A RISK-ORIENTED FRAMEWORK FOR FORMING AND MODELLING INFORMATION SECURITY PROFILES IN MODERN CYBERSPACE

Ruslan Netrebko

e-mail: netr_rv@ukr.net , ORCID ID: https://orcid.org/0000-0003-3212-5249

Korolov Zhytomyr Military Institute, Zhytomyr, Ukraine

Received: December 13, 2025 | Revised: December 28, 2025 | Accepted: December 31, 2025

UDC 004.056

DOI: https://doi.org/10.33445/psssj.2025.6.4.6

Abstract

The purpose of the article is to substantiate the theoretical foundations for forming information security profiles in Ukraine and to adapt established probabilistic, optimization, and economic models for assessing their effectiveness, resilience, and resource feasibility in critical infrastructure information systems. The study combines historical-regulatory and comparative analysis of Ukrainian requirements with NIST SP 800-series and ISO/IEC standards, set-theoretic formalization, a two-state continuous-time Markov model, binary optimization under a budget constraint, annualized loss expectancy, and return on security investment. The development of Ukrainian regulation between 2021 and 2026 is represented as three stages: institutional preparation and wartime transition, harmonization with international standards, and implementation of a risk-oriented approach. Four types of security profiles are distinguished: basic, sectoral, target, and adapted. A security profile is formalized as a set of security and privacy requirements, selected controls, control enhancements, organization-defined parameters, and mappings to identified threats and risks. The proposed indicators support risk-weighted threat coverage, a simplified availability-like resilience estimate, and selection of controls subject to resource constraints. The study integrates and adapts established regulatory, probabilistic, optimization, and economic approaches to the Ukrainian technical information protection framework rather than claiming a universal assessment model. The models may support owners and administrators of critical infrastructure information systems in documenting, selecting, assessing, and authorizing protective measures, provided that model parameters are empirically calibrated for the relevant system.

Key words: ND TZI 3.6-006-24; Risk Management; Critical Infrastructure; Protective Measures; Cyber Resilience; Resource Allocation.

Introduction

In the contemporary world, information has acquired the status of one of the key strategic resources of the system for ensuring the national security and defence of the state. Under the conditions of the armed conflicts and hybrid confrontation of the twenty-first century, the systematic assessment of risks to the security of information processed and stored in automated systems has become particularly important. The active use by an adversary of technical and cyber reconnaissance, cyberattacks, information-psychological operations, and disinformation campaigns substantially increases the level of threats to such systems and creates risks of unauthorized access to, loss of, or modification of protected information.

Under conditions of high-intensity information confrontation and the rapid development of cyber instruments, even minor miscalculations in assessing the risks of breaches of confidentiality,

integrity, or availability of information may lead to serious consequences. These include threats to the security of personnel, reduced effectiveness in the employment of weapons and military equipment, and the disruption of command and control during the performance of combat missions.

Despite the existence of a regulatory and legal framework in the field of technical information protection, one of the key problems remains the practical implementation of, and compliance with, the established procedure for assessing risks to the security of information processed in automated systems, including those of the Armed Forces of Ukraine. This is caused by dynamic changes in the operational situation, limited resources, and the vulnerability of communication channels, which require the constant review, refinement, and adaptation of risk assessment procedures to real conditions.

In an environment of persistent cyber threats and the digital transformation of state institutions, traditional template-based methods of protection are losing effectiveness. A new stage in the development of technical information protection (TIP) in Ukraine began in 2024 with the adoption of ND TZI 3.6-006-24, Procedure for Selecting Measures to Protect Information, the Protection Requirement for Which Is Established by Law and Which Does Not Constitute a State Secret, for Information Systems (Administration of the SSSCIP, 2024). The document establishes a risk-oriented procedure for selecting and tailoring protective measures for information systems. Resolution No. 712 of the Cabinet of Ministers of Ukraine subsequently specified the governance of basic, sectoral, and target security profiles and security authorization (Cabinet of Ministers of Ukraine, 2025). Together, these instruments support a transition from static sets of requirements to profiles adapted to the purpose, criticality, operating environment, and risks of a particular system. Theoretical formalization can reduce subjectivity in selecting measures and improve the transparency of resource allocation.

The purpose of this study is to analyse the evolution of the Ukrainian regulatory framework for security profiling since 2021, with an emphasis on ND TZI 3.6-006-24 and Resolution No. 712 of the Cabinet of Ministers of Ukraine; to systematize the structure of a security profile in relation to NIST SP 800-series and ISO/IEC standards; and to construct an integrated analytical framework for assessing the technical and economic characteristics of such profiles.

To achieve this purpose, the study addresses the following research objectives:

to identify the principal stages in the transformation of the Ukrainian regulatory framework for security profiling between 2021 and 2026;

to systematize the typology and structure of security profiles established by ND TZI 3.6-006-24 and distinguish it from the governance framework of Resolution No. 712;

to develop a formal set-theoretic model of the security profile and an indicator of its threat-coverage effectiveness;

to model the resilience of a protected system using Markov chains and to formulate the problem of the optimal selection of protective measures under budget constraints;

to substantiate economic indicators of the effectiveness of security investment and the procedure for profile verification.

The object of the study is the process of forming information security profiles for critical infrastructure information systems.

The subject of the study is the theoretical foundations and analytical models for the formation, assessment, and verification of security profiles based on ND TZI 3.6-006-24 and the international standards of the NIST SP 800 series.

Literature Review

1. The Systemic Approach to Technical Information Protection in Ukraine

A systemic approach treats information protection not as a set of isolated technical tools but as an organizational and technical system whose composition must be justified by the mission,

architecture, criticality, and risk context of the protected object. In the economic literature, security investment is analysed through expected-loss reduction, budget constraints, and the marginal effectiveness of controls (Gordon & Loeb, 2002; Cavusoglu et al., 2004; Bojanc et al., 2012). Portfolio formulations further show that the selection of controls is a constrained resource-allocation problem rather than an unconstrained maximization of protection (Yevseyeva et al., 2015).

2. International Standards and the Risk-Oriented Approach

International experience provides complementary layers for risk-oriented profiling. NIST SP 800-39 and SP 800-37 Rev. 2 define organization- and system-level risk-management processes; SP 800-53 Rev. 5, SP 800-53B, and SP 800-53A Rev. 5 address controls, baselines, tailoring, and assessment; SP 800-30 Rev. 1 and the NIST IR 8286 series address risk identification, estimation, prioritization, and enterprise integration (Joint Task Force Transformation Initiative, 2011; National Institute of Standards and Technology [NIST], 2012, 2025a, 2025b, 2025c; Joint Task Force, 2018, 2020a, 2020b, 2022). ISO 31000 and ISO/IEC 27005 provide general and information-security risk guidance, while the NIST Cybersecurity Framework 2.0 supports organizational profiles and outcome-oriented governance (International Organization for Standardization [ISO], 2018, 2022; NIST, 2024). Quantitative risk and resilience remain parameter-dependent and require calibrated evidence (Hubbard & Seiersen, 2016; Wang et al., 2020; Linkov et al., 2013; Kott & Linkov, 2019).

However, the reviewed approaches address different analytical layers and are not directly interchangeable. Regulatory standards define governance, control selection, tailoring, assessment, and authorization; economic models estimate expected-loss reduction and investment efficiency; optimization models treat security controls as a constrained portfolio; and resilience models represent system behaviour under disruption and recovery. A methodological gap therefore remains between the formal structure of a Ukrainian security profile and the quantitative procedures used to compare alternative control configurations. The present study addresses this gap by integrating the official Ukrainian procedure for selecting protective measures with established international models, while explicitly limiting quantitative conclusions to systems for which input parameters have been empirically calibrated.

The scientific contribution of the study consists in constructing an integrated analytical representation of the Ukrainian security-profile framework in which regulatory profile components are linked to threat coverage, an availability-based resilience proxy, resource-constrained control selection, economic evaluation, and verification. Unlike approaches that examine these elements separately, the proposed framework treats them as interrelated stages of profile formation, assessment, and authorization without claiming that the resulting indicators constitute a universally validated methodology.

Materials and methods

This study is qualitative-analytical in nature and adopts a theoretical research design supported by formal mathematical modelling.

The empirical and documentary basis of the study consists of:

ND TZI 3.6-006-24, which establishes the procedure for selecting and tailoring information protection measures for information systems, and Resolution No. 712, which regulates the formation and application of basic, sectoral, and target profiles and security authorization (Administration of the SSSCIP, 2024; Cabinet of Ministers of Ukraine, 2025);

NIST SP 800-39, SP 800-37 Rev. 2, SP 800-53 Rev. 5, SP 800-53B, SP 800-53A Rev. 5, SP 800-30 Rev. 1, SP 800-160 Vol. 2 Rev. 1, the NIST IR 8286 series, and the NIST Cybersecurity Framework 2.0;

DSTU ISO/IEC 27001:2023, ISO 31000:2018, and ISO/IEC 27005:2022;

peer-reviewed scholarly publications on information security management, risk quantification, and cyber resilience.

The documentary sources were selected according to five criteria: current normative relevance; a direct relationship to security profiling or information-system protection; applicability to critical infrastructure or high-criticality systems; inclusion of procedures for selecting, tailoring, assessing, or authorizing controls; and methodological compatibility with a risk-oriented approach.

The following research methods were employed:

Historical-regulatory analysis was used to reconstruct the stages in the transformation of the Ukrainian framework for technical information protection between 2021 and 2026.

Comparative analysis was applied to relate the provisions of ND TZI 3.6-006-24 to NIST SP 800-53 and ISO/IEC 27001 across the following analytical categories: baseline requirements, tailoring, organization-defined parameters, documentation of deviations, control assessment, security authorization, and continuous monitoring.

Set-theoretic modelling was employed to formalize the security profile as a system of security and privacy requirements, selected protective measures, control enhancements, organization-defined parameters, and mappings to current threats and risks.

A two-state continuous-time Markov model was used to derive a simplified availability-based proxy for one dimension of cyber resilience in a protected system.

Binary mathematical programming was applied to formulate the selection of protective measures that minimizes residual risk under a budget constraint.

Methods of quantitative risk assessment, including annualized loss expectancy (ALE) and return on security investment (ROSI), were used to illustrate economic evaluation. These calculations are treated as parameter-dependent analytical models rather than empirical estimates for a specific system.

The unit of analysis is the security profile as a regulatory and mathematical object, characterized by its composition of protective measures, its mapping onto threats, its resilience indicators, and its cost of implementation.

Results

1. Stages in the Evolution of the Regulatory Framework for Security Profiling (2021–2026)

For analytical purposes, the development of the regulatory framework for security profiling in Ukraine is divided into three stages. The boundaries between the stages are defined by four criteria: the adoption of a significant regulatory instrument, a change in the object of regulation, a change in the principle used to select protective measures, and a change in the assessment or authorization mechanism.

Stage one: institutional preparation and wartime transition (2021–2022). This stage is interpreted as a preparatory and transitional period rather than as a formally codified stage of security-profile regulation. In 2021, regulatory and organizational preparation focused on updating approaches to comprehensive information protection and system criticality. After the introduction of martial law in 2022, the emphasis shifted toward continuity, operational resilience, and protection under rapidly changing threat conditions. Distinguishing these two contexts avoids attributing the legal regime of martial law to the whole 2021–2022 period.

Stage two: harmonization and European integration (2023). The adoption of DSTU ISO/IEC 27001:2023 made it possible to integrate international practices into the Ukrainian regulatory field (State Enterprise “UkrNDNC”, 2023). The development began of profiles that take into account not only technical measures but also organizational aspects, including the human factor and supply chains.

Stage three: implementation of the risk-oriented paradigm (2024–2026). ND TZI 3.6-006-24 established a procedure for selecting protective measures on the basis of information requirements, system characteristics, and security risks (Administration of the SSSCIP, 2024). Resolution No. 712 of 2025 complemented this procedure by defining the governance of basic, sectoral, and target

profiles and security authorization (Cabinet of Ministers of Ukraine, 2025). The two instruments should be read together but should not be treated as identical classifications.

Protective measures in the information systems of the Armed Forces of Ukraine are implemented within the information protection system in accordance with the criticality category of the information system, its structural and functional characteristics, the results of risk analysis, the technologies employed, and the specific features of its operation.

The process of selecting protective measures is of key importance for an organization and must ensure conformity with the mission, goals, and tasks of the military unit, as well as with the requirements of current legislation, regulatory documents, standards, and security and privacy policies. No universal set of measures capable of covering all aspects of security exists. A rational selection presupposes consideration of the context of use, the specific features of the information system's operation, its environment, and its needs. The effective determination of protective measures requires interaction with stakeholders and is oriented toward achieving an acceptable balance between ensuring the confidentiality, integrity, and availability of information and protecting personal data.

2. The Concept and Typology of Security Profiles

To unify approaches to the selection of protective measures, the concept of a security profile is employed: a coherent set of security and privacy requirements, selected measures, enhancements, parameters, and implementation conditions that reflects the organization's mission, the purpose and criticality of the system, and current risks. ND TZI 3.6-006-24 distinguishes four profile types—basic, sectoral, target, and adapted—whereas Resolution No. 712 regulates the governance relationship among basic, sectoral, and target profiles. Their interrelation is presented in Figure 1. Solid arrows show the principal sequence of profile specification; dashed arrows show that tailoring may be applied to the applicable basic, sectoral, or target profile for a particular system.

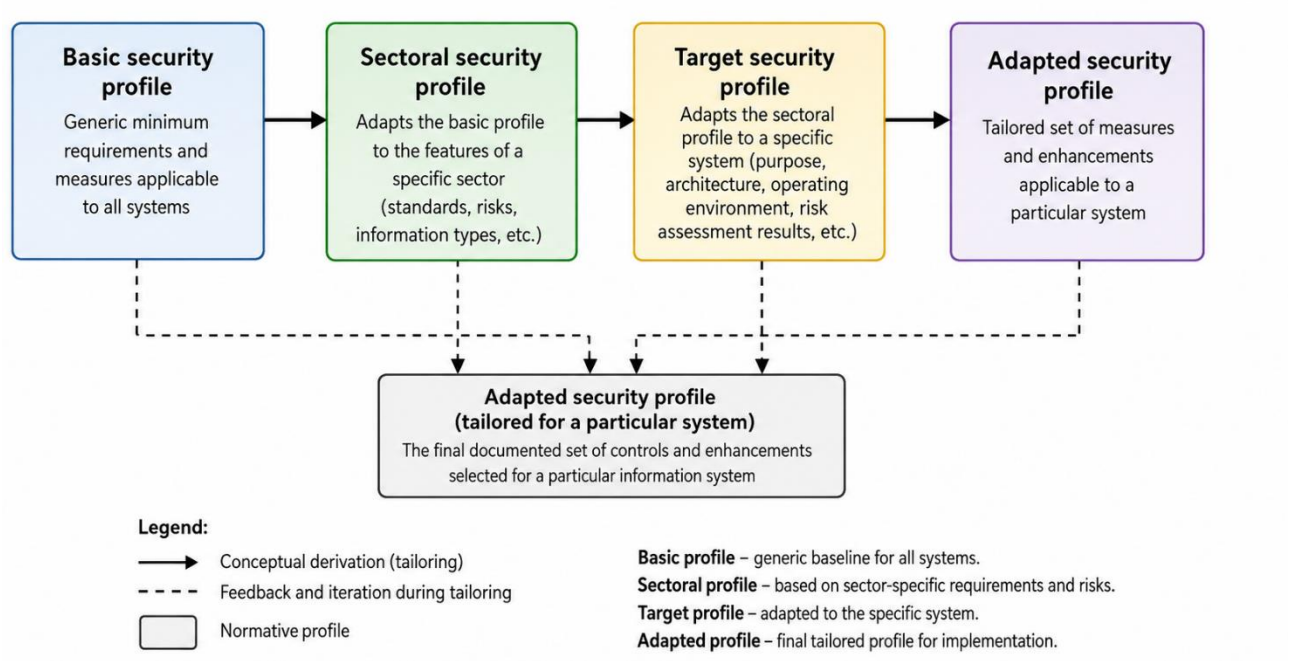

Figure 1: Types of security profiles and their interrelation
Source: Authors' Construct

The basic security profile of a system comprises the minimum information security requirements and an interrelated set of protective measures established depending on the

information processed in the system or its functional purpose. The basic profile establishes general minimum requirements for information protection applicable to all systems in which information is processed. It reflects the general principles, norms, and recommendations approved at the state level and serves as the basis for further elaboration.

The sectoral security profile of a system is an interrelated set of information protection measures defined for the system by the authorized sectoral body, taking into account the minimum requirements of the basic profile, the relevant standards and security policies, and the specific conditions of the system's operation (outside a zone of combat operations or within such a zone), together with the provision of corresponding recommendations. The sectoral profile adapts the basic profile to the specific features of operation and activity in a given sector, detailing protective measures with regard to sectoral risks, types of information, and technical particularities.

The target security profile of a system is an interrelated set of information protection measures defined by the owner or administrator of the system, taking into account the minimum requirements of the basic profile; the requirements of legislation and national standards in the fields of cryptographic and technical information protection and cyber defence; the regulatory documents of the system of technical and cryptographic information protection; the sectoral profile and applicable security policies; the purpose of the system, its structural and functional characteristics, and the specific features of its operation; and the results of the conducted security risk assessment.

The target profile is formed by the owner or administrator of the system and constitutes the concretization of the basic and sectoral profiles with respect to the particular system. It defines the list of security measures actually implemented, as well as the criteria for evaluating the conformity of the adopted measures with the security requirements. The target profile is developed for the specific system subject to security authorization; in the cases provided for by the sectoral profile, the target profile is agreed with the authorized sectoral body. The structure of the security profile is presented in Figure 2.

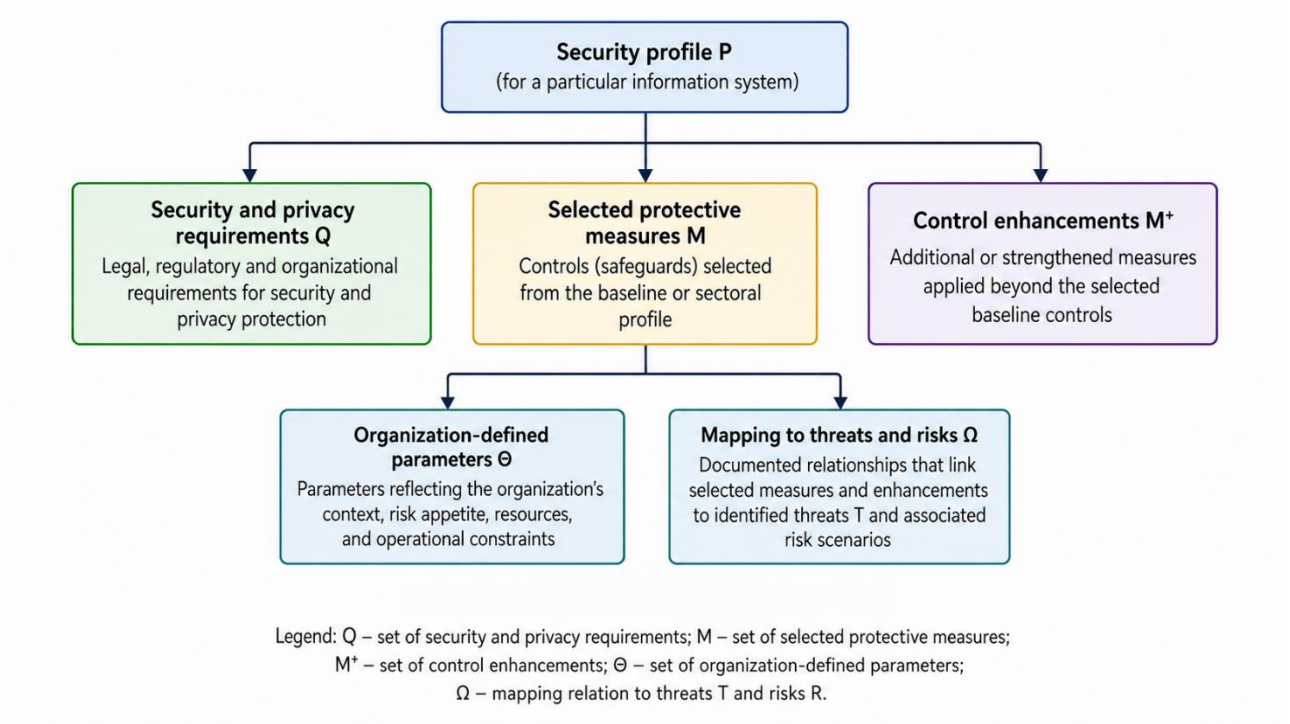

Figure 2: Structure of the security profile P
Source: Authors' Construct

The adapted security profile is produced by tailoring the applicable basic, sectoral, or target profile to the conditions of a particular information system. It records justified inclusions, exclusions,

parameter values, and refinements of protective measures on the basis of the system's purpose, architecture, operating environment, and assessed risks. Adaptation does not cancel mandatory legal requirements; each deviation must be documented and traceable to the risk assessment.

In accordance with ND TZI 3.6-006-24, protective measures are selected and adapted through a risk-oriented procedure. This is methodologically comparable to the tailoring of control baselines in NIST SP 800-53 Rev. 5, while the Ukrainian procedure retains the requirements of national legislation on technical and cryptographic information protection (Joint Task Force, 2020a; Administration of the SSSCIP, 2024).

3. A Formal Model of the Security Profile Structure

For the formal description used in this study, the security profile P is represented as:

$$P = \langle Q, M, M^{+}, \Theta, \Omega \rangle \quad (1)$$

where: Q – is the set of applicable security and privacy requirements;
M – is the set of selected protective measures (controls);
M^{+} – is the set of selected control enhancements;
Θ – is the set of organization-defined parameters;
T – is the set of identified threats and associated risk scenarios; $\Omega \subseteq (M \cup M^{+}) \cdot T$ is the documented relation that maps selected protective measures and enhancements to those threats and risk scenarios.

The threat set T is treated as an external input derived from the system risk assessment rather than as an internal component of the profile structure. For operational application, the model may be extended by an asset set A, a vulnerability set V, and a risk set R; these elements are not included in the minimal representation because the present study focuses on the internal structure of the profile rather than on a complete system-risk ontology.

Each threat or risk scenario $t_i \in T$ is characterized by a potential loss L_i and a probability of realization p_i. The term p_iL_i represents the baseline expected loss of scenario i, with p_i incorporating the event and conditional probabilities defined by the adopted risk model. The effectiveness of profile E(P) is defined as the capacity of the measures selected in the profile to reduce risk:

$$E(P) = [\Sigma_i\, p_iL_i\alpha_i(P)] / [\Sigma_i\, p_iL_i] \quad (2)$$

where $\alpha_i(P) \in [0, 1]$ is the empirically estimated aggregate reduction in expected loss for threat t_i achieved by the measures included in profile P. The normalized indicator $E(P) \in [0, 1]$ expresses the proportion of baseline expected loss mitigated by the profile. It assumes that interactions among measures have already been reflected in $\alpha_i(P)$; otherwise, a model with measure-specific coefficients and interaction terms is required. The formulation also assumes that the risk scenarios are defined so as to avoid double-counting strongly dependent losses.

5. A Simplified Availability-Based Proxy for Profile Resilience

Cyber resilience may be analysed through stochastic state-transition models (Linkov et al., 2013; Gisladottir et al., 2017; Ross et al., 2021). For a deliberately simplified two-state continuous-time Markov model, let S_o denote a secure/operational state and S_1 a non-operational state encompassing compromise and recovery. The compromise intensity λ reflects the rate of transitions from S_o to S_1, while the recovery intensity μ reflects transitions from S_1 to S_o. Under constant transition rates, the stationary probability of the secure state is:

$$\pi_o = \mu / (\lambda + \mu) \quad (3)$$

The value π_o should be interpreted as a simplified availability-like resilience proxy for the stated two-state assumptions, not as a universal regulatory protection coefficient. ND TZI 3.6-006-

24 does not establish a general threshold of 0.999 for this indicator; any threshold must therefore be justified for the particular system and service requirement.

6. Optimization of the Selection of Protective Measures

Let $x_j \in \{0, 1\}$ indicate whether protective measure j is selected, c_j be its implementation cost, and $\alpha_{ij} \in [0, 1]$ be its estimated effectiveness against threat i. A localized binary linear formulation that minimizes expected residual loss under budget B is:

$$\min_x \ \Sigma_i \, p_i L_i (1 - \Sigma_j \, \alpha_{ij} x_j) \tag{4}$$

$$\text{subject to } \Sigma_j \, c_j x_j \le B,$$
$$\Sigma_j \, \alpha_{ij} x_j \le 1, \text{ for all i},$$
$$x_j \in \{0, 1\}, \text{ for all j}.$$

Here $p_i L_i$ is the expected loss associated with threat i before additional measures are selected. The constraint $\Sigma_j \, \alpha_{ij} x_j \le 1$ prevents the linear approximation from implying more than complete risk reduction. The model assumes additive marginal effects and no double-counting, incompatibility, or synergy among controls. Practical application may require mandatory-control constraints, logical dependencies, incompatibility constraints, minimum coverage of critical threats, lifecycle costs, and personnel or implementation-time limits. A multiplicative residual-risk form, $p_i L_i \prod_j (1 - \alpha_{ij} x_j)$, avoids additive overstatement but produces a nonlinear optimization problem (Yevseyeva et al., 2015).

7. Economic Evaluation: Quantitative Risk Assessment and Return on Security Investment

For an illustrative calculation of annualized loss expectancy (ALE), the following traditional quantitative-risk expression is used (Hubbard & Seiersen, 2016; Bojanc et al., 2012):

$$ALE = AV \cdot EF \cdot ARO \tag{5}$$

where:
- AV (asset value) – is the value of the asset, including data, reputation, and potential penalties;
- EF (exposure factor) – is the percentage of the asset lost in the event of a successful attack;
- ARO (annualized rate of occurrence) – is the expected frequency of attacks per year.

For a screening-level comparison of the expected benefit and cost of a security investment, the return-on-security-investment indicator is applied (Cavusoglu et al., 2004; Sonnenreich et al., 2006):

$$ROSI = (R \cdot \rho_p - C_{total}) / C_{total} \tag{6}$$

where:
- R – is the monetary value of the risk (ALE);
- ρ_p – is the proportion of baseline risk eliminated by profile P; where the same loss basis and calibration are used, ρ_p may be operationalized by the normalized indicator E(P);
- C_{total} – is the total cost of ownership (TCO) of the protection system.

In Equation (6), ROSI is a dimensionless relative return: ROSI > 0 indicates that the estimated avoided loss exceeds the total cost of ownership, whereas ROSI < 0 indicates the opposite. The monetary net benefit may additionally be reported as $R \cdot \rho_p - C_{total}$. Because R and ρ_p are uncertain, both indicators should be accompanied by sensitivity or scenario analysis rather than interpreted as precise forecasts (Sonnenreich et al., 2006).

8. Verification of the Security Profile

Verification of a target or adapted security profile should demonstrate that the selected measures are implemented as specified. In this study, verification means confirmation of

implementation against stated requirements; validation means confirmation that the profile is suitable for the actual threat and operating context; assessment means the systematic examination, interview, and testing of controls; and authorization means the accountable management decision to accept residual risk and permit operation. Depending on the applicable profile, system criticality, and risk assessment, evidence may include documentation review, examination, interviews, technical tests, vulnerability analysis, penetration testing, and developer evidence. These activities support security authorization and continuous monitoring; penetration testing and source-code review should not be described as universally mandatory unless the applicable profile explicitly selects them (Joint Task Force, 2018, 2022; Dempsey et al., 2011; Nelson et al., 2025). A proportionate four-part verification structure is:

implementation verification: examination, interviews, and testing against the selected control requirements and organization-defined parameters;

technical validation: vulnerability analysis, penetration testing, resilience exercises, or simulation where justified by the profile and risk assessment;

evidence review: assessment of implementation records, configuration, developer evidence, and operational processes where applicable;

authorization and monitoring: documented assessment of conformity with the target or adapted profile, followed by risk acceptance and continuous monitoring.

Discussion

The findings of this study indicate that the transformation of the Ukrainian regulatory framework for technical information protection between 2021 and 2026 should not be interpreted as a mere accumulation of new documents. Rather, it represents a paradigmatic transition from rigid, template-based protection models toward flexible, risk-oriented security profiles.

First, the introduction of the concept of criticality during the transitional period of 2021–2022 prepared the conceptual ground for differentiated protection requirements, while the adoption of DSTU ISO/IEC 27001:2023 institutionalized the connection between Ukrainian regulation and international information security management practice (State Enterprise “UkrNDNC”, 2023).

Second, ND TZI 3.6-006-24 supports a dynamic, risk-oriented representation of the security profile through requirements, measures, enhancements, parameters, and documented mappings to threats and risks. This representation is methodologically comparable with the tailoring approach of NIST SP 800-53 Rev. 5 and can improve interoperability of assessment practices, but it does not establish automatic mutual recognition between Ukrainian and foreign authorization regimes (Joint Task Force, 2020a; Administration of the SSSCIP, 2024).

Third, the integrated mathematical apparatus converts selected expert assumptions into parameter-dependent indicators. The threat-coverage measure, the two-state Markov resilience proxy, the budget-constrained optimization problem, and the ALE and ROSI indicators can support transparent comparison of alternatives. Their outputs remain conditional on the quality of estimates for threat frequency, loss, recovery, and control effectiveness and should therefore be accompanied by sensitivity analysis (Gordon & Loeb, 2002; Wang et al., 2020; NIST, 2025a, 2025b, 2025c).

At the same time, the proposed models should be regarded as a theoretical foundation rather than a complete methodology. Their practical application requires calibrated input data on threat probabilities, losses, and countermeasure effectiveness, the collection of which constitutes a separate methodological task, particularly under wartime conditions. In comparison with the NIST Risk Management Framework, the proposed framework does not replace system categorization, control selection, assessment, authorization, or monitoring; rather, it supplies optional analytical instruments for comparing control configurations within those governance stages. Its practical

contribution for Ukrainian authorities and critical-infrastructure operators lies in making assumptions, resource constraints, and residual-risk trade-offs explicit. At the same time, quantitative formalization may create an illusion of objectivity when threat probabilities, loss estimates, and control-effectiveness coefficients are weakly supported. Accordingly, expert elicitation, parameter validation, uncertainty ranges, and periodic recalibration are integral conditions of responsible use.

Limitations

This study has several limitations.

First, it relies primarily on regulatory documents, international standards, and academic publications. The formally prescribed provisions of the analysed documents may not fully correspond to actual administrative and technical practice in specific organizations.

Second, the numerical parameters of the proposed models, including threat probabilities, loss estimates, and countermeasure effectiveness coefficients, are treated analytically and are not calibrated against empirical incident data. The collection and validation of such data for the systems of the security and defence sector constitute a separate research task.

Third, the Markov model uses only two states and constant transition intensities. Real systems may require additional degraded or attack states, non-exponential transition distributions, time-varying rates, or semi-Markov formulations.

Fourth, the study does not include an empirical case study of the application of the proposed apparatus to a specific critical infrastructure facility. Incorporating such a case study would strengthen the empirical validation of the study's conclusions. Fifth, the framework does not explicitly model adversarial adaptation or strategic attacker behaviour; consequently, control-effectiveness estimates require periodic reassessment as threat actors modify their tactics, techniques, and procedures.

Conclusions

The evolution of the Ukrainian regulatory framework for technical information protection between 2021 and 2026 can be represented through three stages: institutional preparation in 2021 and wartime transition in 2022; harmonization with international standards in 2023; and implementation of a risk-oriented paradigm through ND TZI 3.6-006-24 in 2024 and Resolution No. 712 in 2025.

ND TZI 3.6-006-24 distinguishes four profile types—basic, sectoral, target, and adapted—while Resolution No. 712 regulates the governance of basic, sectoral, and target profiles and security authorization. For analytical purposes, a profile is represented as a combination of security and privacy requirements, selected measures, enhancements, organization-defined parameters, and mappings to current threats and risks. This representation is compatible at the methodological level with the tailoring logic of NIST SP 800-53 Rev. 5.

The principal theoretical result is an integrated analytical framework that links the regulatory structure of a security profile with normalized threat-coverage assessment, an availability-based resilience proxy, resource-constrained control selection, economic evaluation, verification, and authorization. The methodological result is the explicit formulation of assumptions, variables, constraints, and interpretation limits for each component. The practical value lies in improving the transparency and traceability of technical and budgetary decisions. The proposed indicators are not universal measures of protection: their validity depends on empirical calibration, documented assumptions, uncertainty analysis, and sensitivity testing for the particular information system.

Future research will be directed toward the development of methodologies for assessing the risks associated with individual protective measures and for the verification of security profiles, as

well as toward the empirical calibration of the proposed models using incident data from critical infrastructure systems.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

Use of Artificial Intelligence

Artificial intelligence was used for language editing, translation, and technical verification of the manuscript.

References

Administration of the State Service of Special Communications and Information Protection of Ukraine. (2024). *ND TZI 3.6-006-24: Procedure for selecting measures to protect information, the protection requirement for which is established by law and which does not constitute a state secret, for information systems* [In Ukrainian; author's translation]. https://cip.gov.ua/services/cm/api/attachment/download?id=66109

Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management, 48*(6), 1031–1052. https://doi.org/10.1016/j.ipm.2012.01.001

Cabinet of Ministers of Ukraine. (2025). *Resolution No. 712 of June 18, 2025* [In Ukrainian]. https://zakon.rada.gov.ua/go/712-2025-%D0%BF

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87–92. https://doi.org/10.1145/1005817.1005828

Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations* (NIST SP 800-137). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over- and underregulation. *Risk Analysis, 37*(9), 1644–1651. https://doi.org/10.1111/risa.12729

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457. https://doi.org/10.1145/581271.581274

Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Wiley.

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal, 4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines*.

International Organization for Standardization. (2022). *ISO/IEC 27005:2022 information security, cybersecurity and privacy protection—Guidance on managing information security risks*.

Joint Task Force. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST SP 800-37 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

Joint Task Force. (2020a). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Joint Task Force. (2020b). *Control baselines for information systems and organizations* (NIST SP 800-53B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53B

Joint Task Force. (2022). *Assessing security and privacy controls in information systems and organizations* (NIST SP 800-53A Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53Ar5

Joint Task Force Transformation Initiative. (2011). *Managing information security risk: Organization, mission, and information system view* (NIST SP 800-39). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-39

Kott, A., & Linkov, I. (Eds.). (2019). *Cyber resilience of systems and networks*. Springer. https://doi.org/10.1007/978-3-319-77492-3

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST SP 800-30 Rev. 1). https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology. (2025a). *Integrating cybersecurity and enterprise risk management* (NIST IR 8286 Rev. 1). https://doi.org/10.6028/NIST.IR.8286r1

National Institute of Standards and Technology. (2025b). *Identifying and estimating cybersecurity risk for enterprise risk management* (NIST IR 8286A Rev. 1). https://doi.org/10.6028/NIST.IR.8286Ar1

National Institute of Standards and Technology. (2025c). *Staging cybersecurity risks for enterprise risk management and governance oversight* (NIST IR 8286C Rev. 1). https://doi.org/10.6028/NIST.IR.8286Cr1

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST SP 800-160 Vol. 2 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)—A practical quantitative model. *Journal of Research and Practice in Information Technology, 38*(1), 45–56. https://doi.org/10.3316/informit.937199632104879

State Enterprise "UkrNDNC." (2023). *DSTU ISO/IEC 27001:2023 information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC 27001:2022, IDT)* [In Ukrainian].

Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security, 89*, Article 101659. https://doi.org/10.1016/j.cose.2019.101659

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the ground up*. Syngress.

Yevseyeva, I., Basto-Fernandes, V., Emmerich, M., & van Moorsel, A. (2015). Selecting optimal subset of security controls. *Procedia Computer Science, 64*, 1035–1042. https://doi.org/10.1016/j.procs.2015.08.625