*I.J. Information Technology and Computer Science,* **2025, 2, 24-35**
Published Online on April 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2025.02.03

# Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns

**Oleksandr Korystin***
State Scientifically Research Institute of the MIA of Ukraine, Kyiv, Ukraine
Private Higher Educational Institution "Bukovinian University", Chernivtsi, Ukraine
Institute of Cyber Warfare Research
E-mail: alex@korystin.pro
*Corresponding author

**Serhii Demediuk**
National Security and Defense Council of Ukraine, Kyiv, Ukraine
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
E-mail: cyberdemediuk@protonmail.com

**Yaroslav Likhovitskyy**
Uzhhorod National University, Uzhhorod, Ukraine
E-mail: lihovickiy.jo@gmail.com

**Yuriy Kardashevskyy**
National Agency for the Prevention of Corruption, Kyiv; Ukraine
E-mail: lvivtin@gmail.com

**Olena Mitina**
Odesa National Polytechnic University, Odesa, Ukraine
E-mail: olenamitina@ukr.net

Received: 22 June 2024; Revised: 17 October 2024; Accepted: 25 January 2025; Published: 08 April 2025

**Abstract:** The study is devoted to assessing the risks of cyber threats in the future based on expert sampling patterns. One of the key problems of modern cybersecurity is the dynamic nature of threats that change under the influence of technological progress and socio-economic factors. In this context, the authors consider a methodological approach that involves the use of a multi-level analysis of expert opinions. The main emphasis is placed on taking into account the different points of view, experience and professional activities of experts from the public, private and academic sectors. An important stage of the study is the procedure of data cleaning to form a representative sample that takes into account only logically consistent responses of experts. The paper focuses on the integration of the expert sample patterns‘ features. The key differences in threat assessments between different groups of experts depending on their professional role and experience are identified. This made it possible to formulate comprehensive recommendations for strategic cyber risk management focused on both short-term and long-term priorities. The study makes a significant contribution to understanding the peculiarities of cyber risk assessment through the use of multivariate analysis of expert opinions. The proposed methodology allows not only to improve the quality of forecasts of future cyber threats, but also contributes to the creation of adaptive cybersecurity strategies that take into account the specifics of each sector. The findings of the study emphasize the importance of a multidimensional approach to analyzing cyber threats, taking into account the specifics of each expert group. Integration of assessments and consideration of local peculiarities are key to the development of adaptive and effective cyber defense strategies focused on global and local challenges.

**Index Terms:** Cybersecurity, Cyber Threats, Risk-oriented Approach, Risk Assessment, Pattern, Expert Sample.

## 1. Introduction

The development of state cybersecurity faces a complex of problems that affect both the effectiveness of the implementation of measures and the ability to form strategies focused on the long-term perspective. The main issues of this process are related to the dynamic nature of threats, which are constantly changing under the influence of technological progress, and the need to take into account various factors that determine national specifics, in particular institutional, organizational and social features [1-3].

Formulating a state's cybersecurity strategy requires setting clear priorities based on an integrated risk assessment that takes into account various aspects of expert opinion. Experts representing different sectors, such as public, private, academic, and civil society, provide a multidimensional analysis of current vulnerabilities and threats. For example, experts representing government agencies may emphasize regulatory support, while private sector representatives may emphasize the importance of responding quickly to new technological threats. Assessing these perspectives helps to identify common ground and formulate a balanced strategy. The professional experience, job category, and area of expertise of the experts also play an important role. At the same time, it is important to integrate approaches that take into account the key patterns of the expert sample to determine the strategy's priorities

Analysis of expert sampling patterns plays a key role in the development of an effective cybersecurity strategy, as it allows for a wide range of perspectives, knowledge and experience to be taken into account for a comprehensive understanding of the situation. This analysis ensures the priorities' identification based on consensus, the identification of regional and sectoral specifics, the balance between theory and practice, the optimization of resources, etc. In particular, experts representing different sectors, positions, and professional backgrounds may provide conflicting risk assessments, but pattern analysis helps to identify common areas that most experts consider critical. And given the industry specifics, pattern analysis allows for differences to be taken into account to develop a more flexible strategy.

Thus, the role of expert sample pattern analysis is to create a systematic approach to risk assessment and prioritization, which makes the cybersecurity strategy not only relevant to current challenges but also flexible to adapt to future threats. This avoids subjectivity and ensures more informed, coherent decisions at the level of public policy.

## 2. Related Works

The study of cybersecurity issues is a contemporary theme that is focused on scientific and technological progress and requires significant potential, active scientific research and research initiative. At the same time, the subject area of scientific research is extremely broad. Some works have focused on assessing the reliability of various modern types of communication technology [4], and various models for ensuring the security of the cloud environment are considered [5]. Attention is focused on methods of localizing anomalies and threats in networks, methods of analyzing network traffic [6-8]. The problem also concerns the detection, analysis, and classification of software vulnerabilities [9-10], as well as the use of various forecasting methods based on the construction of appropriate models [11-17].

An important place is occupied by works that focus on the development of a state cybersecurity strategy, in particular: cybersecurity strategies of developed countries are studied, emphasizing the principles of critical infrastructure protection, the importance of international cooperation based on partnership, and focus on proactive actions [18-20]; cybersecurity is revealed as a key part of strategic planning, in particular in the context of the "cybersecurity economy", emphasizing the need to create a national cybersecurity system, analyzes the best practices for creating cybersecurity strategies and notes the need for appropriate audit, and proposes a framework for developing a national cybersecurity strategy with a discussion of the advantages and disadvantages of such strategies [21-24].

A number of scientific publications focus on identifying cybersecurity priorities, taking into account the peculiarities of expert sampling patterns, in particular the use of formal models for analyzing cyber threats, taking into account expert opinion in the process of modeling attack patterns, identifying key components of cyberspace security, studying behavioral patterns, taking into account national characteristics [18, 25-27]; the use of a targeted survey to study cybersecurity strategy and analyze decisions on cybersecurity investments [28-29]; analysis of the critical infrastructure protection strategy based on qualitative research using expert sampling and visualization of patterns of expert assessments [30-31]; studying the logic of risks and threats in the strategic development of EU cybersecurity, taking into account interstate tensions [32]; analysis of the dynamics of High-Tech Areas [33].

A significant body of scientific research focuses on risk assessment in the field of cybersecurity as a methodological basis for forming a strategic vision of experts and determining development priorities, in particular: the use of a game-theoretic model for assessing uncertainties in cybersecurity investments and risk management [34] and a multi-criteria methodology [35], comparative analysis based on average and fuzzy set theory [36], and quantitative assessment of cyber risks based on data from the IT infrastructure security center [37]; study of methodologies for assessing cybersecurity risks in the banking sector with a focus on development in the digital era [38] and a conceptual model for assessing cybersecurity risks used to improve decision-making [39]; describing approaches to cyber risk assessment in critical infrastructure social networks with a focus on cognitive modeling [40], a decision support methodology for optimizing cybersecurity investments in small businesses [41], and a methodology for automatically verifying cyber risk assessments based on security standards [42]; and presenting approaches to cyber risk assessment using reliability engineering and risk theory [43] and a system for assessing the risks of critical infrastructure

information systems with a focus on the human factor [44].

## 3. Proposed Methods and Results

The stages in this research flow shown in Fig. 1


Fig.1. Research flow

### *3.1. UA Data Collection*

The data collection is based on the method of expert survey, taking into account the professional experience of respondents and professional awareness of the survey subject [45]. It is envisaged to allocate expert groups according to various professional characteristics. The questionnaire was filled out online in confidentiality and anonymity, which ensured the participation of a large number of experts and the optimal determination of their opinions on the proposed indicators and rating scale. To ensure the risk assessment, each indicator was evaluated by two characteristics: "Likelihood" and "Consequences".

For further analysis, we have selected only 9 indicators from the total array of threats assessed by experts. At the same time, the selected group of indicators is characterized by a certain relationship as future threats in the field of cybersecurity (see Table 1).

Table 1. Proposed indicators and scales for their evaluation

| № | Intentional cyber threats (*future trend)* | Likelyhood | | | Consequences | | | |
|---|---|---|---|---|---|---|---|---|
| | | high | medium | low | catastrophe | critical condition | serious condition | minor consequences |
| 1. | supply chain compromise of software dependencies (*increased integration of components and services combined into new products)* | | | | | | | |
| 2. | advanced disinformation / influence operations (IO) campaigns | | | | | | | |
| 3. | rise of digital surveillance authoritarianism / loss of privacy (*facial recognition in the public sphere, increased digital surveillance on Internet platforms or the introduction of digital identity, individual freedoms may be restricted for the sake of safety and security)* | | | | | | | |
| 4. | human error and exploited legacy systems within cyber-physical ecosystems *(rapid adoption of IoT and constant skills shortage)* | | | | | | | |
| 5. | targeted attacks (e.g. ransomware) enhanced by smart device data | | | | | | | |
| 6. | rise of advanced hybrid threats (*using a simultaneous combination of methods to gain initial access, including collecting big data to tailor their phishing campaigns, using machine learning to interpret data, developing new tools to bypass defenses, and combining the physical and virtual to carry out attacks)* | | | | | | | |
| 7. | skill shortages (*attackers analyze organizational skills and weaknesses to gain insight into security weaknesses, potential vulnerabilities, and opportunities to exploit their systems and networks*) | | | | | | | |
| 8. | cross-border ICT service providers as a single point of failure (*ICT service providers and their infrastructure, including satellite technologies, are the backbone of society and therefore can be targeted by terrorists and criminal group)* | | | | | | | |
| 9. | abuse of AI (*AI can be used to enhance many dishonest actions, such as creating disinformation and fake content, using prejudice, collecting biometric and other sensitive data, creating military robots, data poisoning, etc.)* | | | | | | | |

We also propose to separate the sample by certain characteristics that characterize experts and the likely difference in their perception of the problem, in particular: region, position, industry, experience, and education.

At the same time, the full statistical characterization of the expert community by groups of the expert sample is extremely sensitive information for Ukraine's cybersecurity, so it can only be partially made publicly available. However, these limitations do not significantly affect the results of the study, as the data obtained and used broadly and diversely identify expert groups and form sufficient prerequisites for using expert sampling patterns in analyzing and interpreting statistical findings and assessing future cyber threats.

### *3.2. Data Cleaning*

Data cleaning involves the formation of a reliable sample based on the application of appropriate filters. The sample limitation contains an appropriate statistical justification based on qualitative selection. Given the complexity of evaluating indicators on a dual scale, their comprehension in a short time, and the corresponding tension, it is possible to assume that respondents' attention spans are unstable and that they may make mistakes in their answers [46]. Some incompetence of respondents, lack of motivation to provide thoughtful answers, and inattention in answering are also possible. The use of appropriate sampling restriction filters ensures that the data of those experts who provided logically consistent answers are taken into account.

In order to check respondents for logical errors and limit the sample to the highest quality and most reliable data, the questionnaire included questions with a logically predictable answer. In particular, when assessed by the "probability" characteristic, the question "*Territory of origin of cyberattacks: russian federation*" cannot reasonably be assessed as "low" at the expert level in the context of war, etc.

This expert sample ensured the formation of a basic set of data obtained from only those experts who provided logically consistent answers [47]. And although 42.01% of the original sample remained after applying the appropriate filters, the quality of the data has improved significantly. In particular, when assessing the threat of "*Rise of advanced hybrid threats*", the difference in the distribution of reliable and unreliable sample groups is significant (see Table 2).

Table 2. Analysis by logic error filter

| INDICATOR | Likelyhood | Sample | | Pearson Chi-Square | Cramer's V |
|---|---|---|---|---|---|
| | | Unreliable part | Reliable part | | |
| 6. Rise of advanced hybrid threats | *low* | 10.2% | 6.7% | 13.940<br>0,001 | .152<br>0,001 |
| | *medium* | 46.7% | 34.5% | | |
| | *high* | 43.1% | 58.7% | | |

Thus, the results of the expert assessment of the threat "*Rise of advanced hybrid threats*" differ significantly: 43.1% of unreliable experts indicated a high probability of this threat, while the reliable part emphasized it more - 58.7% of cases. At the same time, with regard to the low level of assessment, given the reliability of the data, the redistribution of expert opinion shifted downward - from 10.2% to 6.7% This difference in distribution is statistically significant ($\chi^2 = 13.940$, $p < 0.001$) with a significant effect size (Cramer's $V = 0.152$, $p < 0.001$).

The application of this approach allowed us to:

- Improve the quality of the sample: after excluding 57.99% of unreliable data, a representative sample was provided that more accurately reflects expert opinion. This is evidenced by statistically significant differences in the distribution of risk assessments for "Rise of advanced hybrid threats."
- Minimize distortions: the exclusion of illogical answers reduced the share of erroneous assessments, for example, regarding the low probability of cyber threats from the russian federation.
- Increase the reliability of the results: the $\chi^2$ value of 13.940 and the Cramer's V effect value of 0.152 indicate significant differences between the unreliable and cleaned samples, which emphasizes the effectiveness of the applied filters.

Therefore, the data cleansing methodology is effective and relevant for assessing cyber threats, as it eliminates distortions and improves the quality of statistical analysis. Scientific approaches [46] confirm the rationality of the applied filters, emphasizing the need for logical control and respondent competence. The use of this methodology should become a mandatory element of data collection and analysis in studies where the accuracy of expert opinions is critical.

### *3.3. Risk Assessment*

We used the international standard ISO 31000 as the methodological basis for risk assessment [48]. At the same time, while working in various risk-oriented projects, the implementation of this standard has gained some practical research refinement and interpretation [45, 49-50]. Further analysis focuses on determining the level of risk of the spread of future cyber threats.

Thus, based on the risk assessment, the rating of future cyber threats is determined by the average value (Fig. 2).

For visual perception, we traditionally use four colors to indicate the level of risk]:

- red level - level of risk in the zone above 60% (the most significant threats);
- orange level - level of risk in the area of 50 - 60% (significant threats);
- yellow level - level of risk in the area of 40 - 50% (threats that need attention, but not paramount);
- green level - risk level in the area below 40%.

Thus, based on the average risk level, we can note that the highest risk in the future is characterized by “abuse of AI” (60.18%) and “rise of advanced hybrid threats” (59.62%).

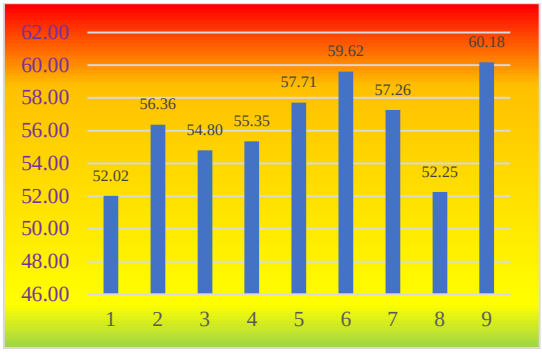


Fig.2. Rating of future cyber threats

At the same time, we have repeatedly noted in previous studies [45, 49-50] the need to clarify the level of risk and a more flexible approach to its analysis. It is particularly critical to study future cyber threats, taking into account the diversity of expert opinion, which is based on a certain probability and subjectivity of judgment and may reveal differences in the perception of risks and prioritization in the future.

### *3.4. Pattern Analysis*

Subsequently, the expert patterns formed on the basis of the sample by job category, professional experience, and area of professional activity are studied.

Assessing the risks of future cyber threats by job category allows for a variety of perspectives that contribute to a balanced and effective approach to cyber defense. Different expert groups, such as executives, specialists, detectives, analysts, and scientists, assess risks based on the specifics of their work. Each group has specific knowledge and experience that influences their risk assessment, differences in threat perception between groups can identify gaps in understanding or shortcomings in the cybersecurity organization, and the integration of the results of different groups helps to form a comprehensive approach to cybersecurity. This creates a unique opportunity to analyze differences in threat perception and identify strengths and weaknesses in the overall security strategy (see Table 3).

Table 3. Risk level in the sample by position category

| | **%** | **Position category** | | | | |
|---|---|---|---|---|---|---|
| **Cyber threats (future trend)** | **Average** | principal | specialist | detective | analytic | scholar |
| 1.Supply chain compromise of software dependencies | 52,02 | 53,73 | 52,46 | 55,16 | 44,36 | 56,14 |
| 2.Advanced disinformation / influence operations (IO) campaigns | 56,36 | 52,95 | 57,78 | 60,53 | 45,86 | 54,39 |
| 3.Rise of digital surveillance authoritarianism / loss of privacy | 54,80 | 50,51 | 58,47 | 42,11 | 44,36 | 57,89 |
| 4.Human error and exploited legacy systems within cyber-physical ecosystems | 55,35 | 56,87 | 51,71 | 68,42 | 63,16 | 60,53 |
| 5.Targeted attacks (e.g. ransomware) enhanced by smart device data | 57,71 | 57,19 | 58,24 | 71,05 | 63,16 | 57,89 |
| 6.Rise of advanced hybrid threats | 59,62 | 59,54 | 58,76 | 78,95 | 67,67 | 61,40 |
| 7.Skill shortages | 57,26 | 58,60 | 54,83 | 68,42 | 73,68 | 68,42 |
| 8.Cross-border ICT service providers as a single point of failure | 52,25 | 51,61 | 51,24 | 42,11 | 60,15 | 55,26 |
| 9.Abuse of AI | 60,18 | 56,25 | 60,50 | 57,89 | 65,41 | 66,67 |

Regarding the cyber threat associated with compromising the software supply chain, analysts (55.16%) and scientists (56.14%) indicated risks at a level above the average (52.02%). This indicates that these groups have a deeper appreciation of the potential vulnerabilities of supply chains. At the same time, executives (53.73%) and professionals (52.46%) perceive this threat at an average level, probably due to their focus on operational aspects. That is, there is a certain lack of perception of strategic risks related to supply or logistics. At the same time, it is scientists who do not limit their activities to operational issues who indicate the highest level of risk (56.14%). That is why emphasis on the importance of ensuring the integrity of program components and partnerships should be considered a strategic component to reduce the risk of this threat.

The threat of “Rise of advanced hybrid threats” with an average score of 59.62% also received high marks among all expert groups. Detectives (78.95%) and analysts (67.67%) stand out, indicating the operational danger of such threats and their impact on overall security systems. Scientists (61.40%) also maintain a high level of attention,

emphasizing the multi-component nature of these attacks. The strategic perception of the problem indicates the need to pay attention to multicomponent attacks that simultaneously include technical, informational and social aspects.

Another example is the threat of “Human error and exploited legacy systems”, which ranks third and is not the average (55.35%). This pattern confirms the attention of the task forces to the shortcomings in current systems. Detectives (68.42%) and analysts (63.16%) identify this risk as one of the most important, which is significantly higher than the average (55.35%). This can be explained by their direct work with real-life cases of errors and outdated systems, and also emphasizes that weaknesses in the human factor and outdated technologies are one of the most vulnerable aspects of modern cyber infrastructure. At the same time, experts (51.71%) assess this risk as below average, which may indicate that they focus on specific technical aspects of protection while underestimating the role of user error or outdated systems. A strategic component going forward is the importance of investing in system upgrades and staff training to mitigate risks.

Targeted attacks (e.g., ransomware) enhanced by smart device data have an average risk value of 57.71%. However, detectives (71.05%) and analysts (63.16%) point to the exceptional danger of this threat. Its high score indicates serious risks associated with the active use of personal data from smart devices, which makes these attacks more targeted and difficult to prevent.

The AI Abuse threat also shows a difference in perception. Scientists (66.67%) and analysts (65.41%) gave the highest scores, which is higher than the average (60.18%). This indicates their tendency to pay attention to long-term consequences and strategic risks, including the possibility of autonomous threats that are difficult to predict. Instead, managers (56.25%), detectives (57.89%) and specialists (60.50%) assess this threat as closer to average or lower, which may be due to the lack of operational focus on this issue. The strategic perception of the problem points to the need to control and monitor the development and use of AI, especially in the face of the growing complexity of autonomous threats.

Although this threat, “Skill shortages,” has an average rating of 57.26%, analysts (73.68%) and scientists (68.42%) point to it as one of the most critical. The high level of concern indicates that the lack of qualified specialists exacerbates the impact of other cyber threats. That is why the strategy should include measures to develop cybersecurity education and attract specialists.

A comparative analysis of the “Rise of digital surveillance authoritarianism / loss of privacy” is also important. Scientists (57.89%) assess this risk as above average (54.80%), focusing on privacy concerns. Detectives (42.11%), on the other hand, indicate a lower than average risk, possibly due to a greater focus on operational issues. This indicates that privacy aspects are not always a priority in the immediate work, although their importance in the long run should not be underestimated.

In general, risk assessment by different expert groups shows that managers tend to underestimate the level of risks, focusing on resource management, while scientists give the highest ratings to the latest threats. Analysts are characterized by a balance in their assessments, matching risks with realistic response capabilities, while detectives overestimate operational threats. Such differences between the groups and the averages emphasize the need to take into account the opinions of all categories to ensure a comprehensive analysis.

Thus, according to the expert's opinion, cyber threats related to innovative technologies (misuse of artificial intelligence), sophisticated hybrid attacks, and human error have the highest risk rating in the future. This pattern indicates certain features:

- groups' focus on specific risks: executives focus on resource management and tend to underestimate emerging threats, such as “Abuse of AI” (56.25%) and “Rise of advanced hybrid threats” (59.54%), while specialists often focus on technical aspects, underestimating the broader context, such as risks associated with human error or loss of privacy.
- low attention to strategic long-term threats: risks related to digital authoritarianism and privacy received less emphasis among operational groups (detectives and analysts). This indicates a focus on short-term threats and a lack of a strategic approach.

Such differences once again confirm the importance of integrating the assessments of all groups to create a balanced cybersecurity strategy.

To develop an effective cybersecurity strategy, it is necessary to

- focus more on underestimated threats such as human error, supply chain compromise, and loss of privacy.
- increase the integration of assessments from different expert groups to ensure the completeness of the analysis.
- take into account strategic threats that may not be operationally relevant but will affect the long-term resilience of cyber infrastructure.

These actions will help to create a balanced strategy that takes into account both short-term and long-term aspects of threats.

Equally important is the analysis based on the expert sample by professional experience (see Table 4). It is likely that younger experts (up to 1 year) often underestimate risks and follow popular trends in cybersecurity, while more

experienced ones assess them much higher. Conversely, groups with less experience can better spot new threats and point out trends that experienced experts have not noticed. In other words, experienced experts are more cautious about new threats, which can lead to underestimation of innovation risks. Due to the diversity of perspectives, groups with different experience can notice different aspects of threats and identify weaknesses. At the same time, in risk management, the experienced experts' views are more practical for developing protection strategies and focus on real-world consequences, especially since data from experts with extensive experience is often based on a broader context, which reduces error.

Table 4. Risk level in the sample based on professional experience

| | **Average** | **Experience** | | | | |
|---|---|---|---|---|---|---|
| **Cyber threats (future trend)** | **%** | up to 1 year | 1-3 years | 3-10 years | 10-20 years | over 20 years |
| 1.Supply chain compromise of software dependencies | 52,02 | 44,99 | 47,10 | 52,81 | 60,03 | 67,84 |
| 2.Advanced disinformation / influence operations (IO) campaigns | 56,36 | 60,10 | 55,49 | 56,75 | 55,19 | 50,29 |
| 3.Rise of digital surveillance authoritarianism / loss of privacy | 54,80 | 56,37 | 56,47 | 52,27 | 57,33 | 52,63 |
| 4.Human error and exploited legacy systems within cyber-physical ecosystems | 55,35 | 51,78 | 57,63 | 55,47 | 55,05 | 52,63 |
| 5.Targeted attacks (e.g. ransomware) enhanced by smart device data | 57,71 | 59,93 | 59,95 | 56,44 | 56,47 | 52,63 |
| 6.Rise of advanced hybrid threats | 59,62 | 56,88 | 60,66 | 57,35 | 64,58 | 63,74 |
| 7.Skill shortages | 57,26 | 56,03 | 59,68 | 56,08 | 57,33 | 56,73 |
| 8.Cross-border ICT service providers as a single point of failure | 52,25 | 53,65 | 55,58 | 51,60 | 51,07 | 36,84 |
| 9.Abuse of AI | 60,18 | 63,33 | 62,36 | 58,50 | 59,32 | 54,97 |

Thus, the analysis of the cyber threats' risks also shows significant differences in assessments between groups of experts with different levels of experience. Taking these differences into account allows us to gain a deeper understanding of threats and develop effective countermeasures.

"Supply chain compromise of software dependencies" has an average risk level of 52.02%. At the same time, the group with the least experience (up to 1 year) estimated this threat at 44.99%, which is significantly lower than average. On the other hand, experts with more than 20 years of experience estimated the risk at 67.84%, which indicates their awareness of the complexity and vulnerability of modern IT ecosystems. This also points to the need for increased attention to the security of complex IT ecosystems, which can be easily vulnerable to supply chain attacks.

The Abuse of AI threat received an average rating of 60.18%. The highest risk ratings (63.33% and 62.36%, respectively) were given by groups with up to 1 year of experience and 1-3 years of experience, which may be due to their awareness of current trends in the development of artificial intelligence. More experienced experts (more than 20 years of experience) assessed the risk at the lowest level - 54.97%, which may reflect their rational approach and consideration of the limitations of the technology, but may also indicate gaps in the consideration of new threats. An integrated strategic solution should still focus on the need for more flexible regulation of the use of artificial intelligence.

Hybrid threats showed the largest deviation between the average level of risk (59.62%) and the estimates of the group with 10-20 years of experience (64.58%). This indicates the high relevance of this threat for experts who have considerable practical experience but have not yet lost their sensitivity to new challenges. Such threats combine cyber, physical, and information components, which require a multidisciplinary approach to addressing them.

In the case of the human factor, the average risk level was 55.35%. The group with 3-10 years of experience rated this risk the highest (57.63%), which is likely due to their practical experience with cyber-physical systems. Younger experts and the group with 20 years of experience showed lower estimates (51.78% and 52.63%, respectively). This may indicate an underestimation of the risks associated with the influence of the human factor on the security of cyber-physical systems, and therefore a logical requirement is to focus strategic efforts on personnel training and system modernization

"Advanced disinformation/influence operations (IO) campaigns" is estimated to be a 56.36% risk in the future. The younger group (under 1 year old) rated this threat the highest (60.10%), which indicates their sensitivity to the problem of information warfare. This area is particularly relevant given the current geopolitical challenges. Instead, more experienced groups demonstrated a downward trend in their assessments.

The comparative analysis demonstrates the importance of integrating the views of both young and experienced experts. Younger experts often notice new threats, while experienced ones focus on real consequences and practical solutions.

To complement the analysis, it is worth highlighting the threats and aspects that received less emphasis in the risk assessment based on the patterns of the expert sample, and to identify possible gaps in priorities and take them into account in the development of a cybersecurity strategy. For example, cross-border ICT service providers as a single point of failure have the lowest risk rating among experts with over 20 years of experience (36.84%). This may indicate that experienced experts are confident in regulatory and technical protection mechanisms, but underestimating this aspect may create gaps in the face of growing dependence on global services. Rise of digital surveillance

authoritarianism / loss of privacy - this threat was rated below average by experts with over 20 years of experience (52.63%), which may indicate a limited focus on this problem among older generations of experts.

At the same time, this aspect is becoming increasingly relevant in the context of the global rise of authoritarian practices. Advanced disinformation campaigns - experts with more than 20 years of experience rated this threat at 50.29%, which is lower than the average (56.36%). This may indicate an underestimation of the significance of this threat by senior experts, especially in the context of information wars.

Summarizing the analysis by expert experience pattern, it is important to highlight the following features:

- *underestimation of new technological risks by senior experts* – experienced experts often demonstrate an underestimation of risks associated with new technologies, for example, "AI abuse" (54.97%) and "Supply chain compromise" (67.84%). This may be due to a cautious and rational approach, but it may also indicate gaps in the consideration of new threats;
- *lack of balance in risk assessment between groups* – the patterns show significant differences between younger experts who tend to overestimate certain threats (e.g., "Advanced disinformation") and older experts who may underestimate their significance. This requires the integration of different perspectives to formulate a balanced strategy;
- *limited emphasis on long-term social consequences* – risks associated with loss of privacy and authoritarian practices receive lower scores from older groups, which may indicate a lack of attention to the socio-political aspects of cyber threats.

When developing a cybersecurity strategy, it is important to consider these smaller emphases to ensure that the threat assessment is complete. In particular, you should

- increase attention to the risks of cross-border IT services, disinformation campaigns, and human factors;
- integrate the perspectives of young and experienced experts to achieve a balance in the threat assessment;
- increase the emphasis on the social and political consequences of cyber threats that may have a long-term impact.

These adjustments will contribute to a flexible and comprehensive cybersecurity strategy.

Analyzing the risks of cyber threats taking into account industry-specific features is also important, as it allows identifying vulnerabilities and priorities for different industries. Based on the data (see Table 5), each cyber threat has a specific impact depending on the type of industry: public administration, energy sector, telecommunications services, and digital services. For example:

- public administration faces a high risk of threats such as misuse of artificial intelligence (62.73%) and hybrid threats (61.55%);
- the energy sector stands out for the highest risk of hybrid threats (67.94%) and skills shortages (66.03%);
- telecommunication services are highly susceptible to artificial intelligence abuse (59.24%);
- digital services are characterized by a high risk of privacy loss due to authoritarian surveillance (59.21%) and a lack of skills (59.59%).

Using the average risk value helps to assess general trends, but to make effective strategic decisions, it is necessary to take into account the details specific to each industry.

Experts in the energy sector identify hybrid threats as the most critical (67.94%), which requires the introduction of innovative protection technologies and the development of scenarios for responding to complex attacks. And the skills shortage (66.03%) indicates the need to train highly qualified personnel to work with critical infrastructure.

The highest risk for the digital services sector is the loss of privacy due to authoritarian surveillance (59.21%). It is critical for this sector to implement transparent data processing policies, new encryption methods, and security certification. And the skills shortage (59.59%) indicates the need to expand educational programs in the field of digital technologies. At the same time, the risk of "*Cross-border ICT service providers as a single point of failure*" has the lowest score (47.18%), which indicates that the sector is focused on local threats and underestimates global risks.

The pattern of expert sampling by the public administration filter focuses on the misuse of artificial intelligence (62.73%), which requires the introduction of ethical standards and technologies to counteract manipulative attacks. At the same time, the risk of privacy loss in public administration (56.50%) is rated lower compared to digital services, indicating less attention to privacy issues in the sector. However, this aspect may be critical in the long run. It is also worth noting that in public administration, the human factor and outdated systems are characterized by the lowest risk (51.45%), which indicates a potential underestimation of problems related to human error.

In turn, experts in the telecommunications services sector point to vulnerability to artificial intelligence abuse (59.24%), which indicates the need to ensure data security in telecommunications networks. At the same time, the priority is to protect software supply chains (50.05%), as compromise can lead to large-scale consequences.

Summarizing the peculiarities of assessing the risks of future cyber threats, we can confidently recommend that cybersecurity strategies should be developed by sectoral strategies, creating individual approaches to cyber defense,

taking into account the most critical threats. The energy sector should focus on hybrid attacks and human resources, public administration on controlling artificial intelligence, and digital services on data protection. Cross-sectoral cooperation is also an important focus - joint initiatives between sectors will facilitate the exchange of experience and technologies to improve cybersecurity. It is also important to take into account international practices, especially for sectors focused on global markets, such as digital and telecommunications services.

Table 5. Risk level in the sample by field of professional activity

| | | Sector | | | |
|---|---|---|---|---|---|
| **Cyber threats (future trend)** | **Average, %** | Public administration | Energy sector | Telecommunication services | Digital services |
| 1.Supply chain compromise of software dependencies | 52,02 | 54,46 | 57,42 | 50,05 | 53,95 |
| 2.Advanced disinformation / influence operations (IO) campaigns | 56,36 | 57,36 | 50,72 | 57,17 | 54,70 |
| 3.Rise of digital surveillance authoritarianism / loss of privacy | 54,80 | 56,50 | 48,80 | 53,35 | 59,21 |
| 4.Human error and exploited legacy systems within cyber-physical ecosystems | 55,35 | 51,45 | 54,55 | 54,59 | 58,65 |
| 5.Targeted attacks (e.g. ransomware) enhanced by smart device data | 57,71 | 56,28 | 59,33 | 57,28 | 54,32 |
| 6.Rise of advanced hybrid threats | 59,62 | 61,55 | 67,94 | 53,46 | 57,33 |
| 7.Skill shortages | 57,26 | 56,93 | 66,03 | 56,35 | 59,59 |
| 8.Cross-border ICT service providers as a single point of failure | 52,25 | 51,88 | 60,77 | 51,08 | 47,18 |
| 9.Abuse of AI | 60,18 | 62,73 | 57,89 | 59,24 | 52,26 |

All industries need to integrate cross-sector initiatives. Sharing resources, joint research on cyber threats, and information exchange between experts from different sectors can significantly increase risk resilience. In addition, the creation of international cybersecurity alliances can be crucial in countering global threats such as artificial intelligence misuse or hybrid attacks.

To successfully respond to cyber threats, each industry must develop its own set of priorities that takes into account both the specifics of the risks and the potential for cooperation with other sectors. The development of adaptive cyber defense strategies, training, and the introduction of innovative technologies can significantly reduce the level of risks. Only through harmonious interaction between public administration, critical industries and the private sector can a high level of cybersecurity be achieved in the future.

Thus, using the opinions of expert groups to analyze the risks of future cyber threats has significant advantages. This allows for industry specifics, threat relevance, cross-sectoral interaction, and identification of hidden risks. The expert groups provide a multidimensional approach to analysis, with each industry focusing on key aspects: energy - on hybrid attacks, digital services - on privacy, telecommunications - on supply chains, and public administration - on manipulative threats. This allows for more resilient and adaptive cybersecurity strategies.

These findings will help to shape a more adaptive and resilient cybersecurity strategy that takes into account both industry specifics and system-wide needs.

## 4. Conclusions

The analysis of the patterns of expert sampling and cyber threat risk assessment demonstrates the need for a comprehensive approach to the development of Ukraine's cybersecurity strategy. The dynamic nature of modern cyber threats requires the integration of different expert opinions, as their positions differ significantly depending on their professional experience, position, and industry specifics. Such an analysis allows for a balanced and flexible strategy that will meet both short-term challenges and long-term threats.

Based on the analysis, it was found that the strategic challenges in the field of cybersecurity in Ukraine are as follows:

- *Technological threats.* The greatest threat is the abuse of artificial intelligence and sophisticated hybrid attacks. The importance of these threats is growing against the backdrop of the active use of smart devices and autonomous systems, which creates risks of uncontrolled spread of threats.
- *Shortage of personnel*. The shortage of qualified specialists is critical. Younger experts focus on emerging risks, while more experienced ones focus on practical aspects. The lack of a balanced personnel approach makes it difficult to counter cyber threats.
- *Social aspects of cyber threats*. Risks of privacy loss and digital authoritarianism are less of a priority among operational experts, which may lead to an underestimation of their long-term impact.
- *Sectoral challenges*. Each industry has its own critical cyber threats. The energy sector faces hybrid attacks, while digital services suffer from staff shortages and the risk of privacy loss.

- Hence, taking into account the analysis of expert sampling patterns, risk assessment, and the conclusions drawn in the study, the following key recommendations can be made:
- *Integration of different expert groups*. Establish expert councils for continuous monitoring of cyber threats, including representatives of the public, private sectors, academia, and civil society. This will ensure a comprehensive approach to risk analysis and rapid response to threats.
- *Develop sectoral strategies.* Introduce individual cyber defense strategies for each critical industry. For the energy sector, focus on hybrid attacks and human resources, for digital services – privacy protection and human resources programs, for the telecommunications sector – protection of software supply chains.
- *Human resources policy*. Introduce educational programs and grant initiatives to train cybersecurity professionals. Provide professional training for civil servants and private sector professionals.
- *Control of artificial intelligence technologies*. Create regulatory mechanisms to monitor and control the development of artificial intelligence. Develop ethical standards for the use of AI for possible future implementation to reduce the risks of manipulation and autonomous threats.
- *Improving international cooperation*. Expand Ukraine's participation in international cybersecurity alliances. Ensure the exchange of information on cyber threats and best practices between partner countries.
- *Social and legal aspects*. Take into account the long-term consequences of cyber threats for society. Implement transparent data protection policies and mechanisms for monitoring authoritarian practices.

The proposed measures will contribute to the creation of a sustainable, flexible and adaptive cybersecurity strategy for Ukraine. Integration of expert assessments will increase the state's readiness to counter current and future cyber threats.

## References


[1] Foresight Challenges (2021). A study to enable foresight on emerging and future cybersecurity challenges. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Foresight%20Challenges.pdf

[2] ENISA (2022). Identifying Emerging Cyber Security Threats and Challenges for 2030. URL: https://www.enisa.europa.eu

[3] Demediuk, S.V. (2024). Rozdil 26. Kiberviina ta forsait kiberstiikosti. V monohafii «Realizatsiia filosofii ILP v systemi kryminalnoho analizu Natsionalnoi politsii Ukrainy», 343-357. DOI: 10.36486/978-966-2310-66-5-26

[4] Biyue Diao, Guoping Chen, Feng He, " Loudspeaker Operation Status Monitoring System based on Power Line Communication Technology", International Journal of Image, Graphics and Signal Processing, Vol.10, No.10, pp. 54-62, 2018.

[5] Orkhan Aslanli, "Cloud and On-premises Based Security Solution for Industrial IoT", International Journal of Information Engineering and Electronic Business, Vol.16, No.5, pp. 55-62, 2024.

[6] Abhinandan H., Patil, Neena, Goveas, & Krishnan, Rangarajan (2016). Regression Test Suite Prioritization using Residual Test Coverage Algorithm and Statistical Techniques, International Journal of Education and Management Engineering, 6 (5), 32-39.

[7] Adeyinka, F., Oluyemi, E.S., Victor, A.N., Uchenna, U.C., Ogedengbe, O., & Ale, S. (2017). Parametric Equation for Capturing Dynamics of Cyber Attack Malware Transmission with Mitigation on Computer Network. International Journal of Mathematical Sciences and Computing, 3 (4), 37-51.

[8] Ghaderipour, Y. & Dinari, H. (2020). A Flow-Based Technique to Detect Network Intrusions Using Support Vector Regression (SVR) over Some Distinguished Graph Features. International Journal of Mathematical Sciences and Computing, 6 (4), 1-11.

[9] Hakan, Kekül, Burhan, Ergen & Halil Arslan (2022). Estimating Missing Security Vectors in NVD Database Security Reports. International Journal of Engineering and Manufacturing, 12 (3), 1-13.

[10] Hakan, Kekül, Burhan, Ergen, & Halil, Arslan (2021). A New Vulnerability Reporting Framework for Software Vulnerability Databases. International Journal of Education and Management Engineering, 11 (3), 11-19.

[11] Kasliono, Suprapto, & Faizal, Makhrus (2021). Point Based Forecasting Model of Vehicle Queue with Extreme Learning Machine Method and Correlation Analysis. International Journal of Intelligent Systems and Applications, 13 (3), 11-22.

[12] Anbarasa A., Pandian, & Balasubramanian, R. (2016). Analysis on Shape Image Retrieval Using DNN and ELM Classifiers for MRI Brain Tumor Images. International Journal of Information Engineering and Electronic Business, 8 (4), 63-72.

[13] Yudianto, Muhammad Resa Arif, Agustin, Tinuk, James, Ronaldus Morgan, Rahma, Firstyani Imannisa, Rahim, Arham, & Utami, Ema (2021). Rainfall Forecasting to Recommend Crops Varieties Using Moving Average and Naive Bayes Methods. International Journal of Modern Education and Computer Science, 13 (3), 23-33.

[14] Lytvynenko, Volodymyr, Kryvoruchko, Olena, Lurie, Irina, Savina, Nataliia, Naumov, Oleksandr, & Voronenko, Mariia (2020). Comparative Studies of Self-organizing Algorithms for Forecasting Economic Parameters. International Journal of Modern Education and Computer Science, 12 (6), 1-15.

[15] Zulkifley, Nor Hamizah, Rahman, Shuzlina Abdul, Ubaidullah, Nor Hasbiah, & Ibrahim, Ismail (2020). House Price Prediction using a Machine Learning Model: A Survey of Literature. International Journal of Modern Education and Computer Science, 12 (60), 46-54.

[16] Yudianto, Muhammad Resa Arif, Agustin, Tinuk, James, Ronaldus Morgan, Rahma, Firstyani Imannisa, Rahim, Arham, & Utami, Ema (2021). Rainfall Forecasting to Recommend Crops Varieties Using Moving Average and Naive Bayes Methods. International Journal of Modern Education and Computer Science, 13 (3), 23-33.

[17] Babatunde, Gbadamosi, Emmanuel, Adeniyi Abidemi, Oluwaseun, Ogundokun Roseline, Bunmi, Oladosu Bukola, & Precious, Anyaiwe Ehiedu (2019). Impact of Climatic Change on Agricultural Product Yield Using K-Means and Multiple Linear Regressions. International Journal of Education and Management Engineering, 9 (3), 16-26.

[18] Tanriverdiyev, E. (2022). THE STATE OF THE CYBER ENVIRONMENT AND NATIONAL CYBERSECURITY STRATEGY IN DEVELOPED COUNTRIES. National Security Studies. https://doi.org/10.37055/sbn/149510.

[19] Carroll, J. (2024). The U.S. National Cybersecurity Strategy: A Vehicle with an International Journey. European Conference on Cyber Warfare and Security. https://doi.org/10.34190/eccws.23.1.2300.
[20] Ukhanova, E. (2022). Cybersecurity and cyber defence strategies of Japan. SHS Web of Conferences. https://doi.org/10.1051/shsconf/202213400159.
[21] Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). CYBERSECURITY AS A COMPONENT OF THE NATIONAL SECURITY OF THE STATE. Journal of Security and Sustainability Issues. https://doi.org/10.9770/jssi.2020.9.3(4).
[22] Gunawan, B., Ratmono, B., & Abdullah, A. (2023). Cybersecurity and Strategic Management. Foresight and STI Governance. https://doi.org/10.17323/2500-2597.2023.3.88.97.
[23] Gercke, M. (2013). Cybersecurity Strategy. 14, 136 - 142. https://doi.org/10.9785/ovs-cri-2013-136.
[24] (2021). National Cybersecurity Strategies. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM. https://doi.org/10.4018/978-1-7998-4162-3.ch005.
[25] Bland, J., Petty, M., Whitaker, T., Maxwell, K., & Cantrell, W. (2020). Machine Learning Cyberattack and Defense Strategies. Comput. Secur., 92, 101738. https://doi.org/10.1016/j.cose.2020.101738.
[26] Tkach, Y. (2020). CONCEPTUAL MODEL OF CYBER SPACE SECURITY. Technical Sciences and Technologies. https://doi.org/10.25140/2411-5363-2020-4(22)-96-108.
[27] Srivastava, S., & Raj, S. (2024). Cyber Security Assessment and Awareness: A Statistical Modelling Approach. 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), 1-6. https://doi.org/10.1109/KHI-HTC60760.2024.10482035.
[28] Burton, S. (2022). Strategy: A Business and Cybersecurity Intertwined Necessity. Int. J. Smart Educ. Urban Soc., 13, 1-12. https://doi.org/10.4018/ijseus.312232.
[29] Kissoon, T. (2020). Optimum spending on cybersecurity measures. Transforming Government: People, Process and Policy, 14, 417-431. https://doi.org/10.1108/tg-11-2019-0112.
[30] Boutwell, M. (2019). Exploring Industry Cybersecurity Strategy in Protecting Critical Infrastructure.
[31] Bowman, C., & Ambrosini, V. (1997). Perceptions of Strategic Priorities, Consensus and Firm Performance. Journal of Management Studies, 34, 241-258. https://doi.org/10.1111/1467-6486.00050.
[32] Backman, S. (2022). Risk vs. threat-based cybersecurity: the case of the EU. European Security, 32, 85 - 103. https://doi.org/10.1080/09662839.2022.2069464.
[33] Sadykov, S., Utkin, A., & Sokolov, A. (2023). Analysis of the Dynamics of the Development of High-Tech Areas for the Formation of Strategic Priorities of Company Management.Proceedings of the Southwest State University. Series: Economics. Sociology. Management. https://doi.org/10.21869/2223-1552-2023-13-5-36-47.
[34] Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk Assessment Uncertainties in Cybersecurity Investments. Games, 9, 34. DOI: 10.3390/g9020034
[35] Ganin, A., Quach, P., Panwar, M., Collier, Z., Keisler, J., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Analysis, 40. DOI: 10.1111/risa.12891
[36] Korystin, O., Korchenko, O., Kazmirchuk, S., Demediuk, S., Korystin, O. (2024). Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Set Theory. I. J. Computer Network and Information Security, 1, 1-13.
[37] Allodi, L., & Massacci, F. (2017). Security Events and Vulnerability Data for Cybersecurity Risk Estimation. Risk Analysis, 37. DOI: 10.1111/risa.12864
[38] Dawodu, S., Omotosho, A., Akindote, O., Adegbite, A., & Ewuga, S. (2023). Cybersecurity risk assessment in banking: methodologies and best practices. Computer Science & IT Research Journal. DOI: 10.51594/csitrj.v4i3.659
[39] Rea-Guaman, A., Mejía, J., Feliu, S., & Calvo-Manzano, J. (2020). AVARCIBER: a framework for assessing cybersecurity risks. Cluster Computing, 23, 1827-1843. DOI: 10.1007/s10586-019-03034-9
[40] Aktayeva, A., Makatov, Y., Tulegenovna, A., Dautov, A., Niyazova, R., Zhamankarin, M., & Khan, S. (2023). Cybersecurity Risk Assessments within Critical Infrastructure Social Networks. Data, 8, 156. DOI: 10.3390/data8100156
[41] Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber Risk Assessment and Optimization: A Small Business Case Study. IEEE Access, 11, 44467-44481. DOI: 10.1109/ACCESS.2023.3272670
[42] Angelini, M., Bonomi, S., & Palma, A. (2022). A Methodology to Support Automatic Cyber Risk Assessment Review. ArXiv, abs/2207.03269. DOI: 10.48550/arXiv.2207.03269
[43] Meshkat, L., & Miller, R. (2022). A Systems Approach for Cybersecurity Risk Assessment. Annual Reliability and Maintainability Symposium (RAMS), 1-9. DOI: 10.1109/RAMS51457.2022.9893966
[44] Mokhor, V., Honchar, S., & Onyskova, A. (2020). Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects. IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 19-22. DOI: 10.1109/PICST51311.2020.9467957.
[45] Korystin, O.Ye., & Korystin, O.O. (2022). Threats in the sphere of cyber security in Ukraine. Nauka i pravookhoronna, 1, 127–131. DOI: 10.36486/np.2022.1(55)12.
[46] Korystin, Oleksandr, Svyrydiuk, Nataliia, & Vinogradov, Alexander (2021). The Use of Sociological Methods in Criminological Research. Proceedings of the International Conference on Social Science, Psychology and Legal Regulation (SPL 2021). Series: Advances in Social Science, Education and Humanities Research, 617, 18 December, 1-6. DOI: 10.2991/assehr.k.211218.001
[47] Korystin, O.Ie., Demediuk, S.V., Panchenko, Ye.V., Korystin, O.O. (2023). Natsionalni realii analizu kiberzlochynnosti za metodolohiieiu Yevropolu IOSTA. Pivdennoukrainskyi pravnychyi chasopys, 3, 44-46. DOI: 10.32850/sulj.2023.3.10
[48] ISO 31000:2018 - RISK MANAGEMENT. URL: https://www.iso.org/ru/publication/PUB100464.html
[49] Korystin, O., & Svyrydiuk, N. (2020). Methodological principles of risk assessment in law enforcement activity. Nauka i pravooxoronna, 3, 191-197. DOI:10.36486/np.2020349
[50] Korystin, Oleksandr, & Svyrydiuk, Nataliia (2021). Activities of Illegal Weapons Criminal Component of Hybrid Threats. Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021). Series: Advances in Economics, Business and Management Research, 170, 22 March, 86-91. DOI: 10.2991/aebmr.k.210320.016

## Authors' Profiles

**Oleksandr Korystin:** DSc (Law), Professor. In 2009 he received DSc degree in information law from NAIA. In 2014 he received Professor degree. Honored Academic of Science and Technology of Ukraine.

Chief Research Scientist of the Criminological Research Laboratory of the State Scientific Research Institute of the Ministry of Internal Affairs of Ukraine. Professor of the Private Higher Educational Institution "Bukovinian University" (Chernivtsi). In 2014–2016 – Rector of the Odesa State University of Internal Affairs. Head of the Risk Management & Resilience Committee NGO "Institute of Cyber Warfare Research". Research interests: cybersecurity; criminology; economic security; intelligence; methodology of strategical (SWOT-analysis; risks assessment); cyber resilience, counteraction to the hybrid threat.

**Serhii Demediuk:** Ph.D (Law), Deputy Secretary of the National Security and Defense Council of Ukraine. Deputy Head of the National Coordination Center for Cyber Security. Professor of the Cybersecurity Department of the National Academy of the Security Service of Ukraine. From 2015 to 2019 - Chief of the Cyber Police of Ukraine. Research interests: information security, cybersecurity, cyber warfare, cybercrime, cyber resilience, intelligence, counteraction to the hybrid threat.

**Yaroslav Likhovitskyy:** DSc (Law), Professor. In 2018 he received DSc degree in administrative law and procedure; financial law; information law. In 2023 he received Professor degree. Professor of the Department of Criminal Law Policy of the Uzhhorod National University. Research interests: criminology; economic security; intelligence; information security, cybersecurity, cybercrime.

**Yuriy Kardashevskyy:** PhD, Head of Internal Control Department, National Agency for the Prevention of Corruption

From 2015 to 2023 - worked at the National Anti-Corruption Bureau of Ukraine. Research interests: information security, cybersecurity, cyber warfare, cybercrime, cyber resilience, intelligence, counteraction to the hybrid threat.

**Olena Mitina:** PhD Philological Sciences, Associate Professor, Head of the English Philology and Translation Studies Dpt., Odesa National Polytechnic University. Research interests: English lexicology; interactive technologies for foreign languages; criminology; cybersecurity;

**How to cite this paper:** Oleksandr Korystin, Serhii Demediuk, Yaroslav Likhovitskyy, Yuriy Kardashevskyy, Olena Mitina, "Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns", International Journal of Information Technology and Computer Science(IJITCS), Vol.17, No.2, pp.24-35, 2025. DOI:10.5815/ijitcs.2025.02.03