# Integrating the compartmentalization method into information protection against OSINT reconnaissance*

Valeriia Ivkova[1,†] and Ivan Opirskyy[1,*,†]

[1] Lviv Polytechnic National University, Information Security Department, 12 Stepan Bandera str., 79013 Lviv, Ukraine

**Abstract**

The article examines the effectiveness of compartmentalization as a strategic tool for protecting personal data and countering open source intelligence (OSINT). It analyzes the conceptual gap between complex corporate cybersecurity systems and the needs of individual users. The author examines the technical aspects of isolating digital identities using the example of the Qubes OS and Tails operating systems and the CHERI hardware architecture. The study includes an experimental simulation aimed at comparing the vulnerability of users with a traditional approach to digital hygiene and users who apply the compartmentalization method. The results showed that the implementation of the "need-to-know" model increases the time required to deanonymize an object by almost four times and significantly complicates the construction of an identity graph for the attacking party. The article emphasizes the need to transform compartmentalization from a highly specialized military method into a widely available model of personal cybersecurity.

**Keywords**

cybersecurity, compartmentalization, OSINT, counter-OSINT, data isolation, digital identity.

## 1. Introduction

The modern architecture of global information communications has led to a paradoxical situation where excessive data availability has become a critical vulnerability for both individual users and government institutions. Open source intelligence (OSINT) has transformed from an auxiliary tool into a dominant methodology for gathering intelligence, allowing aggressors, cybercriminals, and analysts to reconstruct detailed digital profiles of targets with minimal resource investment. In the context of hybrid threats, especially in the context of a full-scale invasion of Ukraine, OSINT technologies have become a tool not only for informational influence but also for physical targeting, requiring the development and implementation of fundamentally new methods of protection.

One of the most promising approaches to minimizing the risks of de-anonymization is the compartmentalization method, which is based on the fundamental principle of isolating digital identities. Unlike traditional digital hygiene, which is often limited to passive measures (changing passwords, adjusting privacy settings), compartmentalization offers a structural reorganization of the subject's interaction with the digital environment. This article presents the results of an in-depth study aimed at quantitative assessment of the protective potential of compartmentalization through simulation modeling of OSINT attacks and statistical analysis of their success.

## 2. Literature review

The current state of scientific research in the field of cybersecurity is characterized by a pronounced emphasis on protecting corporate information systems, while the security of individual users remains a less explored area. Despite this, statistics indicate a rapid evolution of

* CPITS 2026: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2026, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
valeriia.s.ivkova@lpnu.ua (V. Ivkova); ivan.r.opirskyi@lpnu.ua (I. Opirskyy)
0000-0002-2370-1497 (V. Ivkova); 0000-0002-8461-8996 (I. Opirskyy)
© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-09-24

CEUR-WS.org/Vol-4271/short1.pdf

threats targeting individuals, including phishing, ransomware, spyware, and sophisticated forms of social engineering and digital stalking.

An analysis of existing security tools reveals a significant gap between corporate and personal security architectures. Traditional intrusion detection systems (IDS), designed for large infrastructures, are focused on real-time analysis of network packet arrays, as demonstrated by two-stage anomaly detection models [1], and require significant computing resources and professional monitoring. For individual users, the use of such systems is ineffective due to excessive configuration complexity, the need for specialized monitoring hardware [2], and high operating costs. This indicates an ideological gap: while corporate security is based on the principles of centralized control, personal security requires prioritization of simplicity, autonomy, and accessibility for non-technical entities.

A fundamental approach to solving the problem of personal system vulnerability is the compartmentalization method, which has its roots in military practice and intelligence. This method is based on the "need-to-know" model, where access to information is strictly limited to functional needs. The key philosophy of this approach is that compromising one segment of the system should not lead to a cascading collapse of the entire security structure.

Fundamental research in the field of deanonymization of large datasets confirms that even in the absence of direct identifiers, correlation between disparate attributes allows for the reconstruction of a digital identity with high accuracy [3–6]. This makes compartmentalization not just an additional measure, but a necessary architectural requirement, since traditional "hygiene" methods are not able to counteract modern statistical analysis algorithms [7].

In a digital context, compartmentalization transforms into logical and technical isolation of identities. As Nasir Safwan notes, the use of isolation at the operating system level allows threats to be localized within virtual environments [8]. Specifically:

- Tails OS ensures privacy by routing traffic through the Tor network and completely avoiding the storage of data on physical media.
- Qubes OS implements micro-segmentation based on virtualization, creating isolated domains ("qubes") for different types of activities, which makes it impossible to correlate data between them.

The CHERI (Morello) architecture demonstrates the possibility of hardware isolation of processes in memory, which is a direct technical analogue of digital identity separation.

The concept of "Security by Isolation" implemented in Qubes OS is based on the principle that software inevitably contains vulnerabilities, so the only reliable protection is to minimize damage through strict domain segmentation [9]. At the hardware level, this approach is supported by the CHERI architecture, which implements mandatory memory protection, blocking the possibility of an attacker going beyond the boundaries of the isolated process [10].

Research by Javorsek et al. (2015) indicates that although excessive compartmentalization can create obstacles to operational intelligence activities, it remains critical for protecting classified data [11]. In the civilian sector, this principle is effectively implemented through the separation of access rights, where each entity (e.g., doctor, accountant, or administrator) interacts only with a specific cluster of data necessary for the performance of professional functions.

In the field of mobile security, Suarez-Tangil et al. experimentally confirmed that the implementation of compartmentalization policies in Android OS through the creation of shared containers significantly minimizes the risks of information leakage [12].

Research by Koniechny (2025) proposes an Anti-OSINT methodology that focuses on preventing unauthorized data collection through the analysis of relationships between objects. However, the implementation of such methods requires significant computing power and a large number of specialists. Compartmentalization, in turn, shifts the focus to proactively minimizing the user's digital footprint [13, 14].

The compartmentalization method is particularly relevant as a Counter-OSINT tool. For OSINT analysts, the main obstacle is the lack of pivoting points. If, in a traditional object profile, different digital identifiers (phone, email) are linked together, this allows a coherent identity graph to be

constructed. Compartmentalization breaks these links, forcing the attacking party to work with fragmented data that cannot be combined into a single profile without significant analytical capabilities. Despite the potential of the method, its use as a targeted means of protection against OSINT remains understudied in scientific literature, which determines the vector of our research [15].

## 3. Research methods

In order to evaluate the effectiveness of the compartmentalization method as a Counter-OSINT measure, an experiment was conducted in which two groups of identities were studied. In particular, 10 OSINT scenarios were created for 2 groups of identities:

- Group "A" (control) — non-compartmentalized identities. Characterized by the use of single registration data (phone number, e-mail), the presence of cross-references between social networks and professional profiles, repetitive content (photos, geotags) [16].
- Group "B" (experimental) — compartmentalized identities. Built on the principle of isolated "digital compartments": separate technical and identification tools without mutual connections were used for each area of activity (personal, professional, public).

Characteristic features of the groups. Characteristics of Group A: Non-compartmentalized identity. Group A represented a typical model of behavior for modern users who prioritize convenience over security. This group was characterized by:

- Using a single mobile phone number as the primary identifier for MFA (multi-factor authentication), registration on social networks (Facebook, Instagram), and messengers (Telegram, WhatsApp).
- Using a shared email address for professional correspondence, newsletter subscriptions, and registration on interest-based forums.
- The presence of "visual fingerprints" — identical profile photos, the use of the same background during video calls, or the publication of photos with unique interior items that allow the location or person to be identified through reverse image search services.
- Lack of metadata control in publications, which allowed analysts to obtain device data and GPS coordinates directly from the content.

Characteristics of Group B: Compartmentalized identity. Group B was built as a "digital fortress" model, where each area of activity was isolated at the tool and data level. The main parameters included:

- The use of isolated virtual machines or browser containers for different types of activity (for example, one container exclusively for banking operations, another for social networks via VPN).
- Complete absence of cross-references between "compartments": unique registration data (phone numbers, e-mail) with no common history in leak databases was used for each area of activity.
- Conscious management of digital footprints: use of pseudonyms, no shared contacts between profiles, and regular deletion of metadata before uploading any content.
- Use of anonymization tools (Tor, multi-layer VPNs) for each identity separately, making IP address correlation impossible.

Each scenario modeled the working path of a hypothetical analyst attempting to uncover the subject's true identity.

## 4. Main material

Register of experimental data and preliminary analysis.

During the experiment, results were recorded for each of the 20 scenarios. The data included not only the success rate of de-anonymization, but also metrics of time spent and intensity of analytical work.

**Table 1**
Modeling results (raw data register)

| Scenario_ID | Group | Success (1/0) | Time (min) | Effort (steps) | Analyst Confidence (%) |
|---|---|---|---|---|---|
| 1 | A | 1 | 30 | 5 | 90 |
| 2 | A | 1 | 40 | 6 | 85 |
| 3 | A | 0 | — | — | — |
| 4 | A | 1 | 50 | 7 | 88 |
| 5 | A | 1 | 45 | 6 | 92 |
| 6 | A | 1 | 60 | 8 | 87 |
| 7 | A | 0 | — | — | — |
| 8 | A | 1 | 35 | 5 | 95 |
| 9 | A | 1 | 55 | 7 | 89 |
| 10 | A | 1 | 42 | 6 | 91 |
| 11 | B | 0 | — | — | — |
| 12 | B | 0 | — | — | — |
| 13 | B | 1 | 150 | 14 | 80 |
| 14 | B | 0 | — | — | — |
| 15 | B | 1 | 170 | 16 | 85 |
| 16 | B | 0 | — | — | — |
| 17 | B | 0 | — | — | — |
| 18 | B | 1 | 200 | 18 | 82 |
| 19 | B | 0 | — | — | — |
| 20 | B | 0 | — | — | — |

A preliminary review of Table 1 shows that in group A, failures were rather the exception (scenarios 3 and 7), while in group B, the analyst's success was a rare event, achieved only through abnormal expenditure of time and effort. There was a complete absence of false positives, which indicates the high qualification of the analysts involved and the purity of the experimental design.

Statistical analysis and mathematical verification.

To transform observations into scientifically sound conclusions, the results obtained were statistically processed. The main focus was on assessing the reliability of success rates and comparing two independent samples.

Assessment of success rates and confidence intervals.

The proportion of successful attacks $(p)$for each group was calculated as the ratio of the number of successes to the total number of scenarios $(n=10)$:

Group A: $pa=\frac{8}{10}=0.8(80\%)$

Group B: $pa=\frac{3}{10}=0.3\ (30\%)$

A 95% confidence interval $(CI)$ was constructed for each group using the Wald method. The calculation formula is based on the standard error of the proportion $(SE)$:

$$SE=\frac{\sqrt{p(1-p)}}{n} \tag{1}$$

$$CI=p\pm z\times SE \tag{2}$$

where $z=1.96$ for a 95% confidence level.

Calculation for group A:

$$\begin{gathered} p=0.8,n=10, \\ SE=\frac{\sqrt{(0.8(1-0.8))}}{10}=\sqrt{0.016}\approx 0.1265, \\ Margin=1.96\times 0.1265=0.2479, \\ CIa=(0.8-0.2479;0.8+0.2479)\approx(0.552;1.048) \end{gathered} \tag{3}$$

Since the fraction cannot exceed 1.0, we limit the interval: $[0.552,1.000]$

Calculation for group B:

$$p=0.3,\ n=10,$$
$$SE=\frac{\sqrt{0.3(1-0.3)}}{10}=\sqrt{0.021}\approx 0.1449,$$
$$Margin=1.96\times 0.1449=0.2838,$$
$$CIa=(0.3-0.2838;\ 0.8+0.2838)\approx(0.016;\ 0.584) \quad (4)$$

Although a sample size of $n=10$ results in wide intervals, the almost complete absence of overlap indicates that the probability of a successful attack on a compartmentalized identity is fundamentally lower.

Z-test for comparing two proportions.

A Z-test was performed to test the statistical significance of the difference (80% vs. 30%). The null hypothesis $Ho$ stated that there was no difference between the groups ($p1=p2$).

Joint (combined) proportion $P$:

$$P=\frac{(x_A+x_B)}{(n_A+n_B)}=\frac{(8+3)}{(10+10)}=0.55 \quad (5)$$

Standard error of the combined proportion:

$$SEpooled=\sqrt{P(1-P)(\frac{1}{n_A}+\frac{1}{n_B})}=\sqrt{0.55(1-0.55)(\frac{1}{10}+\frac{1}{10})}\approx 0.2227 \quad (6)$$

Calculation of Z-statistics:

$$z=\frac{pa-pb}{SE_{pooled}}=0.8-\frac{0.3}{0.2227}\approx 2.244 \quad (7)$$

The value $z=2.244$ exceeds the critical value 1.96 for $\alpha=0.05$. The two-tailed $p$ value is approximately 0.025, which allows us to confidently reject the null hypothesis. This means that the effect of reducing the success rate of OSINT attacks when compartmentalization is applied is not a random fluctuation in the data, but reflects a real pattern.

Analysis of the time and operational complexity of OSINT attacks.

In addition to the success rate, it is critically important to analyze the resources spent by the attacking party. The simulation experiment recorded a nonlinear increase in the complexity of attacks when encountering compartmentalized profiles.

**Table 2.**

Comparison of OSINT attack effectiveness metrics

| Indicator | Group A | Group B | Effect (B/A) |
|---|---|---|---|
| Success rate of de-anonymization (%) | 80 | 30 | -62.5 |
| $(Tmed)$Median disclosure time | 43.5 min | 170.0 min | x 3.91 |
| $Effort$Average number of steps | 6.25 | 16.00 | x 2.56 |
| Analyst confidence level (%) | 90 | 82 | -8.9 |

Time expenditure dynamics. The median time required for successful de-anonymization increased almost fourfold, from 43.5 minutes to 170 minutes. This indicates that compartmentalization shifts OSINT attacks from the category of rapid automated collection to that of complex intellectual investigation. In group A, analysts often achieved results within the first 30 minutes by identifying common email addresses or phone numbers in leak databases. In group B, successful cases (e.g., scenario 18, where the time was 200 minutes) required in-depth cross-platform analysis and the identification of hidden patterns.

Analytical efforts and cognitive load. The average number of discrete analytical steps increased from 6.25 to 16.0. This indicates that analysts are forced to construct significantly longer logical chains. In group A, a typical chain looked like this: “Nickname \to Email \to Password (through a leak) \to Real name.” In group B, analysts had to use social and behavioral analysis methods, such

as studying the style of posts (stylometry), analyzing publication times, and searching for random common elements in the background of photos. The decrease in the analyst's confidence level from 90% to 82% also highlights the growing ambiguity and complexity of the verification process in conditions of data isolation.

Differentiation of de-anonymization vectors and vulnerabilities. Analysis of successful cases has revealed the vectors that most often led to the compromise of objects. Understanding these vectors is key to improving compartmentalization policies.

Visual identification (45% of cases). This vector proved to be the most effective and, at the same time, the fastest. It includes:

- Using identical or similar profile photos on different resources, which allows you to instantly link accounts via Google Lens or FaceCheck.id.
- The presence of unique artifacts in the frame (paintings, specific books, equipment with serial numbers) that can "migrate" from personal photos to professional ones.
- Geographical correlation: identification of place of residence based on the background from the window or metadata, which is then matched with another identity operating in the same location.

Technical attribution and metadata (30% of cases). Despite the technical training of Group B, some entities made mistakes in technical isolation:

- Using a single phone number to restore access to "isolated" accounts. Analysts checked partially hidden numbers in password reset services, which made it possible to confirm the connection between accounts.
- Data leaks from previous years. If an identity was created based on an old email address that was once linked to a real name, OSINT methods made it possible to "reveal" the historical connection through services such as DeHashed.

Social and behavioral analysis (25% of cases). The most labor-intensive but effective method of countering deep compartmentalization:

1. Identifying identical contact lists or subscriptions in different "compartments." If two seemingly independent accounts subscribe to a narrow group of specific specialists, the likelihood that they belong to the same person increases.
2. Analyzing writing style: the use of unique slang words, specific punctuation errors, or characteristic emojis allows anonymous profiles to be linked.
3. Activity timing: coincidences in publication times or long periods of silence that are synchronized between accounts indicate a single source of activity.

The role of the human factor and psychological aspects of protection. The experiment confirmed the thesis that the human factor remains the "weakest link" even in the most technologically advanced protection systems. In group B, all three successful de-anonymizations were the result of user behavior errors rather than technical breaches of isolation (scenarios 13, 15, 18).

According to research, over 90% of cyber incidents are related to human error. In the context of OSINT, this manifests itself through "security fatigue": it is difficult for users to constantly switch VPNs, remember which cover story they are using for a particular profile, and avoid mentioning their personal life in professional circles. The lack of systematic training in digital hygiene means that even with the tools available (Qubes OS, Tails), users make fatal mistakes in their use.

The errors recorded in experimental group "B" can be explained by the phenomenon of "security fatigue". Maintaining multiple isolated identities creates a high cognitive load, which leads to unconsciously ignoring security protocols for the sake of convenience [17]. In addition, even with complete technical isolation, the identity remains vulnerable to stylometry methods — linguistic analysis that allows you to link anonymous profiles through characteristic writing patterns.

Remarkably, in the Ukrainian context, interest in OSINT and counter-OSINT grew rapidly after 2022, stimulating the development of a culture of cyber security. However, as practice shows, a significant proportion of users and even businesses ignore preventive measures until an incident

occurs. Compartmentalization requires a high level of self-discipline, which makes its implementation not only a technical but also a psychological and educational task.

According to the results of the experiment, the success rate of attacks in group “A” was 80% (8 out of 10 cases), while in group “B” it was only 30% (3 out of 10 cases). The median time required to reveal the identity was 43.5 minutes for group “A” and 170 minutes for group “B.” The average number of analytical steps for successful cases was 6.25 in group “A” versus 16.0 in group “B.” No false positives were recorded in the simulation.

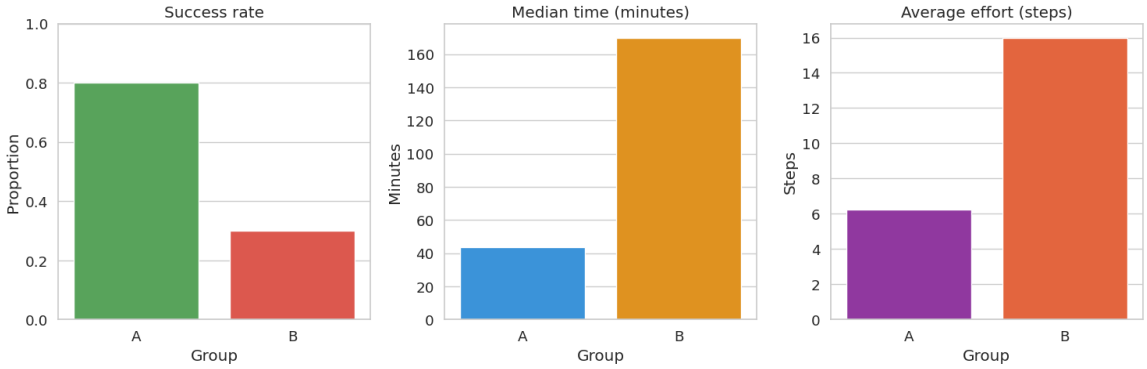


**Figure 1:** Results of the experiment

The results show that compartmentalization of digital identities not only reduces the overall risk of successful de-anonymization, but also increases the time and cognitive costs for the attacker. The experiment confirms the practical feasibility of implementing this approach as a preventive measure in the field of information security [18–20].

## Conclusions

The results of the study confirm that the implementation of the compartmentalization method is a critically effective mechanism for minimizing the risks of de-anonymization in the context of active use of OSINT technologies. Experimental testing demonstrated a significant increase in the stability of the digital profile: the use of the isolated identities model reduced the success rate of attacks from 80% to 30%, while the median time required to uncover the target increased almost fourfold (from 43.5 to 170 minutes). These indicators show that breaking the links between professional, personal, and technical data domains creates an insurmountable analytical barrier for the attacking party, fragmenting the identity graph and making data correlation economically and time-inefficient.

At the same time, the study revealed a significant dependence of protection effectiveness on the user's level of technical competence and operational discipline. Despite the availability of powerful isolation tools at the system kernel level (Qubes OS) or network traffic level (Tails), the main vulnerability remains the human factor and the lack of systematic training in digital hygiene. Thus, further development of the personal cybersecurity industry should be aimed not only at improving virtualization and containerization technologies, but also at developing intuitive interfaces and educational models that will allow the principles of Counter-OSINT to be scaled for a wide range of users in a hybrid threat environment.

## Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication’s content.

## References


[1] V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 23–32.

[2] I. Bogachuk, V. Sokolov, V. Buriachok, Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers, in: 5th International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (2018) 581–585. doi:10.1109/INFOCOMMST.2018.8632151

[3] A. Narayanan, V. Shmatikov, Robust De-anonymization of Large Sparse Datasets, In: 2008 IEEE Symposium on Security and Privacy (2008) 111–125, doi:10.1109/SP.2008.33

[4] O. Harasymchuk, et al. Modern Methods of Ensuring Information Protection in Cybersecurity Systems using Artificial Intelligence and Blockchain Technology, Kharkiv: Technology Center PC, 2025, doi:10.15587/978-617-8360-12-2

[5] O. Harasymchuk, et al., Intelligent Cyber Defence Systems: Detection of Ransomware and Protection of Wireless Networks based on Artificial Intelligence Technologies: Collective Monograph, Kharkiv: Technology Center PC, 2025, doi:10.15587/978-617-8360-22-1

[6] O. Mykhaylova, et al., Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap, in: Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 239–251.

[7] M. Glassman, M. J. Kang, Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT), Computers in Human Behavior, vol. 28, no. 2, pp. 673-682, 2012, doi:10.1016/j.chb.2011.11.014

[8] S. Nasir, Deconstructing Modern Cyber Threats: A Practical Perspective on Privacy, Isolation, and Threat Mitigation for Personal Systems, SSRN, 2025, doi:10.2139/ssrn.5353661

[9] J. Rutkowska, The State of Software Security: The Case for Isolation, Invisible Things Lab Whitepaper, 2010.

[10] R. Watson et al., CHERI: A General-Purpose Capabilities-Based Protection Model, In: IEEE Symposium on Security and Privacy, 2015, pp. 3–18. doi:10.1109/SP.2015.9

[11] D. Javorsek, J. Rose, C. Marshall, P. Leitner, A Formal Risk-Effectiveness Analysis Proposal for the Compartmentalized Intelligence Security Structure, Int. J. Intell. CounterIntelligence, vol. 28, no. 4, pp. 734-761, 2015, doi:10.1080/08850607.2015.1051830

[12] G. Suarez-Tangil, J. Tapiador, P. Peris-Lopez, Compartmentation Policies for Android Apps: A Combinatorial Optimization Approach, In: Network and System Security (NSS 2015), M. Qiu, S. Xu, M. Yung, and H. Zhang, Eds. Cham: Springer, 2015, vol. 9408, pp. 63–77, doi:10.1007/978-3-319-25645-0_5

[13] M. Konieczny, Legal Aspects of Using Anti-OSINT as a Tool to Protect Internet Users Against Identity Theft, RAIP, vol. 4, no. XXIV, pp. 105–123, 2024, doi:10.5604/01.3001.0054.9821

[14] M. Konieczny, Anti-OSINT Methods Ensuring Protection of Personal Data in the Context of Cybercrime, RAIP, vol. 1, no. XXV, pp. 127-144, 2025, doi:10.5604/01.3001.0055.1100

[15] V. Ivkova, I. Opirskyy, Research Into the Possibility of Integrating the Compartmentalization Method Into the Protection of Information in Open Sources, Cyberphysical Syst. Ubiquitous Comput., vol. 2025, no. 02, p. 071, 2025, doi:10.23939/csn2025.02.071

[16] L. Rocher, J. Hendrickx, Y. de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative graphical models, Nat. Commun., vol. 10, no. 1, p. 3069, 2019, doi:10.1038/s41467-019-10933-3

[17] B. Stanton et al., Security Fatigue, IT Professional, vol. 18, no. 5, pp. 26–32, 2016, doi:10.1109/MITP.2016.84

[18] A. Cavoukian, Privacy by Design: The 7 Foundational Principles, Inf. Priv. Comm. Ont., Canada, Tech. Rep., 2011.

[19] M. Bada, J. R. Nurse, Developing Cybersecurity Education and Awareness Programmes, University of Oxford Technical Report, 2019, doi:10.1108/ICS-07-2018-0080

[20] H. Hulak, et al., Formation of requirements for the electronic record-book in guaranteed information systems of distance learning, in: Cybersecurity Providing in Information and Telecommunication Systems, 2021, 2923, pp. 137–142.