurately capture all responses for further analysis. I guarantee confidentiality. Your responses will be anonymized and analyzed in aggregated form. The recording will be used exclusively for academic purposes (including the preparation of scholarly publications). If at any point during the interview you would like to make an off-the-record comment, please inform me.

Do you agree to the recording of this interview?

The approximate duration of the interview is about one hour.

I will speak Ukrainian, and you may respond in whichever language you feel most comfortable.

Please let me know whether this information is clear and whether you consent to participate in this interview and its recording.

If you do not have any questions at this time, we may proceed.

Block 1. Introduction

1. To begin, I would like to learn about your professional experience in cybersecurity.
2. What is your current position?
3. How many years have you worked in the cybersecurity field?
4. Did you obtain formal education in the specialty "Cybersecurity"?

(If NO: How did you acquire the skills necessary for working in cybersecurity?)

5. What motivated you to choose a career in cybersecurity?
6. In your opinion, what are the greatest challenges and achievements of the cybersecurity sector in Ukraine today?
7. How would you comment on the importance of cybersecurity in the context of the full-scale Russian invasion and, more broadly, the Russian-Ukrainian war?

Block 2. Representation of Women in Cybersecurity in Ukraine

8. In your view, is there a noticeable gender imbalance in the cybersecurity sector in Ukraine?
9. How would you assess the level of representation of women and men in your workplace? If possible to generalize, what categories of women (considering age, marital status, and other socio-demographic characteristics) tend to enter cybersecurity? For which categories of women is this field most accessible and why?
10. In your opinion, has the beginning of the full-scale Russian invasion affected women's access to and participation in the cybersecurity sector in Ukraine? What has been the nature of this impact and why?

Block 3. Challenges to Women's Access to Cybersecurity in Ukraine

11. What positions do women occupy in your workplace?
12. In your opinion, is there a gender pay gap in the cybersecurity sector in Ukraine?

12A (for male respondents): Have you observed bias against women in your workplace? Which categories of women experience such treatment and why? Have you witnessed instances of sexual harassment toward women in your workplace?
12B (for female respondents): Have you personally encountered gender bias, stereotypes, or sexual harassment in your workplace? Have your female colleagues encountered such situations?

13. In your view, what factors lead women to leave positions in the cybersecurity sector in Ukraine?

Block 4. Achievements in Women's Access to Cybersecurity in Ukraine

14. Does your organization implement initiatives aimed at attracting or supporting women in cybersecurity (e.g., quotas, training programs, professional development courses)?
15. Are state-level initiatives effective in supporting women's participation in cybersecurity (e.g., information campaigns, grants, women's communities, gender equality legislation)?
16. Could you provide examples of successful women who have built careers in cybersecurity globally? In Ukraine?
17. What do you consider the three greatest achievements of women in cybersecurity in Ukraine?

Block 5. Recommendations

18. What state-level innovations would make cybersecurity more accessible to women?
19. What measures should be taken to encourage greater participation of women in Ukraine's cybersecurity sector?
20. How can cybersecurity institutions/companies/structures in Ukraine support women who are already employed in the field?
21. Is there anything you would like to add?
22. Could you recommend 2–3 colleagues who might be willing to share their views on the achievements and challenges faced by women in cybersecurity in an expert interview format?

Thank you for your time and attention.

Appendix C. List of Units of Analysis

Table C.1. **List of Media Materials Included in the Sample for the Study of the Representation of Women in Cybersecurity in Ukrainian Media**

Item Number	Media Outlet	Number of Materials	Link	Title	Date of Publication
1	0522.ua	1	https://www.0522.ua/news/3854596/natalia-tkacuk-nkck-zapocatkovue-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/	Генерал-майор Євген Степаненко розповів,	29.01.2020

			2020/01/29/general-major-yevgen-stepanenko-rozpoviv-yak-gotuyut-kibervoyiniv-i-zvyazkivcziv/	як готують кібервоїнів і зв'язківців	
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-minoborony-nazvalo-iaki-vakansiyi-obyraiut-zinky-u-rekrutynhovykh-tsentrakh	Міноборони назвало, які вакансії обирають жінки у рекрутингових центрах	27.01.2025
6			https://hromadske.ua/posts/zavdyaki-tomu-sho-ya-zhinka-meni-vdalosya-potrapiti-v-it-yak-zminiti-profesiyu-i-stati-programistkoyu	"Завдяки тому, що я жінка, мені вдалося потрапити в IT". Як змінити професію і стати програмісткою	23.06.2021
7	Громадський Простір	4	https://www.prostir.ua/event/vebinar-zhinky-u-kiberbezpetsi-stvorennya-	Вебінар "Жінки у кібербезпеці: створення професійних асоціацій на основі успішних практик"	10.03.2023

			profesijnyh-asotsiatsij-na-osnovi-uspishnyh-praktyk/		
8			https://www.prostir.ua/?news=genderne-riznomanittya-v-kiberbezpetsi-realiji-ta-mozhlyvosti-dlya-zhinok-v-ukrajini-vidbuvsya-dialoh-v-mezhah-prohramy-dialoh-pro-kiberbezpeku	“Ґендерне 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-karjery-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-studentok-spetsialnosti-kiberbezpeka	Набір на менторську програму для студенток спеціальності “Кібербезпека”	28.07.2022
11	Детектор медіа	1	https://detector.media/infospace/article/239800/2025-04-08-u-cdto-campus-tryvaie-nabir-na-dvi-	У CDTO Campus триває набір на дві програми для жінок: лідерство в цифровізації та кібербезпека	08.04.2025

			programy-dlya-zhinok-liderstvo-v-tsyfrovizatsii-ta-kiberbezpeka/		
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: крізь об'єктив 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-vikhovanki-kiivskoi-man-vidznachili-natsionalniy-den-divchat-u-tekhnologiyakh	Занурення у бізнес компанії “IT-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_Natsion	Екскурсія майбутніх аудиторок та фінансистів у компанію “EY” у рамках Національного Дня Дівчат в технологіях	11.10.2019

			alnogo_Dnja_Divchat_v_tehnologijah/		
16	Львівський портал	1	https://portal.lviv.ua/news/2023/02/02/start-it-cisco4ukaine-bezkoshtovne-onlajn-navchannia-u-sferi-it-dlia-ukraintsiv	Start IT. Cisco4Ukaine: безкоштовне онлайн-навчання у сфері IT для українців	02.02.2023
17	Маріупольський державний університет	1	https://mu.edu.ua/news/zhinki-v-kiberbezpeci-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-syly-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-bezkoshtovnii-kurs-z-kiberbezpeki-dlia-ukrayintsiv-97473.html	Google запустив безкоштовний курс з кібербезпеки для українців	30.05.2023
21	Подробиці	1	https://podrobnosti.ua/2495041-u-stolits-vdbuvsja-forum-	У столиці відбувся Форум талановитої молоді: нагороди та досягнення	26.01.2025

			talanovito-molod-nagorodi-ta-dosjagnennja.html		
22	Рада національної безпеки і оборони України	3	https://www.rnbo.gov.ua/ua/Diialnist/7087.html	Роль жінок у зміцненні кіберстійкості України стала головною темою засідання Національного кластера кібербезпеки	18.12.2024
23			https://www.rnbo.gov.ua/ua/Diialnist/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/Diialnist/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 IT: 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 IT	18.10.2022

28	Українські новини	1	https://ukranews.com/ua/news/741206-na-vebinari-vid-stem-is-fem-ta-oon-zhinky-rozpovily-pro-metody-zahystu-vid-kiberzlochyniv	Як убезпечити себе в Інтернеті – поради з вебінару STEM is FEM та "ООН-Жінки"	27.11.2020
29	Укрінформ	2	https://www.ukrinform.ua/rubric-ato/2568246-kiberoborona-bezpecni-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 ліцей Богуна вперше набиратимуть дівчат	29.03.2019
31	Юридична газета	1	https://yur-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-kiberbezpeczi/	Жінки в кібербезпеці	29.12.2021
33	Finance.ua	1	https://about.pumb.ua/presscenter/news/item/6296-pumb-stal-uchastnikom-	ПУМБ став учасником Національного дня дівчат у технологіях	13.10.2021

			nacionaljnogo-dnya-devochek		
34	IGate.com.ua	1	https://igate.com.ua/news/30553-set-university-ta-darkowl-pochinayut-spvpratsyu-u-sfer-kberbezpeki	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-hhi-stolittya/	Жінки в IT: реалії XXI століття	22.07.2021
36	KRIVBASS.CITY	1	http://krivbass.city/news/view/v-ukraini-zrostae-populyarnist-vijskovoi-osviti-sered-zhinok	В Україні зростає популярність військової освіти серед жінок	22.09.2020
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-viyna-zminila-gendernu-strukturu-v-ekonomici-ukrajini-	Нові реалії: як змінюються ролі жінок у бізнесі?	18.11.2024

			50466406.html		
40	PRportal	1	https://prportal.com.ua/Fakty/posilannya-na-neisnuyuchi-storinki-peretvorili-na-profili-uspishnih-zhinok-naukovic	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 Карьєри Жінок в IT” 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-cyberin-transformuye-novenkih-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-mozhlivosti-u-tsifrovomu-sviti/	Берта Херреро про різноманіття, інклюзію та рівні можливості у цифровому світі	01.01.2021