DOI: https://doi.org/10.12700/btsz.2025.7.1.65

ANALYSIS POSSIBILITIES OF THE TOOLSET OF INFORMATION SECURITY

AZ INFORMÁCIÓBIZTONSÁG ESZKÖZTÁRÁNAK ELEMZÉSI LEHETŐSÉGEI

KÁRÁSZ Balázs[1]

Abstract

Regarding the limited availability of comprehensive Hungarian literature on this topic, this paper aims to collect tools of information security utilised by all involved parties and present them to the professional audience in a structured manner. Involved parties consist of users of information infrastructures who are exposed to threats, defence personnel contributing to the maintenance of security level, and attackers that probe the effectiveness of security systems. Tools are widely mapped, including concepts that belong to the logical layer of cybersecurity, as well as physically manifested devices, systems, networks and programs. The objective of the research presented in this paper is to describe the tools by main dimensions and detailed characteristics in a way that, according to these attributes, a comprehensive analysis of comparison can be performed. As a result of the analysis – since tools are collected both from military and civil background – the author makes efforts to determine ways of classification of information security tools, in order to facilitate more successful targeting of further researches of the topic both within military, administrative (public service) and civil context.

Keywords

information security, security awareness, technical, logical and administrative tools,

Absztrakt

Tekintettel a korlátozottan elérhető magyar szakirodalomra, mely átfogó megközelítésből tárgyalná az információbiztonság eszköztárának kérdéskörét, e tanulmány célja, hogy az érintett felek által alkalmazott információbiztonsági eszközöket összegyűjtse, majd strukturált formában bemutassa a szakmai közönség számára. Az érintett felek az információs infrastruktúrák fenyegetéseknek kitett felhasználói, a biztonsági szint fenntartásában közreműködő védelmi oldal, valamint a támadók, akik a biztonsági rendszerek hatékonyságát próbára teszik. Az eszközök széles körűen kerülnek feltárásra, ideértve a kiberbiztonság logikai rétegéhez tartozó koncepciókat, valamint a fizikailag megfogható eszközöket, rendszereket, hálózatokat és programokat egyaránt. A kutatás célja, hogy főbb dimenziók és részletes tulajdonságok mentén jellemezze az eszközöket, és átfogó, összehasonlító jellegű elemzés készüljön. Az elemzés eredményeképpen – köszönhetően annak, hogy az eszközök köre védelmi és polgári környezetre egyaránt kiterjed – a szerző kísérletet tesz ezek klasszifikációs lehetőségeinek megfogalmazására. Mindez hozzájárul a téma további kutatásában a célok megfelelőbb kitűzéséhez katonai, közszolgálati, valamint polgári kontextusban.

Kulcsszavak

információbiztonság, biztonságtudatosság, technikai, logikai, adminisztratív eszközök

[1] karaszb@gmail.com | ORCID: 0000-0003-2065-4928 | Former PhD Student, National University of Public Service, Doctoral School of Military Engineering | Volt PhD hallgató, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

INTRODUCTION AND RESEARCH DETAILS

Regarding current and possible future trends in the evolution of threats on information society, as well as the increasing pace of technical knowledge development concerning cyberattacks, organisations have to dispose of a diverse toolset of information protection they can easily reach out to. Thanks to the recent dynamic technological improvement of the affected areas, such as IT security, physical security, human risk management (in terms of awareness training), the variety of tools is constantly widening up till today. The year 2020 also brought the entire society an information environment that shortens distance between people thanks to technology in times of social distancing.

Browsing through relevant literature, the author has found no up-to-date systematic overview of the entire toolset of information protection and security, which would enable every kind of users to easily find the most suitable and appropriate solution when facing a particular information security problem. Even in studies that analyse the aspects of tools people currently use for conducting private or business life, keeping in touch and maintaining the information flow, no reference can be found to a comprehensive analysis of the toolset of information security. The above-mentioned approach means the main motivation for the author to construct an appropriately structured overview.

Scientific research problem

Based on the above-mentioned issues, the following question arises: what are the main dimensions, according to which, information security tools can be clearly classified, and how can such a classification system contribute to solving ad-hoc occurring or recurring security issues thanks to its transparency and applicability?

Research objective

The objective of this research is, firstly, to collect all currently available information security tools describing their main features and characteristics, and secondly, outline and define at least three dimensions of at least two attributes, according to which, each of the enlisted tools can be classified. As a third step, various ways of classification are to be determined in order for the expected results to be successfully targeted to further research in military context.

Research methods

The author used theoretical and empirical research techniques, partly with the method of grounded theory. Related scientific literature from Hungary, as well as abroad, from professional of both technical approach and military background are widely mapped and elaborated, in terms of review papers, monographs, conference publications, internet sources.

LITERATURE REVIEW

In this chapter, the author enlists concepts on the role of security as viewed by organisations in general, and how handling information and awareness development relate.

One might think for the first view that there is a lack of relevant, up-to-date literature available in Hungary to analyse the toolset of information security. Researches are

based mostly on international literature published in countries that have a developed security culture, information security and cybersecurity knowledge and defence capacity both in civil and military environment. However, if we dig deep in the content of papers, monographs and conference publications, plenty of references can be found that lead to the tools used as part of information security on the side of users, defence forces and attackers, as well.

Definitions of concepts applied within this research

As of today, in everyday conversations, the most common usage of the terms 'data protection' and 'data security' (as well as information privacy/protection and information security) is that they are synonyms. Firstly, the author aims to make a distinction by pointing to the correct understanding of that in the background, behind the action of protection lie massive legal documentation and measures to protect personal data, pointing at exact steps to be taken in order to *achieve* a secure state, while aspects of security aim to *maintain* an already secure environment in a technical sense (that is, within and across information systems) and on the human level of the entire information society, too. Moreover, information security is a wider concept than IT security, since it would also include protecting all forms of information – not exclusively electronic –, also including information services and supporting systems. [1]

The risk itself – as introduced above in the context of information security management – refers to the possibility of not being able to fully protect – or building an attack surface for a potential invader to take advantage of – the information of the organisation, and therefore causing loss, which can theoretically be quantified in every case. By theoretically I mean, in several cases the quantification process might be clear and easy, while in other ways, the organisation might not have the suitable method, time, money or willingness to manage risks in this depth in spite of it being worth from many aspects. [2]

Security in information society

The evolution process of information society throughout the past decades and centuries shows a clear picture of how security became more crucial step-by-step, as some examples follow. Physical passive security systems, such as fences, have always been serving to defend territories or borders against invaders. Physical active security devices, including automatic weapons applied in military defence operations, became necessary to be ameliorated to have dominance over the enemy. [3] By deeper investigation, one can discover parallelisms between concepts of ancient times and security measures of nowadays. Passive information security features firewalls as defence against malicious or intrusive entries, while active information security is equipped with intelligence methods like OSINT or simply AI-based extensions, improving both effectivity and reliability. [4]

Today's information society features intelligent tools, connected to each other via internet, which people use in their everyday life to deal with their duties, responsibilities, and keep in touch with each other – especially true for 2020, when the world-wide Covid-19 pandemic deeply influenced and changed our regular life in many aspects. Humans continue to realise that without connection, or without functional devices, we cannot survive these types of highly influential challenges. [5]

Adding up to the fastening pace of digitalisation, it has always mostly been crises with global impact that implied a next evolutionary step in digitalisation and automatisation. [6] These steps in both fields came across as fast as mankind could not imagine earlier. The specialty of Covid-19 pandemic can be found in that our global approach to commerce, production, consumption was strictly limited in short of time in terms of not allowed to socialise, to work from the office, to attend school for an uncertain time period or to travel abroad or to farther destinations within one's own country of residence. On the other hand, security has turned into a state of uncertainty when global economy, together with local economic processes (proven also by the trends of indexes [7]), started to regress due to restrictions in various industry sectors, but still, everyday duties of most people (including employed and just unemployed), such as taxes, heating or insurance kept on waiting to be paid just as before.

Significance of information security awareness

Obviously, using the internet, smartphones and connected devices daily, everyone should think about what sorts of information is used and shared via these tools. This is the point when we might forget about the security guidelines, the responsibility of the usage. Consequently, without responsibility on the user's side, the risk of loss or theft of data is increased. There is no question about the importance of security awareness, although it is rather relevant to clarify what it is. As we have shortly described above, one will not be able to avoid living without the continuous necessity of up-to-date tools and devices. Therefore, we must understand and learn this process, using which, we will make successful efforts in favour of keeping our private data/information secure. [8]

Information security is required to protect organisation data/information from threats, which can be classified according to being external or internal. External threat is implied by outsiders from the point of view of the organisation and theoretically, it should not make up a major issue, since by 2020, most of the organisations ought to have implemented advanced security technologies at various levels of the security system. [8] Until recently, internal threat has become the main critical information security issue identified, where threat and therefore risk is caused by internal factors, mainly deriving from the poor user behaviour of the employees such as carelessness, omission, and user errors.

Based on the above-mentioned aspects, apart from the technical part of information security, the toolset serving as the basis of our analysis should also include human behaviour the elements of which strongly influence efficiency and reliability rate of operating technical security layers either to protect data or to handle them securely. [9] Human behaviour and decision-making can be driven by rational and emotional reasons, both implying a certain rate of risk of performing under 100%. When it comes to rational decisions and behaviour of the user, the risk lies in the following three major factors: unawareness (together with carelessness), undereducation (related also to omission), and human error. [10] On the other hand, emotion-driven decisions and behaviour are unpredictable because of the irrationality in thinking, vulnerability and misguidance of the user, or simply the personality pattern the user has, therefore carrying a certain measure of risk (to be further defined in the second next paragraph).

After organisations realised that human behaviour influences the effectivity of all steps made to secure the IT and information systems, consulting firms, IT service providers,

and security experts all have been endeavouring the elaboration of courses and development programs (such as trainings and workshops), which are tailored to the unique needs of the organisation, in order to overcome either undereducation or unawareness of employees. [11] In the first case, the main goal is broadening technical knowledge primarily on basic levels, while in the second case, various techniques are at disposal to train the users realise threats and risk-incurring situations and take appropriate actions and reactions.

From the point of view of our analytic research, we consider the above-described side aspects also as crucial contributors to the whole toolset of information security. Within any area considered in the discussion, the triad of the parties affected by the processes of information security serves as a basis of our discussion, since we collect tools of not only the users' side, but also those of the defence personnel and the attackers. The users mean any person dealing with the information to be protected excluding defence personnel, while the term 'defence personnel' covers in our use all users dedicated to protection or maintaining security, and finally, attackers are affected parties aiming to obtain information without authorisation (mainly for criminal purposes).

DISCUSSION

In this chapter, the author collects concepts and specific tools of information security categorised according to their technical, influential, and protective characteristics, aiming to outline ways of building clusters in order to achieve higher effectivity in applying the tools within the organisational context.

Tools of information security

Referring to the literature reviewed in the Chapter 2, we have seen that many papers discuss various solutions and tools of security, although they do not define or describe the tools themselves or organise these into groups. What all pieces of literature certainly affirm is: the effectiveness of taking any sort of information security measures depends on the complexity of execution. For the structured discussion and analysis of the topic, we discern the following three main areas of information security: technical, logical and administrative – according to which, tools are enlisted by naming their important characteristics.

Technical tools of security

By technical security, the author means all security tools and measures that are physically manifested or can be implemented to serve active or passive protection – this way contributing to security directly, by action, in the physical space. Technical tools aim to protect confidential or sensitive information from unauthorised access – confidential or sensitive from the point of view of its owner or its addressee (in case of communication). For example, should documentation of an organisation be held in either electronic or paper-based, the stored or communicated information has to be protected. As for the location of the information, we can enlist buildings, premises, meeting rooms, cabinets, and storage media (paper-based – printed or handwritten, phonographic, magnetic, optical, electronic, digital – computer-based).

Passive technical security includes passive fire protection, water protection, protection against mechanic vibrations, and electromagnetic compatibility. Active technical security features external and uninterruptible power supply, air conditioning, active fire protection, cable management. The tools at the users' disposal when talking about technical security are limited. This circle includes simple solutions to serve the work-related or everyday life-related information need in a user-friendly way. To have authorised access to the information, walls can be overcome only through doors, and locks are to be unlocked by appropriate keys.

As for the tools applied by the defence personnel, entry points to office buildings have security guards requiring self-identification from arriving guests to let them in and in cases, baggage check/car trunk check when somebody is leaving the building, while highly protected areas can also feature armed guards. Perceptibly forwarded information can be secured by surveillance systems (image and voice recording, closed-circuit television), intrusion detection systems (based on electromagnetic technologies such as infrared vision or radar), DECT phones, electromagnetic shielding, acoustic vibration or barrier film layers (the latter two tools serve for avoiding eavesdropping in case of respective indications).

Attacks aiming at a technical security measure or solution share the objective to find and make use of flaws in either its preparation (design) or its implementation (execution). Forging, deception, and force are the main methods at the attackers' disposal to encompass the flaws or overcome security lines, therefore making it possible to obtain protected information – and at a later point, to use them for malicious intentions. While at first hearing, attack imply something coming from the outside, it would be a mistake not to observe the inside threats including human risk of inappropriate information handling (unintended attack).

Logical tools of security

By logical security, we would like to include all concepts or methodologies that have significant role in actively or passively maintaining a secure environment.

Recently, with the growing importance of work from home, it has become more difficult to keep all information secured when in home office – partly due to the usage of user-owned devices (UOD) and take some of the sensitive documentation with us. At home one feels safe, while having guests that use their devices on these home networks, all sharing the same level of safety. These can easily open the possibility for unauthorised access or vulnerability in the event of an attack. Tools we can use are virus protection, firewall, regulations, awareness of information security better to say conscious protection, software control. To summarise these, we can say logical security.

End-to-end encryption is a logical tool encoding content within digital communication, connected to both ends of communication. The principle is based on using a pseudo-random encryption key, which is generated by an algorithm, provided to authorised recipients. [12] This way, it features numerous but limited number of possibilities to decrypt the content without possessing the key by applying brute force, although only with notable computational capacity. In everyday life, one can encounter the principle at messaging applications, which vary storing the key at the operator or the source/recipient within the communication. The second option provides the user higher level of security and privacy, since this way, even the service provider cannot access the content in a decrypted form.

Key management is strongly linked to encryption where (usually referring to a system) the logic behind the handling of encryption keys is administered – also meaning a domain where keys are generated, distributed, stored, refreshed, recalled or annulled. [13] The crucial points of a successfully operating key management include scalability – capability of managing a large number of encryption keys, security – elimination of vulnerabilities exposed to outside hackers or malicious insiders, availability – ensuring data accessibility for authorised users, heterogeneity – support of multiple databases, applications and standards, as well as governance – definition of policy-driven access control and protection for data.

Folders, domains of storage, virtual protection barriers such as firewalls and other logical units of systems and networks are to be unlocked, accessed, or modified by users and administrators possessing the appropriate access rights. Identity and access management (IAM) is a framework of implemented principles and directives as well as technologies that effectively assure to grant access to (sub)systems, (sub)domains partly or entirely to the authorised users only. A correctly operating IAM framework complies to all three attributes to information security: confidentiality, integrity and accessibility, not only from the perspective of the information but also interpreted in the context of the logical structure of the assigned access rights. [14]

Coming to the question of identifying authorised users to data which is secured/encrypted/protected, the key notion is authentication. Authentication methods can be diversified according to several factors – either if one or more of them implemented at the same time. The more factors implemented, the higher level of security the protection features. Factors can vary from knowledge-based (password) through possession-based (token or text message or push notification on mobile device) to character-based (biometrics) solutions, and multi-factor authentication means at least two different methods used within one authentication process. [15]

Administrative tools of security

Administration tasks – to variable extent – accompany all technical and logical tools of security, as stated above even in paper-based form or electronically. Administrative security is based on the rules, laws, policies to follow and covers compliance to technical specifications, principles, as well. Moreover, it's about the people, it's about the human component. The highest level of security risk can be related to human factors. Through manual controls we can ensure that there is no intentional or unintentional act in the process, however this rather detective way of control. These activities could be identified with detective control, but more secure to build security awareness in the people, teach them how to protect the data, information they use. Those rules, laws and policies mentioned in the beginning of this paragraph each person should acquire, who use the clever tools, the internet even in their private or business life.

Bureaucracy cannot be separated from administrative tasks – which from first hearing implies that complicated processes and paperwork (even if digitally documented) are attached to security measures. On the contrary, thoroughly worded, clear, and detailed description of IAM (paired with full compliance) can keep information systems safer from hacker attacks, as shown by the example of the Hungarian school administration system scandal in late 2022. [16] In this recent case, not only the system's source code was retrieved

by the intruder, but personal data and a wider circle of information about potentially all of the users have been compromised. The system was operated with significant deficiencies in IAM, authentication, security awareness and inappropriate corporate communication. If these administrative processes had been better defined and enforced, the vulnerabilities that led to this breach could have been prevented. This highlights the importance of not only technical defences but also the rigorous implementation of administrative controls to strengthen overall security posture.

Additionally, we have places where the topic of meetings holds the risk to get publicity or fall into the wrong hands. Confidential discussions regarding security strategies, vulnerabilities, or potential future threats can inadvertently become a target for malicious actors if not properly managed. In such cases, ensuring that the right people have access to sensitive information is paramount, and any sharing of such details should be handled with extreme caution. Thus, fostering an environment where confidentiality and discretion are prioritised is critical for effective administrative security.

Security awareness training concepts should be elaborated based on precedent case studies, analogy research, simulation and with an emphasis on solution-focused and decisive thinking development. The process management connected to information security measures within organisations can be considered as more and more developed, whereas nowadays, cyberattacks threatening daily operation of corporates are performed more frequently. Regarding this, it is inevitable to incorporate security awareness to corporate training and development, and the maintenance of high level of preparedness in both technical and non-technical fields, especially in order to adequately handle human risk factors.

ANALYSIS

This chapter aims to provide a concise analysis of the collected information security tools, focusing on their classification across multiple dimensions. By examining these dimensions, the author aims to establish a structured framework that enables a better understanding of the tools' applicability, strengths, and limitations. Such a framework can guide both military and civil organisations in selecting the most appropriate tools for their unique contexts.

Impact: direct vs. indirect security

Direct security tools are capable of immediately handling specific vulnerabilities or threats. For instance, the implementation of firewalls in a network system has been proved to be highly effective in preventing unauthorised access and blocking malicious traffic. A frequently occurring example can be a firewall which, during a coordinated phishing attack, successfully filters and flags suspicious links in emails, preventing the users from compromising sensitive systems. Examples can also cover intrusion detection systems, antivirus software, and access control tools. These tools act as a front line of defence, blocking or mitigating risks in real-time.

Indirect security tools focus however on enhancing the overall defence ability of a system. These include awareness training programs, security policies, and compliance mon-

itoring systems, among others. While they do not confront threats directly, they aim to create an environment that reduces the probability of carrying out successful attacks by the means of improving user behaviour, organisational culture, or system configurations.

Contribution: active vs. passive security

Active security tools are based on continuous monitoring, capability of intervention, and are adapted to maintain effectiveness of defence level. List of examples include most importantly intrusion prevention systems, security information and event management systems. These tools often demand a higher level of expertise and resource allocation but provide immediate responses to dynamic threats.

Passive security tools however function in the background or in a fully automated manner, providing basic and ideally continuous support, such as encryption algorithms, hardware security modules, or even physical barriers like locked server rooms. These tools make active security measures complete by providing a stable basis for them to operate effectively. For instance, encryption ensures data integrity, which is critical for intrusion detection systems to accurately analyse information, whereas secure hardware and physical barriers ensure the reliability of active monitoring. While their maintenance needs are typically low, their effectiveness depends on proper implementation and regular updates.

Approach: proactive vs. protective security

Proactive security tools are focusing on risk identification and mitigation before they are effectuated as threats. However, implementing such tools result in higher upfront costs and also, they need specialised configuration and maintenance expertise. Moreover, potential false positives strain resources or desensitise response teams. Additionally, their effectiveness depends on accurate threat intelligence, which can be difficult for seamless integration. Examples cover vulnerability scanning software, penetration testing, threat intelligence platforms, and predictive analytics systems. These tools are critical for reducing the exposure to emerging threats and ensuring resilience of systems and networks.

Protective security tools, in contrast, are designed to detect, or recover from security breaches. Examples include backup and recovery solutions, incident response plans, and endpoint detection and response tools. These tools are indispensable for minimising the damage caused by successful attacks and restoring normal operations.

Control: management vs. operational vs physical security

Management-level tools approach information security from the strategic viewpoint, often serving as a bridge between operational and physical security by ensuring that strategic-level decisions take both technical and tangible aspects of protection into consideration. For example, risk assessments guided by governance standards (e.g., ISO 27001) can influence physical security measures like access zones, and in parallel, also shaping operational strategies, such as automated monitoring protocols. They are essential for aligning security efforts with organisational goals and regulatory requirements.

Operational-level tools are implemented at the tactical level to manage day-to-day security challenges. Monitoring dashboards, automated patch management systems, and user access provisioning tools belong to this layer of control. These tools translate strategic goals into actionable measures.

Physical security tools cover various tangible measures to physically protect technical assets and visible parts of infrastructure. Surveillance systems, biometric access controls, and environmental monitoring sensors are part of this layer, while addressing physical vulnerabilities that could compromise information systems. Major risks mitigated by their presence could cover disruption of critical infrastructure, or undermining of the integrity of digital operations. For example, a physically compromised server room can lead to data breaches or system failures that directly impact virtual systems relying on it.

Integrating these three layers of the dimension of control ensures a holistic security posture, as each layer addresses distinct aspects of organisational security.

Manifestation: virtual vs. physical security

Virtual security tools are solutions that are based on software, and are designed to protect digital assets including information at first place. Firewalls, data loss prevention systems, and secure coding practices are of highest importance to be enlisted within this element. These tools combat cyber threats that seek to exploit vulnerabilities in digital systems and networks.

Physical security tools, on the contrary, aim to protect the tangible components of an information infrastructure. Examples include hardware firewalls, secured server enclosures, and electromagnetic shielding for critical systems. These tools are crucial for defending against threats like unauthorised access, theft, or environmental hazards. While virtual security tools dominate modern cybersecurity discussions, the increasing interconnectivity between digital and physical domains (for instance, in IoT environment) underscores the importance of physical security measures.

CONCLUSION

By analysing information security tools across these five dimensions and their elements or layers (as referred to in the analysis), this paper provides a comprehensive overview for understanding their roles and applications. Organisations can use it, supporting their security objectives, to identify and classify tools effectively and select the most suitable options based on their specific needs. Furthermore, the approach used within this analysis in setting up the five dimensions supports further research into developing integrated security solutions that can relate to complex challenges in both military and civil context.

REFERENCES

[1] R. Von Solms and J. Van Nieker, “From information security to cyber security.” *computers & security*, vol. 38, pp. 97-102, 2013. doi: 10.1016/j.cose.2013.04.004

[2] E. Gelbstein, “Quantifying information risk and security.” in *ISACA Journal*, 2013, no. 4 (access: https://www.isaca.org/resources/isaca-journal/past-issues/2013/quantifying-information-risk-and-security (04.02.2025)

[3] Z. Haig, *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó, 2018. ISBN 978-615-5945-05-2

[4] Cs. Kollár, “A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában,” in *Kiberbiztonság – Cybersecurity 2.*, Z. Rajnai, Ed.,

Budapest, Hungary: Óbuda University, Doctoral School on Safety and Security Sciences, 2019, pp. 47-61.
[5] K. Härmand, *Digitalisation before and after the Covid-19 crisis,* ERA Forum vol. 22, pp. 39–50, 2021. doi: 10.1007/s12027-021-00656-8
[6] F. Debasa, "Digitalisation, pandemics and current world (2019-2021)", *unio,* vol. 7, no. 1, pp. 18–32, Oct. 2021. doi: 10.21814/unio.7.1.3575
[7] H-J. Trenz, et al., Resilience of public spheres in a global health crisis. *Javnost-The Public,* vol. 28, no. 2, pp. 111-128, 2021. doi: 10.1080/13183222.2021.1919385
[8] Cs. Kollár, "Életünk a digitális korban," in: *Pedagógia a digitális korban*, Cs. Kollár, R. Tóth, Eds., Budapest, Hungary: PREMA Consulting, 2014 pp. 1-30.
[9] R. Klint, 'Cybersecurity in home-office environments : An examination of security best practices post Covid', Dissertation, 2023.
[10] Cs. Kollár, *Az információbiztonság jogi- és humán aspektusai*. Budapest: Szerzői kiadás, 2023.
[11] B. Kárász and Cs. Kollár, "Leadership Responsibilities in Information Security Awareness Development", *AARMS,* vol. 19, no. 2, pp. 79–91, May 2021, doi: 10.32565/aarms.2020.2.6
[12] G. Kovács and J. Hornyacsek, „Korszerű oktatási eszközök és módszerek alkalmazása a polgári védelmi felkészítésben." *Műszaki Katonai Közlöny* vol. 29, no 2, pp. 117-132, June 2019, doi: 10.32562/mkk.2019.2.10
[13] K. Ermoshina, F. Musiani, H. Halpin, (2016). "End-to-end encrypted messaging protocols: An overview." presented at the Internet Science: Third International Conference, INSCI, Florence, Italy, Sept. 12-14, 2016, Proceedings 3, pp. 244-254, Springer International Publishing.
[14] W. Fumy and P. Landrock, "Principles of key management," in *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 785-793, June 1993, doi: 10.1109/49.223881
[15] M. A. Thakur and R. Gaikwad, "User identity and Access Management trends in IT infrastructure- an overview," *2015 International Conference on Pervasive Computing (ICPC),* Pune, India, 2015, pp. 1-4, doi: 10.1109/PERVASIVE.2015.7086972.
[16] B. Kárász, "Social Aspects of Reliability and Security Issues of Authentication Solutions" *Hadtudományi Szemle* vol. 13, no. 2, pp. 111-127, June 2020, doi: 10.32563/hsz.2020.2.9
[17] Telex: 110 milliós bírságot kapott a KRÉTA meghekkelt fejlesztője, súlyos hiányosságokra derült fény. https://telex.hu/techtud/2024/02/21/kreta-hekkertamadas-feltores-szemelyes-adatok-naih-vizsgalat-eredmeny-adatvedelmi-birsag (access: 29.01.2025)