bility of imposing significant fines in case of violation of data protection rules. The method will allow businesses to assess the potential financial consequences of a data leakage and implement effective preventive measures to saving themselves from possible fines. This developed method will help organizations effectively implement the GDPR requirements, ensuring a high level of data protection and appropriate risk management. The purpose of this paper is to develop a method for assessing the negative consequences of a PD confidentiality leakage in case of violation of the requirements established by the GDPR. The method of assessment in accordance with the provisions of the GDPR Regulation, which, through the stages of identifying the object of assessment (providing information about the enterprise), determining the level of violation, forming primary expert information and finalizing the procedure for processing expert data, analytically transforms the sets of input data of the developed tuple model of the integrated representation of parameters, values of values reflecting the judgment of experts, developed new assessment rules, scattering of points and a certain set of recommendations.

**Keywords:** cybersecurity, cyber security, information protection, information security, personal data, a multiple-theoretical representation, GDPR-model, model of personal data parameters, assessment in the area of information security, GDPR regulation, losses assessment, loss of personal data.

**Шульга Володимир Петрович,** доктор історичних наук, в.о. ректора Національного авіаційного університету, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
**Volodymyr Shulha,** Acting Rector of National Aviation University, professor of IT-Security Academic Department, National Aviation University.
E-mail: shulga.khnuvs@gmail.com.
Orcid ID: 0000-0003-4356-7288.

**Корченко Олександр Григорович,** доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, в.о. проректора з наукової роботи Національного авіаційного університету.
**Oleksandr Korchenko**, Dr Eng (Information security), professor, laureate of the State Prize of Ukraine in Science and Technology, Acting Vice-Rector for Scientific Work of National Aviation University.
E-mail: icaocentre@nau.edu.ua.
Orcid ID: 0000-0003-3376-0631.

**Заріцький Олег Володимирович**, доктор технічних наук, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
**Oleg Zaritskyi**, Dr Eng (Information security), professor of IT-Security Academic Department, National Aviation University.
E-mail: oleg.zaritskyi@gmail.com.
Orcid ID: 0000-0002-6116-4426.

**Лозова Ірина Леонідівна**, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.
**Iryna Lozova**, Senior lector of IT-Security Academic Department, National Aviation University.
E-mail: illozovaya@gmail.com.
Orcid ID: 0000-0002-7224-4763.

**Педченко Євгеній Максимович**, аспірант, асистент кафедри безпеки інформаційних технологій Національного авіаційного університету.
**Yevhenii Pedchenko**, PhD Student, Assistant of IT-Security Academic Department, National Aviation University.
E-mail: ympedchenko@gmail.com.
Orcid ID: 0000-0001-8436-5792.

**DOI: 10.18372/2410-7840.25.18233**
**УДК 004.056.5**

# DEFINING THE SEQUENCE OF INTEGRATING TRUSTWORTHINESS COMPONENTS INTO INFORMATION SECURITY SYSTEMS

***Oleksandr Bakalynskyi, Fedir Korobeynikov***

*The article explores the concept of trustworthiness as an approach to building information security systems, which helps to maintain trust in the information systems they protect. Key components of trustworthiness are identified and ranked: resilience, security, safety, privacy, and compliance. Attention is focused on the significance of the emergent interaction of these components, providing a justified percentage weight for each of them. Two approaches to creating trustworthy systems are considered: the integration of trustworthiness components into the system architecture at the design stage, and the adaptation of existing systems. The advantages and disadvantages of each approach are discussed in the context of implementation speed, cost-effectiveness, and alignment with the philosophy of trustworthiness.*

***Keywords**: trustworthiness, privacy, security, resilience, safety, information security systems.*

## RELEVANCE AND PROBLEM STATEMENT

The level of civilizational development is primarily determined by the volume of information required for creating products produced by civilization [1]. This not only includes goods and services but also social institutions, forms of state governance, ideas, cultural phenomena, etc.

Existing principles for constructing information security systems [2, 3] are based on the triad of confidentiality, integrity and availability (the CIA triad) [4]. However, there is a growing need to supplement such systems with new properties aimed primarily at ensuring trust in the information systems being protected and, consequently, in the information they process. This is because the principle of trust, according to some scholars [5], is one of the fundamental principles underlying the functioning of cyberspace.

Thus, there is a need for research into concepts for constructing information security systems that aim to ensure trust in information systems. The concept of trustworthiness proposed by NIST [6], and further developed by other scholars [7, 8], is based on the idea of integrating information processing systems with the security systems by introducing components into the overall architecture that can maintain trust in these systems: reliability, resilience, security, safety, privacy, operational stability, compliance, among others.

The aim of this article is to define the sequence for integrating trustworthiness components into existing information security systems.

To achieve this, a classification of the set of components (those that pertain to the broad domain of information security) is conducted, followed by their ranking. The ranking criterion is the impact of a particular component on the overall level of trust in the information system.

## MAIN PART

*Defining Trustworthiness*

So, it is precisely the set of components that ensure trust in information systems, each of which somewhat differently formulates its own problem domain and potential solution space, that led to the genesis of trustworthiness. NIST proposed this specifically to reconcile the concepts, frameworks, and analytical processes of all these strategies in order “to achieve a compromise between various approaches to ensuring trust that can be applied to each system” [6].

There are several definitions of trustworthiness in the domain of information security. According to NIST, trustworthiness is: "The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities." [9];

A characteristic of information systems that are: “...reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and adhere to generally accepted security procedures." [10];

"The degree to which the behavior of a component is demonstrably compliant with its stated requirements." [6].

"In addition to security, other aspects of trustworthiness include reliability, safety, and resilience" [11].

Industrial Internet Consortium (IIC) defines trustworthiness as the degree of confidence one has that the system performs as expected. Characteristics include safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks [8].

The U.S. Department of Homeland Security provides a more detailed and comprehensive (but quite tolerant of the NIST and IIC definitions) interpretation, according to which trustworthiness is "a multidimensional measure of the extent to which a system is likely to satisfy each of multiple aspects of each stated requirement for some desired combination of system integrity, system availability and survivability, data confidentiality, guaranteed real-time performance, accountability, attribution, usability, and other critical needs” [12].

Summarizing the above definitions, it can be said that trustworthiness in the context of information systems signifies a multifaceted characteristic that determines whether the system is deserving of trust. Trustworthiness comprises five main components related to the domain of security, namely: security, resilience, safety, privacy, and compliance.

*Ranking Trustworthiness Components*

To determine the priority of integrating additional trustworthiness components into existing information security systems, definitions for each component were clarified, and they were ranked based on their level of importance.

A model has been proposed in which the five key components of trustworthiness emergently interact with each other, together constituting 100% of the system's trustworthiness level.

This model provides for the following distribution (fig. 1) of the significance of components: Security accounts for 25%, Resilience for 25%, Privacy for 20%, Safety for 20%, and Compliance for 10%.

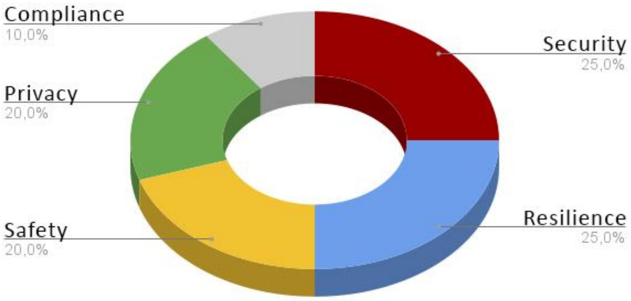

Fig. 1 Distribution of the significance of the trustworthiness components

Let's delve into each of these components to determine why security and resilience occupy the most significant positions in this model, and also justify the relative contributions of other components.

1. Security – 25% Importance in the Model.

The concept of security within the context of trustworthiness aligns closely with definitions presented in Ukrainian information security regulations, the NIST Cybersecurity Framework 1.1 [13], and ISO 27000 series standards [14]. Security is the safeguarding of systems and data against unauthorized access, use, disclosure, disruption, modification, or destruction. It includes measures to protect against both external threats, such as cyber-attacks, and internal threats, such as human error or insider threats.

The notion encompasses several key areas:

- confidentiality: ensuring that only those who have the right to access the information can do so;
- availability: ensuring reliable and timely access to information by authorized entities;
- integrity: maintaining and assuring the accuracy and completeness of data.

The reason security holds a 25% weight in the model is that it forms the fundamental layer of trust. Without proper security measures, any other aspects of trustworthiness could be compromised, undermining the overall reliability and functionality of the system.

2. Resilience – 25% Importance in the Model.

Resilience refers to the ability of systems to withstand, recover from, and adapt to adverse conditions, disruptions, or threats, whether intentional (e.g., a cyberattack) or unintentional (e.g., a system failure or natural disaster). Unlike security, resilience focuses on ensuring continuous operation even under unforeseen circumstances [15].

Resilience consists of four stages: preparation, resistance, adaptation and recovery. The stages of adaptation and recovery are crucial and involve the system's or organization's ability to change its structure, processes, or behavior in response to changing conditions or new threats. Adaptation can be both reactive and proactive, encompassing not only immediate responses to challenges but also ongoing learning and optimization based on the analysis of past events and anticipation of future changes.

Resilience fortifies trust in a system or organization by ensuring the system's operability under conditions of stress and uncertainty.

Both Security and Resilience occupy top positions in this hierarchy because they form the foundational level of trust. These are primary criteria without which all other components of trustworthiness become unfeasible.

In essence, while security lays the groundwork to prevent unauthorized access and protect data integrity, resilience ensures that even if a system faces challenges or setbacks, it can recover and adapt. Together, they constitute 50% of the model’s trustworthiness because they are essential for any system to function reliably and to maintain stakeholder trust.

3. Safety – 20% Importance in the Model.

Safety focuses on minimizing the risk of harm to users and surrounding systems. This aspect explores how a system can be employed to either eliminate or minimize the likelihood of adverse human or infrastructural impact [16].

Safety is not merely a mechanism for preventing physical or psychological harm; it is an integral attribute that ensures a system poses no threat to other "friendly" systems. This is particularly crucial in complex information ecosystems where multiple systems of various types interact with one another.

This component is garnering increased attention in contemporary research, as not only technological but also ethical aspects of safety are beginning to play a larger role in fostering trust in systems. It concentrates on preventing negative interaction scenarios, thus strengthening trust and, consequently, the overall trustworthiness of the system. While security deals with protecting the system against unauthorized access and data breaches, and resilience is about the system's ability to recover and adapt to adverse conditions, safety adds an additional layer by focusing on the well-being of users and other interconnected systems. This is why it has been assigned a 20% weightage in the trustworthiness model.

Safety acts as a supportive component that complements security and resilience. It helps in building a more comprehensive trust model, ensuring that not only is the system secure and resilient, but it is also designed and deployed in a manner that is safe for users and other systems it interacts with.

4. Privacy – 20% Importance in the Model

Privacy in the context of trustworthiness is both a right and ability for an individual or organization to control who, how, and when access can be gained to their personal or sensitive information [17].

Privacy involves measures to ensure personal data is processed properly and only according to specific, lawful, and clearly outlined purposes. It also includes the right to anonymity, where information about an individual or organization remains hidden from unauthorized parties. Unlike confidentiality, which can relate to any kind of data, privacy is specifically oriented towards information associated with individuality. Privacy is a key aspect in building trust in information systems and ensuring an individual's right to control their personal sphere and digital footprint. Trust in a system is greatly enhanced when users know that their personal and sensitive data are well-protected, thus reinforcing the system's overall trustworthiness.

Both Safety and Privacy occupy equal positions in the hierarchy of trustworthiness with a weightage of 20%. They focus on different but complementary aspects of ensuring the system does not harm users or adjacent systems.

Safety aims at minimizing physical or systemic risk, ensuring the system does not become a threat due to flawed architecture.

Privacy concentrates on protecting personal data and the sanctity of users' personal lives.

Together, they provide a significant foundation for ensuring trust in the system, as both are geared towards user protection but through different mechanisms and parameters. While security sets up the base layer of trust by defending against unauthorized access and data breaches, privacy adds a more personal layer by safeguarding individual rights and freedoms. The two components are mutually reinforcing, each complementing the other's shortcomings to create a robust framework of trustworthiness.

5. Compliance - 10% Importance in the Model.

Compliance, as a component of trustworthiness, is the process and practice of aligning information systems, processes, and operations with norms, standards, internal organizational policies, as well as national and international legislation [18]. It involves continuous monitoring and verification of systems, processes, and personnel actions to ensure compliance with established requirements, as well as responding to deviations from these requirements and changes in legislation.

Compliance aims to ensure that all aspects of the operation of information systems or organizational activities are conducted not just within the bounds of the law but also in accordance with commonly accepted norms and values. This enhances the level of trust from clients, partners, regulators, and other stakeholders. Compliance not only reduces legal and operational risks but also reinforces the organization's reputation as a reliable and responsible player in the digital space.

Compliance is crucial for adhering to laws and regulations, but its role is limited compared to other components. It provides a minimal level of trust through conformity to standards but is not sufficient for full trust in the system.

*Noteworthy*

In information systems, trustworthiness is not a simple sum of its individual components [12]. Rather, a high level of trust arises from emergent relationships between them, where the interaction and interdependence of each component lead to the formation of a comprehensive, dynamic, and adaptive property of the system to ensure its own safety at all levels. The choice of additional components depends on the context and needs of a specific organization or system.

*Approaches to Implementing Trustworthiness Components in Information Systems*

In contemporary academic discourse [12], two distinct methodologies have been identified for developing trustworthy information systems based on the construct of trustworthiness. The first approach advocates for a complete overhaul of existing systems, designing them "from scratch" with an architecture intrinsically aligned to principles of security, resilience, user safety, privacy, and regulatory compliance. This method is inherently congruent with the trustworthiness framework, offering a multi-layered, systemic implementation of trust mechanisms that address three insurmountable challenges associated with traditional, exogenously applied information security systems:

- trust gap in security personnel: traditional information security systems often bestow system administrators and operators with elevated privileges and access [19], posing risks of abuse for personal gains, potentially leading to information leakage or other security violations;
- security system vulnerability: just as primary systems are susceptible to attacks; their corresponding security systems are not exempt from vulnerabilities [20]. malicious actors may exploit these weak points to circumvent security measures and gain access to critical data;
- scalability issues: traditional security systems may become an impediment to scaling the primary systems as they necessitate additional resources, intricate management, and constant monitoring [12].

However, we are confronted with organizational realities of constrained resources that hinder the wholesale replacement of extant information systems. Implementation of this first approach demands not only significant initial capital investments and the availability of skilled trustworthiness experts in every development team, but also mandates the reservation of substantial organizational time resources for comprehensive integration of complex security architectures. Moreover, existing legislative frameworks [21] may also restrict the adoption of certain types of information security systems, further complicating matters.

In such circumstances, a pragmatic alternative is the incremental deployment of key trustworthiness components. This could be done in accordance with their hierarchical significance as outlined in the proposed ranking model, aiming to augment trust levels and assure multifaceted security within the scope of available resources.

By adopting a phased approach, organizations can methodically address each facet of trustworthiness, incrementally bolstering system reliability without a complete system overhaul, thus allowing for a more feasible transition towards a trustworthy architecture.

## CONCLUSION AND FUTURE DIRECTIONS

In the current study, key components and ideas shaping the concept of trustworthiness in information systems were identified. A ranking model was developed to prioritize these components, offering an effective strategy for their integration into either newly developed or existing information security systems.

It was established that Security and Resilience are fundamental to the concept of trustworthiness, each contributing 25% to the overall trust metric. These components should be prioritized for implementation as their absence undermines the effectiveness of all subsequent trust-based features. Privacy and User Safety, each accounting for 20% of the overall trustworthiness score, focus on the prevention of harm through different mechanisms. Compliance, with the least weight of 10%, ensures the system's alignment with legislative standards.

Two primary approaches to the development of trustworthy systems were analyzed: full-scale integration of trust elements at the inception stage and an incremental approach to retrofitting existing systems. While the former represents the ideologically purer form of trustworthiness, its practical implementation is often marred by resource constraints and organizational inertia. Conversely, the incremental model, albeit suboptimal from a theoretical standpoint, offers a pragmatic compromise, allowing organizations to sequentially enhance system trustworthiness within existing resource allocations.

The findings of this research can serve as a basis for further exploration and development of trustworthiness integration mechanisms in information systems. Given the increasing digital transformation of society, the importance of building inherently trustworthy systems is underscored. Future research may focus on the development of adaptive trust models that can respond to emerging security challenges and technological advancements.

The contributions of this work provide a foundational framework that can catalyze further academic inquiry and practical application in the burgeoning field of information system trustworthiness. As digital transformation continues to accelerate, the exigency to build inherently trustworthy systems has never been more critical. Future studies could delve deeper into creating adaptive trust models that can evolve in response to emergent security threats and technological advancements, thereby ensuring the relevance and resilience of our framework in dynamically changing digital ecosystems.

## REFERENCES

[1] Castells M. The Rise of the Network Society: The Information Age: Economy, Society, and Culture. Volume 1. 2nd ed. Oxford, UK: Wiley-Blackwell Publishers Ltd, 2010. 597 p.

[2] Mokhor V., Tsurkan V. Conceptual basis of description for the information security management system architecture. Collection "Information technology and security". 2019. Vol. 7, no. 2. pp. 197-207. URL: https://doi.org/10.20535/2411-1031.2019.7.2.190569.

[3] On Protection of Information in Information and Communication Systems: Law of Ukraine dated 05.07.1994 № 80/94-ВР Bulletin of the Verkhovna Rada of Ukraine № 1994, № 31, 286 p.

[4] Spyridon Samonas, David Coss. The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. Journal of Information System Security. 2014. Vol. 10, no. 3. pp. 21-45.

[5] Clark D. The Role of Trust in Cyberspace. Trust, Computing, and Society / ed. by R. H. R. Harper. New York, 2014. pp. 17-37. URL: https://doi.org/10.1017/cbo9781139828567.005.

[6] Special Publication 800-160, Volume 1. Engineering trustworthy secure systems. 2022. 113 p. URL: https: //doi.org/10.6028/NIST.SP.800-160v1r1.

[7] Henschke A., Ford S. B. Cybersecurity, trustworthiness and resilient systems: guiding values for policy. Journal of Cyber Policy. 2016. Vol. 2, no. 1. pp. 82-95 URL: https://doi.org/10.1080/23738871.2016.124372.

[8] M. Buchheit, F. Hirsch, R.A. Martin. Trustworthiness Framework Foundations. An Industrial Internet Consortium Foundational Document. 2021. URL: https:// www.iiconsortium.org / pdf / Trustworthiness_Framework_Foundations.pdf.

[9] NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2018. URL: https: // doi.org /10.6028/nist. sp. 800-37r2.

[10] NIST Special Publication 800-12. An introduction to information security. Gaithersburg, MD: National Institute of Standards and Technology, 2017. URL: https: //doi.org/10.6028/nist.sp.800-12r1.

[11] NIST SP 800-160 Vol. 2. Developing Cyber-Resilient Systems / R. Ross et Gaithersburg, MD National Institute of Standards and Technology. 2021 URL: https:// doi.org/10.6028/nist.sp.800-160v2r1.

[12] A Roadmap for Cybersecurity Research. Washing-ton, USA. Department of Homeland Security, 2009. 126 p. URL: https: // www.dhs.gov /sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf.

[13] NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Ukrainian Translation). (2022). National Institute of Standards and Technology. URL: https://doi.org/10.6028/nist.cswp.04162018uk.

[14] Bakalynskyi O., Bezshtanko V. The ISO / IEC 27000 family of standards as a source for creating a national cybersecurity standard. Materials of the 13th meeting of the Interdepartmental Expert Working Group on countering threats to the proliferation of weapons and materials of mass destruction, Kyiv, 11 March 2014. 2014. URL: https: //niss.gov.ua/sites/default/files/2014-03/0311_prez2.pdf.

[15] Korobeynikov F. Resilience Paradigm Development In The Security Domain. Electronic Modeling. 2023, 45(4): pp. 88-110. URL: https: // doi.org / 10.15407 /emodel. 45.04.088.

[16] NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, 2015. URL: https://doi.org/10.6028/nist.sp.800-82r2.

[17] NIST Privacy Framework. National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/nist.cswp.01162020.

[18] Angraini, Alias R. A., Okfalisa. Information Security Policy Compliance: Systematic Literature Review. Procedia Computer Science. 2019. Vol. 161. pp. 1216-1224. URL: https://doi.org/10.1016/j.procs.2019.11.235.

[19] Patrick A. S., Briggs P., Marsh S. Designing systems that people will trust //Security and Usability. 2005. v. 1. №. 1. pp. 75-99.

[20] Viega J., Kohno T., Potter B. Trust (and mistrust) in secure applications. Communications of the ACM. 2001. Vol. 44, no. 2. pp. 31-36. URL: https: // doi.org /10.1145/359205.359223.

[21] On Approval of the Rules for Ensuring Information Protection in Information, Electronic Communication and Information and Communication Systems. Resolution of 29.03.2006. No. 373: as of October 21. 2022. URL: https: // zakon.rada.gov.ua / laws / show / 373-2006-п#Text.

## ВИЗНАЧЕННЯ ПОСЛІДОВНОСТІ ІНТЕГРАЦІЇ КОМПОНЕНТІВ ТРАСТОСПРОМОЖНОСТІ В СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

В статті досліджується концепція трастоспроможності (trustworthiness) як підхід до побудови систем захисту інформації, що сприяє підтриманню довіри до інформаційних систем, які вони захищають. Визначаються та ранжуються ключові компоненти трастоспроможності: резильєнтність, безпека, безпечність, приватність і комплаєнс. Акцентується увага на значущості емерджентної взаємодії цих компонентів, надається обґрунтована відсоткова вага кожного з них. Розглядаються два підходи до створення систем, що заслуговують на довіру: інтеграція компонентів трастоспроможності в архітектуру систем на етапі проектування, та адаптація наявних систем. Висвітлюються переваги та недоліки кожного підходу в контексті швидкості впровадження, економічності та відповідності ідеології трастоспроможності.

**Ключові слова**: трастоспроможність, приватність, безпека, резильєнтність, безпечність, системи захисту інформації.

**Бакалинський Олександр Олегович**, кандидат технічних наук, старший дослідник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

**Oleksandr Bakalynskyi**, Candidate of technical sciences, Senior Researcher, Pukhov Institute for Modeling in Energy Engineering of the National Academy of Sciences of Ukraine.
E-mail: baov@meta.ua.
Orcid ID: 0000-0001-9712-2036.

**Коробейніков Федір Олександрович**, аспірант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

**Fedir Korobeynikov**, Ph.D. Candidate, G.E. Pukhov Institute for Modeling in Energy Engineering of the National Academy of Sciences of Ukraine.
E-mail: admin@cybersecurity.com.ua.
Orcid ID: 0009-0003-8127-4379.