

Technical Protection Measures in Information Security Systems in Organizations

Pavlin Kutinchev

*Institute of Information and Communication Technologies,
Bulgarian Academy of Sciences, Sofia, Bulgaria
Email: kutinchev@gmail.com*

Abstract: Modern organizations rely on information assets, which form the foundation for all other assets and are among the most vulnerable to attacks. This article proposes a lightweight and traceable procedure for the preliminary selection of security measures. A simplified selection method is presented, linking three elements that are typically considered separately: organizational roles and communication flows, data states (at rest, in motion, or in use), and available technical controls. Sensitive data are identified in relation to roles and communication channels; threats are mapped to data states; and each potential control mechanism is characterized by just two relative parameters: effectiveness and cost. A multiplicative residual risk model and a cost-effectiveness ratio are used to rank the controls. This renders the calculations transparent and reproducible, without requiring the detailed quantitative data that most organizations do not maintain. An illustrative example, involving six widely used controls, demonstrates a reduction in residual risk from 100% to 31.8%. The point of diminishing returns is also identified: the four primary controls deliver approximately 90% of the achievable risk reduction at roughly half the total cost. The same approach is applied to compare traditional controls with innovative trends.

Keywords: *cost-effectiveness analysis, data classification, information security system, residual risk, risk assessment, technical security controls.*

1. Introduction

Modern organizations are complex systems characterized by technological, economic, scientific, legal, and human factors. Regardless of their size, geographic location, or the sector in which they operate, organizations rely heavily on the assets at their disposal - human, technological, production, informational,

and financial. Information assets hold a particularly significant position - they provide the infrastructure used by all other assets and are directly involved in business processes. At the same time, they are among the most vulnerable assets, and their compromise can jeopardize the operations of the entire organization. Therefore, it is crucial to protect these assets from attacks.

In this article we consider technical means to protect the information assets of modern organizations, which at a later stage can be used to design an information security system (ISS) in the organization [1], [2]. The primary threats to organizations are cyber threats, such as data leaks, or attacks against services and information systems. Although organizations have access to a vast array of technical security solutions, including access controls, cryptography, intrusion detection systems (IDS), intrusion prevention systems (IPS), and data loss prevention (DLP) solutions, the main challenge lies in selecting the right ones. This is because no organization possesses unlimited financial or human resources. Consequently, a proper risk analysis must be conducted, taking into account the assets that require protection and the resources necessary to secure them.

Current economic models link investments in security to vulnerability and potential losses [3], while established guidelines provide a structure for risk identification and assessment processes [4]. The proposed procedure employs a simpler, explicitly relative index, which renders the underlying assumptions and calculations transparent and verifiable. It does not assess the monetary return on investment, nor does it claim superiority over the aforementioned approaches.

The article proposes a lightweight and traceable procedure for preliminary selection of security measures. It is based on three components that are typically considered separately: communication flows within the organization, the state of the data and the available technical resources. Each technical security measure is evaluated based on two parameters: effectiveness and cost, which facilitates prioritization while minimizing operational and maintenance resource requirements. The article examines roles, communication, and data classification within the organization, as well as the proposed method for selecting technical security measures. It covers both traditional and innovative technical measures, while also addressing economic, organizational, and regulatory aspects. The intended contribution is an operational workflow rather than a new probability model or a substitute for comprehensive risk management.

2. Roles, Communication, and Data Classification

Every modern organization is characterized by a specific business model. This model defines its operations, structure, communication, and assets, as well as the necessary financial and human resources. A manufacturing enterprise may serve as an example. Such enterprises are characterized by complex processes, including design, production, storage, sales, and transport. These processes are managed by

the administration, accounting, and human resources (HR) departments, in compliance with the regulatory and legal requirements dictated by the specific nature of the organization's activities.

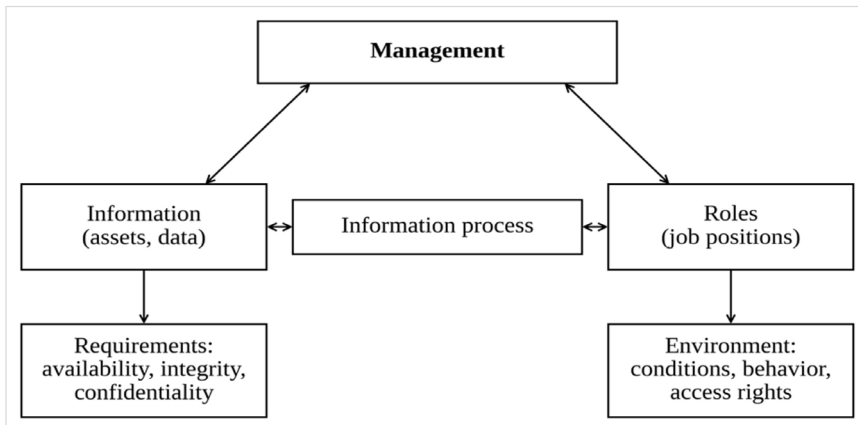


Fig. 1. Business model of the organization: relation between information, roles and management

Figure 1 illustrates a conceptual business model for an organization, integrating information processes, professional roles (management, engineers, technologists, sales personnel, and administration), and the surrounding environment, which encompasses production conditions, the regulatory framework, market conditions, and more. Tasks and the oversight of roles within an organization are managed by the leadership. This management is structured across various levels, ranging from operational and intermediate to senior (executive) levels. To fulfill their duties, individuals in each role utilize different forms of communication: electronic, written, or oral. The presence of communication indicates the existence of an information process. This process encompasses the creation, processing, utilization, and exchange of information—both within the organization and externally. It is precisely this process that an information security system is designed to protect.

Communication within an organization can be classified based on three main characteristics. In terms of direction relative to the organizational hierarchy, it is defined as either horizontal or vertical. Depending on the environment in which it takes place, it is divided into internal and external communication. Based on the nature of the data being transmitted, it can be classified as either routine or sensitive. Horizontal communication encompasses the daily exchange between employees within one or more units. Vertical communication connects management with subordinates and individual units; as a rule, this channel conveys data with a higher degree of sensitivity. Both types of data are found in both internal and external communication.

Sensitive data refer to information whose leakage could lead to dire consequences for an organization, such as loss of reputation or competitiveness, legal sanctions, or operational disruption. Ordinary data, by contrast, consist of information used in day-to-day communication, the loss of which would not cause serious issues. Each organization determines for itself which data are critical and which are not. This determination depends on the nature of its operations, the regulatory requirements it must comply with, and its existing knowledge and experience. Such classification forms the foundation for effective information protection. Without prior classification, an organization risks either overly restricting data access and flow, potentially disrupting workflows or leaving critical data insufficiently protected [1], [2].

In addition to their level of sensitivity, data are also classified according to their processing state. A distinction is made between data at rest, data in motion, and data in use. This classification has direct technological implications, as each of these states requires different protection measures (Table 1).

Table 1. Data states, characteristic threats and priority technical measures

Data state	Typical examples	Main threats	Priority measures
Data at rest	file servers, databases, archives, mobile media	unauthorized access, theft of media, ransomware	media encryption, access control, backup
Data in motion	e-mail, exchange with counterparties, remote access	eavesdropping, tampering, man-in-the-middle	TLS, VPN, digital signature, PKI
Data in use	documents opened on the workstation, reports, queries	leakage through endpoints, insider misuse	DLP, rights management, logging and audit

Once sensitive data have been defined and their states identified, the question remains: how should they be protected? The following section addresses this question.

3. Method for Selecting Technical Measures

The proposed method consists of five steps and is designed to be carried out by a small team within a short timeframe (Fig. 2):

1. Description of roles and communication flows within the organization, and identification of sensitive data associated with each role.
2. Identification of relevant threats and vulnerabilities for each state of the data.
3. Assessment of risk on a relative scale.

4. Selection of appropriate protective measures, with each evaluated based on effectiveness and cost.
5. Calculation of residual risk, with the results subject to periodic review.

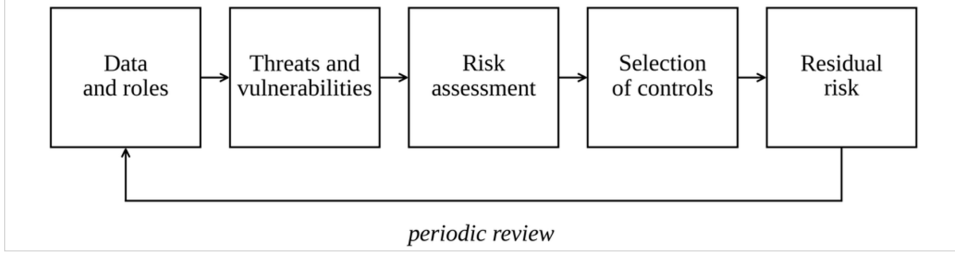


Fig. 2. Steps of the procedure for selecting technical measures

The method follows the general logic of the risk management process described in ISO/IEC 27005 [5], but deliberately restricts the required input to relative estimates. The risk to an individual asset or data flow can be represented as the product of probability and impact:

$$R_i = P_i I_i \quad (1)$$

where P_i is the relative probability that the threat will materialize, and I_i is the relative impact on the organization. Both variables are determined using a simple three or five-point scale. The goal is not to achieve absolute precision, but rather to ensure comparability between different risks.

Implementing a technical measure does not eliminate risk, it reduces it. If a given measure j has a relative effectiveness $e_j \in [0, 1]$ with respect to a specific risk, the residual risk following its implementation is:

$$R_{res} = R_i (1 - e_j) \quad (2)$$

When multiple independent measures are applied to the same risk, their effects accumulate multiplicatively:

$$R_{res} = R_i \prod_j (1 - e_j) \quad (3)$$

The multiplicative form was chosen over the additive one quite deliberately. It reflects the practical observation that each subsequent protective measure acts upon a risk that has already been reduced, and therefore makes a smaller absolute contribution. This also represents a mathematical expression of the law of diminishing returns in the realm of security.

The ratio between the achieved risk reduction and the costs of a given measure is used to prioritize the measures:

$$CE_j = \Delta R_j / C_j \quad (4)$$

where C_j represents the relative costs of implementing and maintaining the measure, expressed in terms of a common conventional unit, and $\Delta R_j = R_{\text{res},j-1} - R_{\text{res},j}$ is the reduction of the residual risk obtained by that measure.

Since $\Delta R_j = R_{\text{res},j-1} e_j$, the value of (4) depends on how much risk has already been removed by the preceding measures. For ranking purposes the ratio is therefore evaluated at a common baseline, which is equivalent to ordering the measures by e_j / C_j . This quantity is independent of the order of application.

The measures are ranked in descending order of their e_j/C_j value and implemented sequentially until the residual risk reaches a level acceptable to management, or until the budget is exhausted.

The four relationships (1) – (4) constitute the entire computational framework of the method. No additional formalization has been introduced, by design, to ensure that the procedure can be applied without specialized software and without requiring data that the organization does not already possess [3], [4].

4. Technical Protection Measures

4.1. Traditional Measures

The technical security measures used in modern organizations can be divided into five main categories. The first category includes access control systems. These employ various methods to verify identity and determine user rights. Examples include multi-factor authentication (MFA), biometric solutions, and smart cards. Their purpose is to ensure that access to sensitive information is restricted solely to authorized individuals.

The second category covers network firewalls as well as intrusion detection and prevention systems (IDS/IPS). They monitor network traffic, detect suspicious activity and block unauthorized access attempts.

The third category includes cryptographic tools for information security. It covers data protection technologies, covering both "Data at rest" and "Data in motion", such as AES and Transport Layer Security (TLS), as well as electronic signatures and public key infrastructure (PKI). These tools help prevent eavesdropping, unauthorized access and manipulation of data.

The fourth category includes data backup and recovery systems. These measures help an organization continue its operations following an incident or technical issue. The absence of a verified recovery plan can lead to significant financial losses, particularly after attacks involving malicious software that blocks access to data and demands a ransom (ransomware) [6].

The fifth category encompasses antivirus software and other tools for protection against malicious software. While these constitute a fundamental element of security, modern solutions also employ more advanced methods, such

as machine learning and behavioral analysis, to detect even previously unknown threats [7].

Data Loss Prevention (DLP) systems should be added to these categories. They monitor how data are used and restrict their unauthorized copying, transmission, or sharing. This is particularly important when dealing with data that are already accessible to, or being processed by, users. In this area, traditional network defenses and encryption alone do not provide sufficient protection [1].

4.2. Innovative Trends

Technological development is transforming both the security tools employed and the way organizations manage risk. Rather than relying solely on pre-configured protective mechanisms, they are increasingly utilizing systems that adapt to emerging threats. The six trends characterizing this shift are summarized in Table 2, along with their level of development and their impact on the risk remaining after the implementation of protective measures.

Artificial intelligence and machine learning are used to detect unusual activity in network traffic, identify phishing attacks, and predict potential actions by attackers. Unlike systems that follow pre-set rules, these technologies analyze data and are capable of recognizing new patterns of behavior [7].

Table 2. Innovative trends and their role in the protection system

Trends	Main effect on protection	Maturity
Artificial intelligence and machine learning	detection of anomalies and unknown threats, shorter reaction time	deployed
Zero Trust architectures	removal of the assumption of a trusted internal network; every request is validated	deployed
Cloud security	separation of provider–customer responsibilities, encryption and monitoring	deployed
Automation and SOAR	automated detection – analysis – response cycle, relief for the teams	in progress
IoT and 5G security	reduction of the attack surface with a large number of endpoints	in progress
Post-quantum cryptography	resilience of cryptography against quantum computation	standardization

The "Zero Trust" model is based on the principle that no request should be considered safe simply because it originates from the internal network. Every access request is verified, which helps to limit threats arising from within [8].

The use of cloud services introduces specific risks related to the distribution of responsibilities between the provider and the client, as well as the management of access to data and systems [9].

SOAR platforms automate specific stages of security operations, including threat detection, analysis, and incident response. At the same time, the proliferation of Internet of Things (IoT) devices and 5G networks increases the number of potential entry points for attacks. According to the ENISA Threat Landscape report, a substantial share of the IoT devices deployed in Europe lack basic protective measures and are therefore exposed to high risk [6].

Quantum computers pose a long-term challenge to some of the cryptographic algorithms used today. As a result, standards for post-quantum cryptography are already being developed and adopted, designed to provide protection against the future capabilities of these computers [10].

It is important to emphasize that new technologies do not replace traditional security measures, but complement them. For example, implementing a SIEM/SOAR platform in an organization that does not have effective access controls and clear data protection policies will not solve the underlying security problems. New tools are most effective when used in conjunction with solid baseline measures and well-organized processes. Otherwise, costs can be high without achieving significant risk reduction. This finding will also be addressed quantitatively in the next section.

5. Illustrative Example

To demonstrate how the method works, we consider a hypothetical medium-sized organization with approximately 150 workstations, which carries out both administrative and production activities and exchanges data with external counterparties. It is assumed that the initial risk, calculated according to (1) and normalized against the worst-case scenario, amounts to 100%. Six measures have been evaluated in terms of their effectiveness and relative costs, on the basis of expert judgment; the values are illustrative and are not derived from a specific empirical data set (Table 3).

Table 3. Input parameters of the illustrative example

Measure	Main threats covered	Effectiveness, e_j	Cost, C_j
MFA	compromised passwords, unauthorized access	0.30	6
Encryption	theft of media, eavesdropping in transit	0.22	9
IDS/IPS	network intrusions, malicious traffic	0.20	12
Backup	ransomware, data loss, hardware failure	0.12	8
DLP	leakage of data in use, insider threat	0.10	14
SIEM/SOAR	slow detection, uncoordinated response	0.08	20

The sequential application of (3), ordered by decreasing CE value, results in the residual risk trajectory shown in Fig. 3. After the first measure, the risk drops to 70%; after the second, to 54.6%; and after the sixth, to 31.8%. The total reduction is 68.2 percentage points, at a total cost of 69 arbitrary units.

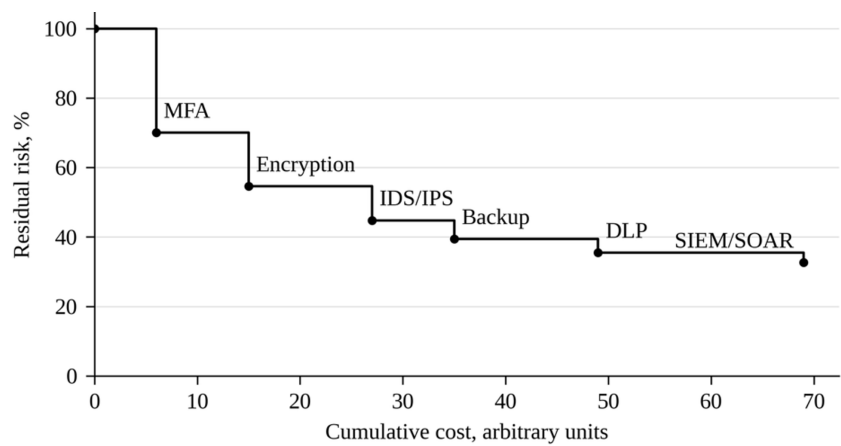


Fig. 3. Residual risk as a function of the cumulative protection cost

The main practical conclusion is evident from the shape of the curve. The first four measures: multi-factor authentication (MFA), encryption, intrusion detection and prevention systems (IDS/IPS), and backup, account for 35 units of cost (i.e., 51% of the total expenditure) but deliver 61.6 out of the total 68.2 percentage points of reduction, representing approximately 90% of the overall impact achieved. The last two measures consume nearly half the budget yet yield less than 10% of the additional benefit. This does not mean that DLP and SIEM/SOAR are superfluous - they address specific threats not covered by the other measures – but rather that their implementation is justified only after the core measures have been put in place.

The same conclusion follows directly from indicator (4). In Fig. 4, the measures are ranked according to the reduction in risk per unit of expenditure. The difference between the first and last measures is more than twelve-fold, making the implementation sequence more important than the actual selection of measures.

The values in Table 3 are illustrative and may be replaced by values, specific to the respective organization. The result that matters for practice is nevertheless robust: when the effectiveness values are varied by $\pm 20\%$, the four baseline measures remain separated from DLP and SIEM/SOAR, even though the order within each of the two groups may change. It is this separation, rather than the accuracy of the individual values, that determines the practical value of the approach.

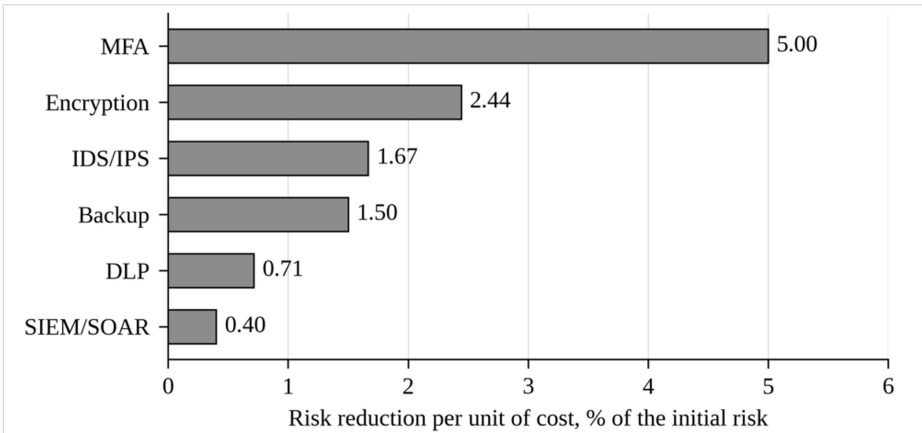


Fig. 4. Effectiveness-to-cost ratio by measure

6. Discussion

The implementation of technical security solutions within an organization does not depend solely on their technical specifications; it also encompasses economic, organizational, legal, and ethical aspects.

An economic assessment requires a consistent time horizon covering the entire life cycle, as well as the inclusion of costs related to personnel, integration, training, licenses, maintenance, and operational disruptions. Although automation may lead to a reallocation of tasks, the example under consideration provides no evidence that it necessarily reduces total operating costs. Priority should not be given to technologies in the absence of appropriate scenarios and well-substantiated estimates of their benefits [3].

Certain solutions, such as quantum cryptography and blockchain infrastructure, require significant initial investments and are planned with a long-term horizon. In contrast, solutions based on artificial intelligence can reduce ongoing costs by automating monitoring and analysis. In the context of the Internet of Things (IoT), the primary challenge relates to the vast number of devices. Although an individual device may be inexpensive, the costs associated with updates, maintenance, and access control increase significantly when dealing with thousands of such devices.

From an organizational perspective, new technologies necessitate changes in work culture and the distribution of responsibilities. As analytical tasks and decision-making are increasingly delegated to algorithms, the question arises: who bears responsibility if an automated system makes a mistake? Consequently, it is essential that the decisions generated by these systems be explainable and understandable.

Automation also alters the skill requirements for employees. The need for continuous process monitoring is diminishing, while the demand for specialists in system security and data management is growing.

From a regulatory standpoint, the NIS2 Directive (2022) [11] introduces stricter requirements for organizations operating in critical sectors. The General Data Protection Regulation (GDPR) [12] establishes the rules for processing personal information. Thus, security ceases to be merely a technical matter; it requires clear rules, sound organization, and commitment at all levels within an organization.

Compliance with the requirements of ISO/IEC 27001 [13] and NIST SP 800-53 [14] is one of the most direct ways for an organization to demonstrate that it implements good practices for information security, and the NIST Cybersecurity Framework 2.0 [15] provides a complementary high-level structure for this purpose. The proposed procedure can assist in identifying the most critical measures; however, it does not replace these standards and guidelines, nor does it serve as an alternative to them.

Finally, the procedure encompasses only technical controls, while a significant portion of the residual risk is borne by individuals. Empirical assessments of cybersecurity readiness among educators [16], as well as awareness among parents [17], indicate that a certain level of competence among the general public cannot be taken for granted; this level can be measured using tools similar to those employed in the present analysis. Similar variations are observed regarding skills in using artificial intelligence (AI)-based tools, as well as attitudes toward them [18] – an aspect relevant to the implementation of the adaptive controls discussed in Section 4.2. For an organization, this means that a given control measure, such as multi-factor authentication (MFA) or data loss prevention (DLP) achieves its nominal effectiveness e_j only to the extent that the employees operating within that system understand and accept it; otherwise, the actual effectiveness achieved is lower.

The proposed approach has two main limitations. First, the cost-effectiveness assessments are based on expert judgment. Consequently, they cannot be directly applied across different organizations without accounting for their specific characteristics. Second, the model treats security measures as independent of one another. In practice, however, they are often interconnected. For instance, the effectiveness of a SIEM system (a platform for collecting and analyzing security events) depends on the completeness and quality of the data it receives from other systems. Therefore, the next step in the development of this approach is to account for these interdependencies.

7. Conclusion

The article proposes a simplified, practical procedure linking organizational roles, communication flows, and data states to the selection of technical security controls. The contribution of the procedure lies in a traceable workflow with explicitly formulated assumptions, rather than in novelty regarding probability, the product of probability and impact, or the multiplicative expression. Each security measure is described using two relative parameters, and the computational model involves only four relationships. This allows the method to be applied without specialized software and without the need for precise data—the kind that most organizations do not maintain.

The illustrative example demonstrates how this procedure identifies the point of diminishing returns. Given the assumed values, the four primary control measures account for approximately 90% of the achievable reduction, while their associated costs amount to about half of the total expenditure. This figure is specific to this particular example, rather than being representative of organizations in general.

Innovative approaches build upon this layer but do not replace it. Consequently, the key practical takeaway is that the sequence of implementation is more important than the choice between specific products.

Future work includes accounting for the interdependencies between individual measures, validating relative estimates based on real-world data from Bulgarian organizations, and expanding the model to incorporate organizational and procedural measures alongside technical ones.

References

1. Gaidarski, I.: Model driven development of information security system. *Problems of Engineering Cybernetics and Robotics*, 76, 47–62 (2021). <https://doi.org/10.7546/PECR.76.21.04>.
2. Gaidarski, I., Kutinchev, P.: Some aspects of information security and cybersecurity problem area. *Problems of Engineering Cybernetics and Robotics*, 79, 55–66 (2023). <https://doi.org/10.7546/PECR.79.23.03>.
3. Gordon, L.A., Loeb, M.P.: The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457 (2002). <https://doi.org/10.1145/581271.581274>.
4. Joint Task Force Transformation Initiative: Guide for Conducting Risk Assessments. NIST SP 800-30, Rev. 1. National Institute of Standards and Technology, Gaithersburg (2012). <https://doi.org/10.6028/NIST.SP.800-30r1>.
5. ISO/IEC: ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO, Geneva (2022).
6. ENISA: ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, Athens (2023). <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>, last accessed 2026/10/20.

7. Buczak, A.L., Guven, E.: A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176 (2016). <https://doi.org/10.1109/COMST.2015.2494502>.
8. Rose, S., Borchert, O., Mitchell, S., Connelly, S.: *Zero Trust Architecture*. NIST SP 800-207. National Institute of Standards and Technology, Gaithersburg (2020). <https://doi.org/10.6028/NIST.SP.800-207>.
9. Jansen, W., Grance, T.: *Guidelines on Security and Privacy in Public Cloud Computing*. NIST SP 800-144. National Institute of Standards and Technology, Gaithersburg (2011). <https://doi.org/10.6028/NIST.SP.800-144>.
10. NIST: *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. FIPS 203. National Institute of Standards and Technology, Gaithersburg (2024). <https://doi.org/10.6028/NIST.FIPS.203>.
11. European Parliament and Council of the European Union: Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union* L 333, 80–152 (2022).
12. European Parliament and Council of the European Union: Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* L 119, 1–88 (2016).
13. ISO/IEC: *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO, Geneva (2022).
14. Joint Task Force: *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53, Rev. 5. National Institute of Standards and Technology, Gaithersburg (2020). <https://doi.org/10.6028/NIST.SP.800-53r5>.
15. National Institute of Standards and Technology: *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. NIST, Gaithersburg (2024).
16. Yoshinov, R., Chehlarova, N., Dishkova, G.: Assessment of teachers' preparedness in cybersecurity. *Problems of Engineering Cybernetics and Robotics*, 84, 21–34 (2026). DOI: 10.7546/PECR.84.26.02
17. Yoshinov, R., Dishkova, G., Chehlarova, N.: Assessment of parents' awareness in the field of cybersecurity. *Problems of Engineering Cybernetics and Robotics*, 84, 35–45 (2026). DOI: 10.7546/PECR.84.26.03
18. Yoshinov, R., Kotseva, M., Madzharov, A., Chehlarova, N.: Skills and attitudes towards using AI based chatbots. *Environment. Technology. Resources*, 2, 138–142 (2024). DOI: 10.17770/etr2024vol2.8064.