DOI 10.31558/2307-2318.2025.3.2

УДК 004.056.5:005.336.3(477)
JELClassification: J24, O33, H56

Bezzubchenko Olga
Associate Professor. Department of Economic and International Economic Relations,
Mariupol State University, Kyiv, Ukraine, o.bezzubchenko@mu.edu.ua,
ORCID ID: https://orcid.org/0000-0001-6791-3881
Balabanova Natalya
Associate Professor. Department of Economic and International Economic Relations,
Mariupol State University, Kyiv, Ukraine, n.balabanjva@mu.edu.ua,
ORCID ID: https://orcid.org/0000-0003-4391-3451

STRENGTHENING THE CYBERSECURITY WORKFORCE: CHALLENGES AND STRATEGIC PRIORITIES FOR NATIONAL RESILIENCE

The article explores current challenges and strategic prospects for developing a professional workforce in the field of cybersecurity. In the context of digitalization and growing cyber threats, the shortage of qualified personnel becomes one of the main barriers to ensuring national cyber resilience. The study analyzes the international experience of leading countries such as the USA, Israel, Singapore, Estonia, and EU members, which implement systemic models of training, certification, and professional development for cybersecurity specialists. Special attention is paid to the current state and challenges of cybersecurity workforce development in Ukraine, including government policy, international cooperation, retraining programs, and the advancement of educational initiatives. A comparative analysis of key cybersecurity indices (GCI, NCPI, NCSI, ENISA, etc.) is provided, with an emphasis on the human capital dimension. The paper substantiates the need for a multilevel approach to the development of cybersecurity workforce to ensure digital sovereignty and national cyber resilience.

Keywords: *cybersecurity, labor resource provision, digital transformation, cyber resilience, international labor market, cyber education, human capital, public policy, cybersecurity indices.*

Tab. - 3, Ref. - 22.

Беззубченко Ольга
к.е.н., доцент кафедри економіки та міжнародних економічних відносин,
Маріупольський державний університет, Київ, Україна, o.bezzubchenko@mu.edu.ua,
ORCID ID: https://orcid.org/0000-0001-6791-3881
Балабанова Наталя
к. н. з держ. упр., доцент кафедри економіки та міжнародних економічних відносин,
Маріупольський державний університет, Київ, Україна, n.balabanjva@mu.edu.ua,
ORCID ID: https://orcid.org/0000-0003-4391-3451

ПОСИЛЕННЯ КАДРОВОГО ПОТЕНЦІАЛУ У СФЕРІ КІБЕРБЕЗПЕКИ: ВИКЛИКИ ТА СТРАТЕГІЧНІ ПРІОРИТЕТИ ДЛЯ НАЦІОНАЛЬНОЇ СТІЙКОСТІ

У статті досліджено актуальні виклики та стратегічні перспективи формування професійного кадрового потенціалу у сфері кібербезпеки. В умовах *цифровізації та зростання кіберзагроз кадровий дефіцит стає одним із головних бар'єрів для забезпечення національної кіберстійкості. Проаналізовано міжнародний досвід провідних країн світу, зокрема США, Ізраїлю, Сінгапуру, Естонії та країн ЄС, які впроваджують системні моделі підготовки, сертифікації та професійного розвитку фахівців. Особливу увагу приділено стану та викликам розвитку кіберкадрів в Україні, включаючи державну політику, міжнародну співпрацю, перепідготовку кадрів та розвиток освітніх програм. Представлено порівняльний аналіз ключових індексів кібербезпеки (GCI, NCPI, NCSI, ENISA тощо) з акцентом на кадрову складову. Обґрунтовано необхідність багаторівневого підходу до розвитку людського капіталу для забезпечення цифрового суверенітету та кіберстійкості держави.*

Ключові слова: *кібербезпека, трудоресурсне забезпечення, цифрова трансформація, кіберстійкість, міжнародний ринок праці, кіберосвіта, кадровий потенціал, державна політика, індекси кібербезпеки.*

Табл. - 3, Літ. – 22.

Problem Statement In today's context of accelerated digitalization and the growing number of cyber threats, ensuring national cybersecurity has become one of the key challenges for countries around the world, including Ukraine. The resilience of the state, business, and society to cyberattacks directly depends on the quality and quantity of specialists in this field. The formation of a qualified cybersecurity workforce is a strategic priority that will define the country's future in the digital age.

Review of Recent Research and Publications Issues related to skilled workforce development in cybersecurity are being studied by individual researchers as well as prominent international organizations and academic groups. Among the most influential contributors are teams from ISC2, NIST NICE, BCG, and the SANS Institute, along with researchers from the Delft University of Technology and the University of Waterloo. Their studies cover topics such as workforce shortages, the development of training standards, motivational factors, and career pathways in cybersecurity [1,2,3,4,5,6].

Notably, Prof. Dr. Michel van Eeten (Delft University of Technology, Netherlands) focuses on the economics of cybersecurity, workforce motivation, labor market trends, and public policy in the cybersecurity domain. Dr. Simon Parkin (Delft University of Technology) explores behavioral aspects, professional development, and workforce management. A multidisciplinary research group (Papageorgiou, Jacqueline Wong, Qinyi Liu, Mohammad Khalil, A.J. Cabo, and others) investigates training methodologies, skills development, and educational strategies in cybersecurity [7,8]. Additionally, the ISC2 Research Team conducts in-depth annual studies on the global cybersecurity workforce, analyzing skills shortages, professional development, certification pathways, and talent acquisition strategies. Their reports are among the most authoritative in the field. The National Initiative for Cybersecurity Education (NICE) unites researchers, educators, and industry representatives to explore workforce development, labor market trends, and competency frameworks. The Boston Consulting Group (BCG) and the Global Cybersecurity Forum (GCF) jointly examine workforce shortages, gender balance, skills needs, and strategies for attracting new talent to the cybersecurity sector [5]. The SANS Institute, one of the world's leading training and certification organizations, regularly publishes analytics on talent development, effective recruitment practices, training, and talent retention [6].

Research Objective The aim of this study is to identify the key challenges and future prospects for the development of a professional cybersecurity workforce in the context of global trends, international best practices, labor market demands, and state policy. It also aims to provide practical recommendations for strengthening human capital as a critical factor in ensuring national cyber resilience.

Main Content Overview Modern cyber threats compel governments to design comprehensive security ecosystems that combine legal, technological, and organizational mechanisms.

The level of cyber resilience of a state or organization depends on multiple interrelated factors encompassing both technical and institutional dimensions. Key indicators allow for a comprehensive assessment of the ability to withstand cyberattacks, respond effectively, and recover from incidents. These include cyber readiness—ensuring timely and effective responses through incident response plans, training, and system testing. Equally important is the protection of critical information infrastructure, which is essential for the continued functioning of energy, transport, and communications systems.

Other critical aspects include continuous monitoring, rapid incident detection, and effective response mechanisms. All of these require a skilled workforce, underscoring the importance of human capital and continuous professional development. Cyber hygiene awareness among employees and the public is fundamental to digital security. Protection against modern threats increasingly depends on implementing cutting-edge solutions such as Zero Trust, cloud security, and multi-factor authentication [9].

Cyber resilience also depends on the presence of a robust institutional and regulatory framework that defines standards and coordinates efforts between government, industry, and civil society. Investments in new technologies, research, and innovation are likewise crucial for assessing the current state of cybersecurity and building forward-looking strategies [10].

The experience of cybersecurity-leading countries demonstrates the effectiveness of a systemic approach to workforce development. Countries such as the USA, the United Kingdom, Israel, and Estonia implement continuous learning, certification, and practical training programs. Leading nations actively integrate international standards (e.g., ISO 27001) into curricula and focus on certifying professionals according to global requirements. Both public and private initiatives are successfully implemented: specialized training centers are created, tailored courses are developed, and partnerships with universities and businesses are strengthened [11]. Successful training models are based on close collaboration among universities, IT companies, and government bodies. This approach ensures responsiveness to market needs, practical skill-building, and timely updates to educational content. Another growing trend is practice-oriented and dual education. Global experience confirms the effectiveness of combining theory with practice through internships, hackathons, real-world projects, and cyber ranges. This prepares students with in-demand skills sought by employers.

Non-formal education and initiatives such as workshops, trainings, online courses, and IT cluster programs also play an important role in increasing student engagement and hands-on experience. Equally crucial is the development of soft skills and interdisciplinary competencies. Modern specialists must possess not only technical expertise but also teamwork, communication, critical thinking skills, and the ability to work with real-world data and security testing tools.

The integration of emerging technologies and current cybersecurity trends is also a defining feature. Leading countries are embedding topics such as artificial intelligence, machine learning, cloud security, Zero Trust, and encrypted traffic analysis into educational programs. This ensures that training aligns with industry demands.

Furthermore, international experience exchange, participation in global initiatives, and lifelong learning are increasingly seen as key to maintaining a high professional standard. Leading universities and organizations participate in international training sessions, conferences, and joint projects, enabling the rapid adoption of best practices and adaptation to changing cybersecurity landscapes. In response to the rapid evolution of cyber threats, leading countries promote continuous skill upgrading through modern educational platforms, certification programs, corporate learning, and personalized learning paths.

Cyber hygiene awareness among the population is emphasized through public information campaigns and training programs. Broad public-private partnerships facilitate rapid adaptation to emerging threats and experience sharing, while investments in research spur innovation, new specializations, and increased system flexibility. Standardization and certification—especially through internationally recognized credentials—ensure workforce quality and harmonization of professional requirements. Countries with high levels of cyber resilience combine national policy, educational innovation, and global best practices to effectively confront digital-era challenges.

These trends confirm that cybersecurity workforce development is a complex, multilayered process requiring adaptability, innovation, and close cooperation among all stakeholders. Leading countries provide key models and innovative strategies. Cybersecurity development rankings, analytical reports, and indices are typically used to identify global leaders. The most authoritative indices include the Global Cybersecurity Index (GCI), National Cyber Power Index (NCPI), National Cyber Security Index (NCSI), and ENISA reports, each assessing the workforce dimension to varying extents [11,12,13,14]. The most authoritative indices include the following:

Table 1 – Comparison of Country-Level Cybersecurity Assessment Methods

Index Name	**Objective**	**Main Components**	**Example of Use**	**Methodology (Does it account for workforce development?)**
Global Cybersecurity Index (GCI)	Assessment of countries' cybersecurity commitments across five areas	Legal framework, technical measures, organizational measures, capacity development, cooperation	GCI reports show countries' overall readiness level	The "capacity development" component includes the assessment of training programs, certifications, and training centers
National Cyber Power Index (NCPI)	Evaluation of cyber capabilities for both defense and offense	National capabilities, intentions, influence potential in cyberspace	The U.S. and China rank highest due to strong offensive capabilities	Assesses the ability to build cyber forces, including education, science, and technology
National Cyber Security Index (NCSI)	Assesses countries' ability to prevent cyber threats and respond to incidents	Legislation, institutions, cooperation, policy effectiveness	Estonia ranks high due to transparent governance structures	Indirectly, via the presence of programs and bodies responsible for cyber education
Cybersecurity Readiness Index	Assesses how prepared companies/countries are for modern cyber threats	Identify, protect, detect, respond, recover	Applied in the private sector to determine risk levels	Focused on technical measures and corporate readiness
ENISA Reports	Analyze threats, trends, and the effectiveness of national strategies	Policy analysis, infrastructure, standards, cyber skills	Used to inform EU cybersecurity policy	The "Human Capacity" section highlights workforce training, educational initiatives, and national strategies

Based on the analysis, all indices incorporate workforce development to some extent, although the degree of focus varies. GCI, NCPI, and ENISA reports place particular emphasis on this aspect, making them especially valuable for analyzing human capital in cybersecurity. Rankings may differ as they focus on various indicators—for instance, ENISA focuses on the European context and assesses compliance with EU directives and standards, while NCSI concentrates on measurable aspects implemented by central governments such as existing legislation, established structures, cooperation formats, and outcomes.

Table 2 – NCSI Country Rankings [13]

Rank	Country	Index	Education & Professional Development	Digital Development Level
1	Czech Republic	98.33	100%	72.93
2	Canada	96.67	100%	78.14
3	Finland	95.83	100%	85.76
4	Poland	92.50	100%	73.21
5	Belgium	92.50	100%	73.55
6	Germany	90.83	100%	75.73
7	Italy	88.33	100%	73.58
8	Estonia	88.33	100%	82.56
9	Australia	87.50	100%	82.60
10	Lithuania	85.00	80%	62.34
21	Ukraine	80.83	60%	71.87

Other Rankings - FM Resilience Index 2025: Denmark, Luxembourg, Norway, Switzerland, Singapore, Sweden, Germany, Finland, Belgium, and the central U.S. rank in the top 10 in overall resilience, including cybersecurity. - Cisco Cybersecurity Readiness Index 2025: Measures the "maturity" of organizations across five key pillars of cyber defense. The top performers include the U.S., Canada, the UK, Germany, Singapore, Japan, and Australia. - Global Cybersecurity Index (GCI, ITU): Consistently led by the U.S., the UK, Saudi Arabia, Estonia, South Korea, Singapore, UAE, Finland, and Canada.

Key trends in 2025 include: first, European leadership in cybersecurity, with EU countries—especially Czech Republic, Finland, Estonia, Poland, and Belgium—strengthening their positions through state policy, investment, and international cooperation. Second, the regional gap: Europe and North America exhibit the highest confidence in cyber resilience, while African and Latin American countries lag due to limited resources and expertise. Third, the growing importance of cyber resilience as more countries integrate cybersecurity into their national strategies for resilience and economic development.

With the rise of digitalization and the corresponding need for effective cybersecurity, leading countries increasingly invest in specialized educational centers and training programs to systematically qualify cybersecurity professionals.

Table 3 – Key Features of Cybersecurity Workforce Development

Country / Region	Workforce Education Characteristics
USA	Over 300 educational programs; emphasis on certifications (CompTIA, (ISC)², Cisco); active involvement of major tech companies (Google, IBM); large-scale digital skills development from early education (e.g., CISA CETAP).
Israel	Mandatory military service in cybersecurity (notably Unit 8200); use of modern training platforms (e.g., Cympire); support for startups and innovative approaches.

Country / Region	Workforce Education Characteristics
Singapore	CyberSG Talent & Innovation Center for training, reskilling, and international exchange; collaboration between government, universities, and business; state funding of educational initiatives.
EU (ENISA)	Development of the European Cybersecurity Skills Framework; support for educational programs and harmonization of cybersecurity training across EU member states.

Approaches to developing cyber education and workforce capacity in leading countries demonstrate strategic vision and systematic actions covering all levels—from early education to professional training and international cooperation.

In the United States, significant attention is paid to cybersecurity skills development starting from elementary school (K–12), fostering a cybersecurity culture from an early age. The certification system covers numerous areas (CompTIA, $(ISC)^2$, Cisco, etc.) and is actively supported by major tech corporations such as Google and IBM. Large-scale retraining programs are in place, including for non-traditional target groups—veterans, individuals without technical education, and professionals from other sectors. Programs like CISA and GIAC are examples of an integrated career development policy in cybersecurity [15,16].

Israel is known for its military unit Unit 8200, which has become a source of highly qualified personnel for the cyber industry. Military service serves as an important stage of training, with many veterans later founding startups or joining the tech sector. Innovative training platforms such as Cympire simulate cyber threats for hands-on skill development. Collaboration between the military, academic institutions, and the startup ecosystem creates an effective environment for workforce development. Israeli startup initiatives focused on training military personnel in cybersecurity are examples of this synergy [17].

Singapore is actively investing in the creation of educational and innovation centers. A key project is the CyberSG Talent, Innovation and Growth (TIG) Center, launched in 2023 as a joint initiative of the Cyber Security Agency of Singapore (CSA) and the National University of Singapore (NUS). The center, funded with USD 20 million from the state and the university, aims to foster talent, innovation, and economic growth in the field of cybersecurity. This strategic platform not only supports professional advancement but also strengthens Singapore’s position as a global cybersecurity innovation hub [18].

The European Union (via ENISA) works toward the unification of competency standards in cybersecurity. The focus is on developing educational programs, supporting certification initiatives, and ensuring workforce mobility across EU member states. The European Cybersecurity Skills Framework is designed to create a unified approach to training and mutual recognition of qualifications. ENISA also publishes practical resources, such as the Handbook for Cyber Stress Tests, which assist in assessing the cyber resilience of organizations and systems.

Estonia is one of the world leaders in digitalization, making cybersecurity a national priority. The government implements the "Cyber-Conscious Estonia 2024–2030" strategy, which covers education development, workforce training, and strengthening the protection of critical services and infrastructure. The country employs a decentralized cybersecurity governance model, with responsibilities distributed among various institutions that coordinate across sectors.

Estonian universities, notably Tallinn University of Technology (TalTech), offer specialized cybersecurity programs, where over 50% of instruction involves labs, simulations, and case analysis. Curricula include both fundamental IT disciplines and advanced topics such as cryptography, penetration testing, and cyber risk management. A key feature is close cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), allowing students to participate in international exercises, including Locked Shields—the world's largest cyber defense simulation. The government invests in upgrading educational infrastructure, developing exchange programs, and expanding certification pathways.

Despite significant achievements, the 2025 Global Cybersecurity Outlook by the World Economic Forum shows that the global cybersecurity talent shortage has reached a critical level: two-thirds of surveyed organizations report a significant or severe skills shortage, which slows cybersecurity development and increases business risk. Only 14% of companies feel adequately prepared for current cyber threats [11].

This explains the annual rise in demand for cybersecurity experts across countries. By 2025, cybersecurity jobs in the U.S. are expected to grow by 33% over the next eight years—one of the fastest growth rates globally, according to the U.S. Bureau of Labor Statistics and industry reports. In Finland, demand grows by 15–18% annually due to ongoing digitalization of the economy and public services. Singapore shows impressive yearly growth in demand, with some reports estimating a 16.14% annual increase, driven by the expanding cybersecurity market projected to reach significant scale by 2029. In Israel, labor market data show a 35% surge in cloud security roles, a 31% increase in penetration testing positions, and a 24% rise in cybersecurity management roles—driven by a dynamic cyber industry, startup ecosystem, and military programs. Estonia sees annual demand growth of 13–15%, supported by public service digitalization and international cooperation.

Key causes of the shortage include:

– Low education standards: Many training programs do not meet labor market needs, often lacking practical experience and valid certifications.

– High expectations for experience and credentials: Employers increasingly require internationally recognized certificates (e.g., CompTIA, (ISC)², Cisco) alongside academic degrees, which complicates job placement for junior professionals.

– Competition between public and private sectors: Skilled professionals prefer higher-paying private-sector roles, making public-sector recruitment difficult.

– Lack of retraining pathways: There is a shortage of structured retraining opportunities and continuous education for professionals from adjacent fields.

A 2025 study by the SANS Institute confirms that effective training, certification programs, and attracting non-traditional candidates (e.g., career switchers) are vital to narrowing the cybersecurity talent gap. As digitalization intensifies, leading countries increasingly invest in specialized educational centers and structured training programs to build systematic qualifications in cybersecurity.

In Ukraine, despite active progress, the lack of qualified cybersecurity professionals remains a major barrier to strengthening national cyber defense. The shortage is estimated at around 100,000 specialists, creating a critical gap between existing threats and available resources to counter them. Even advanced technology cannot function effectively without skilled personnel to conduct analytics, respond to incidents, manage infrastructure, and make decisions under pressure [20,21,22].

The causes are complex. First, the full-scale war has led to the mobilization of many specialists and driven emigration—many experts were forced to leave the country. Second, international demand for Ukrainian professionals promotes outsourcing and brain drain. Third, the current education system lacks practical skill development: graduates often have only theoretical knowledge and no certifications, hindering their job prospects. Moreover, low public-sector salaries push young professionals toward private or international firms.

Given the rising number and complexity of cyberattacks—especially during wartime—the workforce shortage threatens the effectiveness of Ukraine's cyber defense. It limits monitoring and incident response capacity, which is vital for protecting government registries, infrastructure, and businesses. The lack of qualified personnel also slows the adoption of innovative solutions and technologies that could enhance national cyber resilience.

Thus, the issue of securing human resources in the field of cybersecurity is not merely an educational or staffing concern, but a strategically important factor for national security. Overcoming this barrier requires a systemic approach, including the reform of workforce training systems, increased motivation for public sector employment, and the creation of conditions for the return of specialists from abroad.

In the context of rapidly growing cyber threats and digitalization, Ukraine is actively implementing measures to develop a robust cybersecurity workforce. The State Service of Special Communications and Information Protection (SSSCIP), as a key governmental body, is focusing on expanding the national occupational classifier: the number of cybersecurity-related specializations has significantly increased—from two to twenty-seven. At the same time, a network of qualification centers is being developed, where specialists can take professional certification exams, improving the quality of training and competitiveness on the labor market. International cooperation—particularly with NATO, the EU, and the USA—plays a significant role in implementing modern educational standards and certifications.

Ukraine's educational system is adapting to new challenges by offering upskilling and reskilling programs for professionals from other sectors. Modern digital platforms and cyberattack simulation tools are becoming vital components of practical training. Simultaneously, international certifications such as CompTIA Security+, CEH, and CISSP are gaining importance, significantly improving employability and salary prospects.

Ukraine is gradually integrating into the global cybersecurity ecosystem by participating in international hackathons, training exercises, and knowledge exchange projects. Close cooperation between the government, business, and educational institutions enables the formation of joint cyber incident response teams and strengthens the resilience of the country's critical infrastructure.

Career prospects for cybersecurity specialists are extremely broad—from entry-level positions to senior leadership roles such as Chief Information Security Officer (CISO) or Security Director. Earnings in this field vary significantly depending on qualifications and experience: junior specialists may earn from 25,000 UAH, while top-level managers can exceed 200,000 UAH.

Conclusions. Therefore, strengthening human resources in cybersecurity is not just an educational or staffing issue but a matter of national security. Overcoming this barrier requires a systemic approach: reforming education, improving public-sector motivation, and creating conditions for professionals to return from abroad. Without a systematic resolution—through educational reform, competitive remuneration, the development of certification programs, and robust international cooperation—the country will remain vulnerable to modern cyber threats.

A multilevel approach is essential for addressing this challenge, combining efforts from the state, the private sector, the academic community, and international partners. Priorities must include the modernization of training programs, support for lifelong learning, creation of retraining pathways for professionals from related fields, and the introduction of practical, certification-based education.

Ukraine must also enhance motivation to work in the public sector by improving career prospects and remuneration, while simultaneously developing mechanisms for attracting and retaining specialists. Investments in cyber education, training infrastructure, and human capital development must become a key component of national cybersecurity policy. Only through the synergy of education, policy, business, and international collaboration can Ukraine achieve cyber resilience and safeguard its digital sovereignty in the face of rapidly evolving threats.

REFERENCES

1. World's leading member association for cybersecurity professionals. Revealing New Opportunities for the Cybersecurity Workforce. https://www.isc2.org/research

2. How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

3. ISC2 Cybersecurity Workforce Study, 2024. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

4. New Data on the Cybersecurity Workforce. https://www.nist.gov/news-events/news/2024/10/new-data-cybersecurity-workforce

5. Cybersecurity Workforce Report 2024: Bridging the workforce shortage and skills gap. https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap/

6. Cyber security workforce recruiting, development, and retention. sans.org/build-your-team

7. Veerle Van Harten, Carlos Hernandez Ganan, Michel Van Eeten, Simon Parkin (2025), All Sorts of Other Reasons to Do It.

8. E. Papageorgiou, Jacqueline Wong, Qinyi Liu, Mohammad Khalil, A.J. Cabo (2025), A Systematic Review on Student Engagement in Undergraduate Mathematics: Conceptualization, Measurement, and Learning Outcomes, In Educational Psychology Review Volume 47.

9. Trendy z kiberbezpeky v blahodiinosti u 2025 rotsi. https://www.prostir.ua/?library=trendy-z-kiberbezpeky-v-blahodijnosti-u-2025-rotsi

10. The Cyber Resilience Compass: Journeys Towards Resilience, 2025. https://www.weforum.org/publications/the-cyber-resilience-compass-journeys-towards-resilience/

11. Global Cybersecurity Outlook 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

12. ENISA https://www.enisa.europa.eu/sites/default/files/2025-06/The%20EU%20Cubersecurity%20Index%202024_en_0.pdf

13. National Cyber Security Index (NCSI). https://ncsi.ega.ee/country/fi/

14. National Cyber Power Index (NCPI). https://www.belfercenter.org/publication/national-cyber-power-index-2022

15. Cybersecurity Workforce Research Report 2025. https://www.giac.org/mlp/2025-attract-hire-retain-cybersecurity-roles/

16. Perspective: Revitalizing America's Cybersecurity – A Call for Public/Private Partnership and National Standards. https://www.hstoday.us/featured/perspective-revitalizing-americas-cybersecurity-a-call-for-public-private-partnership-and-national-standards/

17. Israeli Cybersecurity Startup To Provide Training For IDF https://nocamels.com/2024/10/israeli-cybersecurity-startup-to-provide-training-for-idf/

18. Opening of CyberSG Talent, Innovation and Growth (TIG) Collaboration Centre. https://www.csa.gov.sg/news-events/press-releases/opening-of-cybersg-talent--innovation-and-growth-(tig)-collaboration-centre

19. Finland Cybersecurity Job Market: Trends and Growth Areas for 2025. https://www.nucamp.co/blog/coding-bootcamp-finland-fin-finland-cybersecurity-job-market-trends-and-growth-areas-for-2025

20. Stratehiia kiberbezpeky Ukrainy (2021 – 2025 roky). nbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

21. Ukrainskyi rynok pratsi u 2025: populiarni profesii, kliuchovi navychky y trendy. https://happymonday.ua/ukrayinskyj-rynok-pratsi-u-2025
22. Ohliad rynku kiberbezpeky v Ukraini. https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. World's leading member association for cybersecurity professionals. Revealing New Opportunities for the Cybersecurity Workforce. https://www.isc2.org/research
2. How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
3. ISC2 Cybersecurity Workforce Study, 2024. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study
4. New Data on the Cybersecurity Workforce. https://www.nist.gov/news-events/news/2024/10/new-data-cybersecurity-workforce
5. 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/
6. Cyber security workforce recruiting, development, and retention. sans.org/build-your-team
7. Veerle Van Harten, Carlos Hernandez Ganan, Michel Van Eeten, Simon Parkin (2025), All Sorts of Other Reasons to Do It.
8. E. Papageorgiou, Jacqueline Wong, Qinyi Liu, Mohammad Khalil, A.J. Cabo (2025), A Systematic Review on Student Engagement in Undergraduate Mathematics: Conceptualization, Measurement, and Learning Outcomes, In Educational Psychology Review Volume 47.
9. Тренди з кібербезпеки в благодійності у 2025 році. https://www.prostir.ua/?library=trendy-z-kiberbezpeky-v-blahodijnosti-u-2025-rotsi
10. The Cyber Resilience Compass: Journeys Towards Resilience, 2025. https://www.weforum.org/publications/the-cyber-resilience-compass-journeys-towards-resilience/
11. Global Cybersecurity Outlook 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
12. ENISA https://www.enisa.europa.eu/sites/default/files/2025-06/The%20EU%20Cubersecurity%20Index%202024_en_0.pdf
13. National Cyber Security Index (NCSI). https://ncsi.ega.ee/country/fi/
14. National Cyber Power Index (NCPI). https://www.belfercenter.org/publication/national-cyber-power-index-2022
15. Cybersecurity Workforce Research Report 2025. https://www.giac.org/mlp/2025-attract-hire-retain-cybersecurity-roles/
16. Perspective: Revitalizing America's Cybersecurity – A Call for Public/Private Partnership and National Standards. https://www.hstoday.us/featured/perspective-revitalizing-americas-cybersecurity-a-call-for-public-private-partnership-and-national-standards/
17. Israeli Cybersecurity Startup To Provide Training For IDF https://nocamels.com/2024/10/israeli-cybersecurity-startup-to-provide-training-for-idf/
18. Opening of CyberSG Talent, Innovation and Growth (TIG) Collaboration Centre. https://www.csa.gov.sg/news-events/press-releases/opening-of-cybersg-talent--innovation-and-growth-(tig)-collaboration-centre

19. Finland Cybersecurity Job Market: Trends and Growth Areas for 2025. https://www.nucamp.co/blog/coding-bootcamp-finland-fin-finland-cybersecurity-job-market-trends-and-growth-areas-for-2025
20. Стратегія кібербезпеки України (2021 – 2025 роки). nbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf
21. Український ринок праці у 2025: популярні професії, ключові навички й тренди. https://happymonday.ua/ukrayinskyj-rynok-pratsi-u-2025
22. Огляд ринку кібербезпеки в Україні. https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf