UNIVERSIDAD & SOCIEDAD
Presentation date:July, 2025
Date of acceptance: August, 2025
Publication date: September, 2025

EVALUATION

OF INNOVATIVE ROBOTIC TECHNOLOGIES FOR COMPREHENSIVE INFORMATION SECURITY

EVALUACIÓN DE TECNOLOGÍAS ROBÓTICAS INNOVADORAS PARA LA SEGURIDAD INTEGRAL DE LA INFORMACIÓN

Kirill Pitelinsky[1,2*]
E-mail: yekadath@gmail.com
ORCID: https://orcid.org/0000-0001-6459-9364
Sergey Makovey[1]
E-mail: intele577tuver@gmail.com
ORCID: https://orcid.org/0000-0002-6926-1079
[1] Moscow Polytechnic University, Russia
[2]All-Russian Institute for Scientific and Technical Information of the Russian Academy of Sciences, Russia.
*Corresponding author

Suggested citation (APA, seventh ed.)

Pitelinsky, K. & Makovey, S. (2025). Evaluation of innovative robotic technologies for comprehensive information security. *Universidad y Sociedad, 17*(5). e5417.

ABSTRACT

This study evaluates innovative robotic technologies for comprehensive information security in organizational management. The mobile robotic platform RoboTurtle was designed to strengthen protection of data flows and material assets through robotics, IoT, and advanced encryption methods. The research applied vulnerability analysis, simulation modeling, and testing of authentication and communication protocols to assess security effectiveness and reliability. Results show that RoboTurtle enhances managerial control by ensuring secure communication with two-factor authentication, VPN channels, and encrypted document handling. The platform also improves resilience against cyberattacks and unauthorized access, contributing to organizational risk management and continuity. Findings confirm the potential of integrating robotic systems into management strategies, offering scalable and innovative solutions for improving security, efficiency, and trust in digital operations.

Keywords: Information security, Mobile robotics, Management systems, Innovation, Risk management, Intelligent systems.

ABSTRACT

Este estudio evalúa tecnologías robóticas innovadoras para la seguridad integral de la información en la gestión organizacional. La plataforma robótica móvil RoboTurtle fue diseñada para fortalecer la protección de los flujos de datos y activos materiales mediante robótica, IoT y métodos avanzados de cifrado. La investigación aplicó análisis de vulnerabilidades, modelado de simulación y pruebas de protocolos de autenticación y comunicación para evaluar la eficacia y fiabilidad de la seguridad. Los resultados muestran que RoboTurtle mejora el control gerencial al garantizar una comunicación segura con autenticación de dos factores, canales VPN y gestión de documentos cifrados. La plataforma también mejora la resiliencia frente a ciberataques y accesos no autorizados, lo que contribuye a la gestión de riesgos y la continuidad organizacional. Los hallazgos confirman el potencial de integrar sistemas robóticos en las estrategias de gestión, ofreciendo soluciones escalables e innovadoras para mejorar la seguridad, la eficiencia y la confianza en las operaciones digitales.

Palabras clave: Seguridad de la información, Robótica móvil, Sistemas de gestión, Innovación, Gestión de riesgos,

Sistemas inteligentes.

INTRODUCTION

The advancement of technology naturally leads to the complication of requirements to ensure the security of the Earth's information field (noosphere) and the technosphere. Humanity constantly maintains rigid norms of behavior in society, trying, if possible, to maintain positive spiritual and socioeconomic relationships, passing them on to future generations (Pitelinskii et al., 2022). However, along with the striving to peacefully coexist with other elements (objects and subjects) in the biosphere, human beings retain a hereditary "defect" (Cain's sin), which causes constant violation (distortion) of the laws of the fragile Universe. Human subconscious impulses to pursue and create favorable conditions for themselves have always been noble. Yet, with the passage of time and generations, the understanding of the methods and means of achieving personal comfort has gradually grown perverted, leaning into ensuring selfish and hedonistic consumption.

In this context, the accelerated expansion of digital technologies, artificial intelligence, and intelligent robotics has profoundly transformed the way society's function, interact, and establish rules of coexistence. While these innovations provide unprecedented opportunities for communication, productivity, and education, they also increase systemic vulnerabilities. The world of technology and the degradation of traditional methods of communication have brought about the notion that every element of the socioeconomic system requires various methods and means of protection, ranging from installing door locks and security checkpoints at company entrances to ensuring cybersecurity frameworks that protect digital infrastructures and, ultimately, human life in times of geopolitical conflicts. The growing dependence on digital ecosystems underscores the urgency of designing resilient security systems capable of addressing threats at both the physical and virtual levels.

Previously, in the framework of educational activities and testing various ways of attracting talented youth (as key representatives of modern society and the future of spiritual, ethical, and socioeconomic relations) to higher education institutions, we proposed a mobile robotic platform in the form of an avatar RoboTurtle to assist in collecting applications during admission campaigns. The concept of RoboTurtle incorporates machine learning, the Internet of Things (IoT), virtual reality (VR), and the principles of voice control and intelligent vision. This integration of advanced technologies not only positions RoboTurtle as an effective interactive tool but also reflects the broader paradigm of the digital university, where automation and intelligent systems play an active role in academic, administrative, and research environments.

Consequently, the most important issue here is not limited to the quality of modeling and design but lies in ensuring comprehensive security, particularly at the hardware-software level. Guaranteeing protection from external interference, data leakage, and malicious tampering becomes essential for preserving institutional integrity and trust in such platforms. In this light, the aim of this article was to investigate current security systems that can protect both the information flows and resources of the company or university, prevent malicious tampering with hardware, and offer a reliable way to safeguard information on various carriers. Performing all these functions, the mobile robotic platform has the potential to become a key element in digital university ecosystems, enhancing resilience and security in the education system in the context of digital transformation.

MATERIALS AND METHODS

The methodology integrates robotics, information security, and IoT to address the security of information flows and physical assets in educational institutions using the RoboTurtle platform.

The research began with a literature review to identify security threats to mobile robotic systems, such as cyberattacks and unauthorized access. This informed the design of the robot, with a focus on selecting secure hardware and software components, including sensors, cameras, and processing units, alongside protective mechanisms to prevent tampering.

To ensure data security, advanced encryption methods like the Advanced Encryption Standard (AES) and Transport Layer Security (TLS), along with virtual private networks (VPNs) and two-factor authentication (2FA), were implemented for secure communication between the robot and the educational network. The robot's physical security was addressed by integrating a secure container, such as a safe, to store sensitive documents.

Simulations and testing were conducted to model security scenarios, assess vulnerabilities, and refine the system. The robot's interface was designed for secure user interaction, utilizing voice control, machine learning, and real-time monitoring. Risk assessment models and monitoring tools, such as intrusion detection systems (IDS), were applied to evaluate the robot's security.

The robot was integrated with the institution's information systems for secure document handling during the admission process. Finally, the system was evaluated for performance, reliability, and security, with optimizations proposed based on the results.

This methodology ensures that the mobile robotic platform is both secure and efficient for use in educational environments.

RESULTS AND DISCUSSION

The competitiveness of companies in implementing new technological solutions for business processes continues to be a relevant problem because of the great importance of the business process management lifecycle. Dynamic contour flows (Monoscalco et al., 2022) directly impact the quality and efficiency of company management because they can be used to describe and optimize its operations, and simulation modeling can be applied to address and evaluate existing and prospective risks. All these flows can be distinguished into five categories (flows): information (any information circulating in the company that is of interest to all its owners and customers, including malicious parties), financial (company revenues, expenses, profits, etc.), material (tangible assets in the structure of the company), energy (utilities, fuel, etc.), and human resources (company personnel). Only the integrated application of methods and means of ensuring the company's economic and information security (EIS) can protect these flows and support their dynamism.

As socioeconomic relations became more complex and intensified, the requirements for ensuring the continuity and security of business processes carried out by each company became more stringent. The catalyst for this was the steady and permanent digitalization of human life, which allowed implementing methods and tools that have now become an integral part of the infrastructure of enterprises and organizations. One significant result of this process is the utilization of mobile robots (robotic platforms) in all professional fields.

Mobile robots are increasingly applied in industry and education (Çam & Kiyici, 2022; Sun & Zhou, 2022). In a previous study, we proposed a concept model of the RoboTurtle with a detailed description of its functional characteristics, potential set of control principles, features of interaction with users (university applicants), and an automated document management system (Pitelinskii et al., 2024).

Being an inescapable accompanying feature of information systems, threats of control override and physical damage (accidental damage or intentional vandalism) are a serious issue that requires reliable methods of mitigation.

These methods include (Pitelinskii et al., 2021):

- ensuring a secure connection when exchanging information;
- thoroughly testing of the system's functional characteristics;
- restricting access to the robot control system and to the room where the robot is kept;
- control over the robot's autonomous behavior by the operator (manual development and update mode, production planning software);
- theft alert system (alert sensors that transmit a message to the responsible person when the set distance marker is crossed).

The best option for reliable network interaction between the robot and the university database is Wi-Fi with a secure connection.

The technologies utilized in this solution include:

- two-factor authentication (2FA) — without additional verification (an SMS code), possessing the password will not be enough for interception;
- virtual private networks (VPN) — chances of interception are reduced by changing the IP address with traffic encryption;
- To ensure secure interactions with applicants, providers will need to comply with the following requirements (Seleman, 2016):
- network segmentation (limiting network security threats by splitting the network into multiple virtual segments (VLAN));
- monitoring of the network with programs to detect, alert to, and prevent network anomalies (e.g., IDS and IPS);
- up-to-date security protocols (WPA2 or WPA3);
- traffic encryption with advanced encryption algorithms (e.g., AES-128/256);
- regular software updates to keep the security system stable;
- etc.

The Enterprise Wi-Fi authentication mode is a good fit for companies that require a high level of security, granular access control, and centralized management of credentials and policies. Unlike the Personal Wi-Fi authentication mode (all users having the same password), the Enterprise mode uses 802.1X authentication, where each user has their own credentials. As a result, even if one user's authentication credentials are compromised, the network is not compromised (Akyildiz et al., 2020; Sadkhan & Abbas, 2016).

Enterprise Wi-Fi networks support various types of 802.1X Extensible Authentication Protocol (EAP) authentication: EAP-TLS (Transport Layer Security), EAP-PEAP (Protected Extensible Authentication Protocol), and EAP-TTLS (Tunneled Transport Layer Security). Among these, EAP-TLS is the most secure type of Enterprise 802.1x authentication, because it uses public-key cryptographic algorithms and certificates (instead of static credentials) (Robai, 2024).

The safest Wi-Fi network (according to the standards of the National Security Agency, NSA) is WPA3-Enterprise

with EAP-TLS. A detailed overview of the different Wi-Fi security levels and versions with their characteristics is presented in Table 1 (Ikechukwu, 2024).

Table 1. Overview of Wi-Fi security levels and versions.

Standard	WEP	WPA	WPA2	WPA3
Year of release	1997	2003	2004	2018
Cipher suite	RC4	TKIP with RC4	CCMP (encryption with the AES counter mode and a cipher block chaining message authentication code (CBC-MAC))	GCMP (encryption with the AES counter mode, the Galois Message Authentication Code) and the CCMP block encryption protocol
Supported key size	64 and 128-bit	128-bit	128-bit	128 and 256-bit
Cipher type	Stream	Stream	Block	Block cipher mode (with stream cipher mode)
Authentification	Open system and shared key	WPA 4-Way-Handshake to check for correct account data (PSK or 802.1x)	WPA 4-Way-Handshake to check for correct account data (PSK or 802.1x)	Simultaneous Authentication of Equals (SAE) to securely check for correct account data (PSK or 802.1x)

Source: own elaboration.

Sadly, the WEP protocol has been obsolete since 2003, so the numerous shortcomings of WEP needed to be addressed immediately. However, the slow and meticulous process required to develop a new security specification was at odds with its demand. As an interim standard, the Wi-Fi Alliance released WPA in 2003, while IEEE developed its more robust replacement, the WEP specification WPA2.

WPA2 is the minimum Wi-Fi security standard demanded of modern information and computing networks. Today, it is the most widely used enterprise-level Wi-Fi security standard. However, despite its reasonable reliability, several vulnerabilities have been discovered (decryption of network traffic, connection hijacking, content injection into the traffic stream, etc.), leading to the advent of WPA3.

WPA3 also introduced some new features for users to improve the authentication standard, make algorithms more crypto-resistant to protect sensitive data, and improve the fault tolerance of mission-critical networks. Therefore, the highest level of Wi-Fi security to date is provided by the WPA3-Enterprise 192-bit mode with EAP-TLS.

Reliability of the mobile RoboTurtle

The reliability of any object or process is understood as its ability to perform the stated tasks without failure in the presence of undesirable influences. In our case, the factors at play are the above-described restrictive measures of information security and energy independence of the informatization object.

Today, the operation of the technosphere is not feasible due to the human factor, which plays a pivotal role. Therefore, we conclude that to make mechatronic systems fault-tolerant, we need to address the issues of the optimal battery recharging method and the material equipment of structures that can have a critical impact on the functions of control, interaction with the user, and information transmission and processing.

The RoboTurtle is intended to function within the admission campaign of an educational organization (higher education institution) to ensure fast, efficient, and secure processing of applicants' documents, as well as to improve operational operability in the provision of logistics and consulting services with the implemented protection measures (if the robot is misused or deliberately damaged). Accordingly, the issue of resilience to technical failures and third-party interference is central to user security, which affects the reputation of the entire organization.

It is also crucial to ensure the uninterrupted operation of the RoboTurtle throughout its workday. The battery, in addition to basic functions (to move in a given area, interact with users, and collect and store their applications), needs to power the camera, scanner, VR/AR technologies, news display, the safe lock (combination or biometric), and the emergency alert system (in operating mode).

Once the workday is over, the RoboTurtle returns to its electric "base" following a preset algorithm, completes its work, and recharges until the next workday. In the future, there may be a solution for recharging backup batteries "on the go", which would prevent sudden shutdown by increasing the time of operation without recharging at the base. One such solution is manufactured by Wibotic (USA) (Pitelinskii et al., 2021).

Physical media for protected information used by the RoboTurtle

Protecting the material assets of the company (university) is another important aspect in the process of using the RoboTurtle, since both the robot itself and the archive of applications to be stored in its metal container can be of interest to potential intruders.

Regarding the optimal type of container, we proceeded primarily from the parameters of durability and resistance to various influences (mechanical, electrical, chemical, etc.). Safes are preferable for such purposes, as they are more reliable and many of them are fire-resistant. Moreover, safes are protected by thick locking tabs and walls. The disadvantages in our case are their weight and cost. However, if a safe is to be installed, a 5–6 kg version will be suitable for the task. An example of a safe appropriate for our purposes is shown in Figure 1.

Fig 1. A metal safe for the RoboTurtle.

Source: own elaboration.

The priority is to establish the purpose and dimensions of the safe that will not impair the performance of the mobile RoboTurtle (slowing it down or causing it to skid due to overloading). The safe will be fixed on the RoboTurtle's back, embedded in its shell. The other two features (lock and safe type) should be given more careful consideration.

Safes come in different types, each with its own advantages and disadvantages. A brief overview of the different types of safes is given in Table 2 (Esenogho et al., 2013). For the practical implementation of the RoboTurtle, a gun safe was chosen due to its popularity and constructive sophistication.

Table 2. Overview of the types of gun safes.

Safe box type	Description
Steel safes	The most common type of gun safe. Usually made of steel with additional hardening treatment or thicker steel and often reinforced with additional steel plates. Steel safes are relatively affordable and provide decent protection against theft and fire, but are not as resistant to drilling as other types of gun safes
«Alligator»	Made of drill-resistant steel. More expensive than steel safes, but provide better protection against theft and fire
Fireproof safes	Designed to protect objects from fire. Made of steel resistant to high temperatures and may have a fireproof lining. Fireproof safes are the most expensive type of gun safes, but also provide the best protection against fire
Waterproof safes	Designed to protect objects from water damage. Made of stainless steel and may have a waterproof lining. Waterproof safes are not as common as fireproof safes, but they can be a good option for humid climates
Combination lock safes	Opened with a combination of digits. Convenient, but generally less secure than biometric or key-locked safes

Biometric safes	Opened with fingerprint scans. Expensive, but more secure than combination safes
Key safes	Opened with a key. The safest type of gun safes, but also the most inconvenient in terms of equipment

Source: own elaboration.

The safe is installed by mounting it on the RoboTurtle with fasteners. Since the mobile robot is supposed to collect applicants' forms, a 3-4 mm wide slot for A4 paper is needed. After the paper is fed into the safe, the application will fall on the drum scanner fixed inside the container, scanned, and immediately sent to the database for further processing via Wi-Fi.

Moreover, the external condition of the safe requires upkeep to prevent it from rapid wear and tear and loss of functionality. The safe should be inspected regularly, checking for signs of damage (dents or scratches) and inspecting the door to make sure it closes and locks properly. The inside of the safe also needs to be kept clean to prevent the accumulation of dust and dirt and protect the stored objects. Furthermore, the safe interior must be kept dry to prevent the accumulation of moisture and the consequent emergence of rust and corrosion.

Comparative analysis of padlocks

The type of access is another critical characteristic for choosing a safe, with market trends in digitalization indicating a growing interest in biometrics. Biometric credentials can be used as a sole form of identification or combined with other credentials to provide multi-factor authentication (MFA). The introduction of MFA raises the level of security in controlled areas where biometric entry systems are installed. A biometric reader (access control scanner) compares the user's characteristics with a biometric template stored in the database. If the characteristics match, a door opening signal is issued to open the electronic biometric door lock.

Despite their impressive capabilities owing to the unique biological traits of an individual or authentication advantages (e.g., verification in real time — a low response time, which reduces the risk of unauthorized persons gaining access and enables a consistent and efficient user experience), these cutting-edge devices also raise significant concerns about their ability to provide adequate data security. Legal and ethical considerations (ensuring user consent, data privacy, etc.) must also be addressed. The key to striking this balance is innovation, from advanced encryption algorithms to privacy-oriented rules. Considering the option of biometric door locks, it is important to note the low cost of biometric data collection and the practical ease of use of such a system.

Biometric identification methods have their peculiarities and limitations, which are worth looking into when choosing the priority practical solution. The performance of such methods hinges on the probability of errors. This includes the False Accept Rate (FAR), the probability of an unregistered user (potential intruder) being allowed to enter the system, and the False Reject Rate (FRR), i.e. the frequency at which authorized users are denied access. The error rates of the main static biometric identification methods provided in Table 3 are calculated using the formula (F1).

$$FAR = \frac{EM}{M} * 100\% \; FRR = \frac{EK}{K} * 100\% \quad \text{(F1)}$$

where: EM — the number of times intruders have successfully gained access;

M — total number of attempts by intruders to gain access;

EK — number of access denials to authorized users;

K — total number of entries attempts by authorized users.

Table 3. Error probability of static biometric identification methods.

Technique	Error rate
Fingerprint	FAR = 0.001%, FRR = 0.6%
Iris	FAR = 0.00001%, FRR = 0.016%
Retina	FAR = 0.0001%, FRR = 0.4%
Face geometry (3D)	FAR = 0.0005%, FRR = 0.1%
Face geometry (2D)	FAR = 0.1%, FRR = 2.5%

Source: own elaboration.

Due to the high demands on the company's infrastructure, we opted for a more familiar security solution — combination locks. Examples of such solutions are shown in Figures 2 and 3.

Fig 2. ABUS combination padlock.

Source: Khochueva & Shugunov (2020).

Fig 3. Master Lock combination lock.

Source: Khochueva & Shugunov (2020).

Increasing the durability of components

The strength of components correlates with reliability while meeting the requirements of fault tolerance. The primary ways to improve the strength of the casing of the mobile RoboTurtle are the characteristics of 3D printing and casing design. In addition, the chosen materials (e.g., composites) can enhance the strength and resistance of the device to external factors (including corrosion) due to their specific physical/chemical properties (Tomo et al., 2024).

Carbon fiber, also known as graphite fiber, has undeniable advantages as a material created specifically to improve material strength. It is made up of long strands of carbon fibers that intertwine with each other to form a fabric-like structure. Carbon fiber parts are similar to steel in their properties and to plastic in weight. Thus, in terms of strength-to-weight ratio (as well as stiffness-to-weight ratio), carbon fiber parts have much higher performance characteristics than parts made of steel or plastic. Carbon fiber is used, for example, as a reinforcing material in composite materials. It is not damaged by acids, alkalis, salts, and organic solutions and is highly heat resistant, retaining its mechanical properties at temperatures up to 2,000°C (Parandoush et al., 2019).

Carbon fiber is about five times stronger than steel and twice as stiff, but lighter than aluminum, so it is often used as a substitute for alloys where the metal is not strong enough. Because of its electrical conductivity, carbon fiber is also used in place of metals in many simpler items such as boats, bulletproof suits, and more. It is also increasingly utilized

in wind turbines, the aerospace industry (commercial and military aircraft), and in the manufacturing of pressure vessels (to increase strength-to-weight ratio and stiffness). The main drawback of this material is its brittleness. Despite its durability, carbon fiber often gets destroyed when broken. Another disadvantage is the high cost of this material. Furthermore, although carbon fiber is more biodegradable than steel and other materials, it is harmful to the human body, causing some forms of lung cancer.

Because of the high hardness, if the cutting force is too small, carbon fiber is difficult to machine (e.g., drill, as the workpiece can be easily broken with not enough cutting force). This problem can be solved by using glass fiber, synthetic fiber, or aramid fiber mixed with carbon fiber, which not only preserves flexibility, strength, and hardness but is also more suitable for machining.

The durability of 3D printed parts depends largely on the chosen material. Each material (such as PLA, ABS, or nylon) has unique properties that affect its durability, flexibility, and resistance to impact or heat. Choosing the right material based on its intended application is critical to ensuring the desired functional strength characteristics. Therefore, it is wise to utilize CAD systems during the design process.

The basic properties of popular 3D printing materials are described in Table 4.

Table 4. Basic properties of common 3D printing materials.

Material	Properties
PLA (polylactic acid)	The material is easy to use, quite durable, with an ultimate tensile strength of 611 kg/cm2, but it can become brittle under heavy loads.
ABS (acrylonitrile butadiene styrene)	An engineering-grade material used in everyday items, more stable than PLA, but with a slightly lower ultimate tensile strength (224.3 kg/cm2).
Nylon	A material that is flexible in its thin state, with excellent layer adhesion, making it durable and suitable for functional parts such as hinges (843.3 kg/cm2).
Polycarbonate	Extremely strong and heat resistant, the material is ideal for high-strength components such as bulletproof glass (458.8–611 kg/cm2).

Source: own elaboration.

Other factors include 3D printer settings and post-processing techniques (Table 5).

Table 5. 3D printer settings and post-processing methods.

3D printer settings	Result
Infill percentage	The percentage of solid body in the printed part. A part with 0% infill is hollow, and one with 100% fill is solid.
Layer height	The thickness of each printed layer directly affects the strength of the structure, as thinner layers provide greater strength.
Part orientation	The bonding between layers is important for the overall strength of the structure. Therefore, it is vital to account for the occurrence of stresses in the product and formulate manufacturing process requirements to optimize the orientation of the product during processing and thereby its strength.
Post-processing	Sanding, painting, and coating typically increase the strength of a 3D printed object, as these steps ensure that any irregularities in the product's surface are filled in.
Annealing	A technological process that consists in slowly heating and cooling the printed product, which significantly improves the strength and heat resistance of materials such as PLA. This process, suitable for parts produced with strong 3D printing materials, can relieve internal stresses and rearrange the molecular structure of the product's material, thereby improving its mechanical properties.
Print speed	Lower print speeds result in more durable products due to optimal heating and curing.
Shell thickness	A typical 3D printed design has a shell thickness of only 1.0–1.5 mm, but greater thickness can significantly improve the tensile strength and impact resistance of the product.

Source: own elaboration.

It is also a good idea to use functional technological rounding on the thin areas of the 3D model to reinforce them and reduce their proneness to tearing and cracking. This technique will also reduce the load on the model and make the design sturdier. The layering of the structure should also be considered, as it can become a weak point, as layers can separate. This problem can be solved by printing the layers at different angles.

It is also recommended to use prototyping before printing important elements, where a "draft" functional model of the ABS/PLA product is manufactured to analyze and eliminate potential design errors that could lead to failures or loss in durability. Next, relying on the created mock-up (model), an already optimized version (using the intended construction material) is sent for printing.

Today, designs created with additive technologies can possess such properties as high heat resistance, hardness, durability, and even biocompatibility. Composite materials used for 3D printing can contain various particles, notably wood, carbon, metal, or ceramic particles (Tang, 2024).

CONCLUSIONS

The study demonstrated that information security is among the topical issues in the digitalization of business processes. The current situation calls for a comprehensive approach to protecting the object of informatization, which includes regulatory protection and a modern technological system for comprehensive information security. The introduction of the mobile RoboTurtle into university infrastructure is an important and time-consuming problem. Nonetheless, with a series of necessary measures, it will solve a wide range of topical tasks of the admission campaign and attract applicants through gamification elements with the help of a set of basic information and communication rules and technologies of the university.

To enable the mobile robotic platform to collect forms and forward them to the university database, it is necessary to decide on the right hardware and software for all its required components. A combination safe will work as the RoboTurtle's form collection container. The main casing, equipped with a machine vision camera, sensors, secure Wi-Fi for communication, and a base for recharging the battery at the end of the workday, should be made of strong and lightweight materials that can withstand significant loads and are resistant to damage. Printed or molded parts from composite materials (where carbon fiber can be added if necessary) may be a good choice. In addition, it is important to consider the features of 3D printer settings to prevent defects, material overruns, and design flaws. The younger generation is a complex and dynamic foundation of the future of society and the state. Therefore, it is important to start teaching youth to competently interact with digital environments now to ensure that the innovations and inventions that used to feature only in science fiction not become prototypes for technological disasters (also described in detail by science fiction writers and futurologists) but instead help prevent threats and challenges to public safety, protect the interests of human beings and the Earth's biosphere in all their manifestations, assisting future generations in finding a path to mutually beneficial coexistence and constructive cooperation.

The study was financed by the Moscow Polytechnic University under the V.E. Fortov grant.

REFERENCES

Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and beyond: The future of wireless communications systems. ***IEEE Access,*** 8, 133995-134030. https://doi.org/10.1109/ACCESS.2020.3010896

Çam, E., & Kiyici, M. (2022). The impact of robotics assisted programming education on academic success, problem solving skills and motivation***. Journal of Educational Technology and Online Learning,*** *5*(1), 47-65. https://doi.org/10.31681/jetol.1028825

Esenogho, E., Idiagi, N., & Igimoh, J. A. (2013). Development and implementation of a biometric security lock system. ***Journal of Nigeria Association of Production Engineers NIPRO-DE***, 14, 121-133.

Ikechukwu, L. (2024). Everything you should know about Wi-Fi security. Smallstep. https://smallstep.com/blog/everything-wifi-security/

Khochueva, F. A., & Shugunov, T. L. (2020). Ensuring information security as a key factor in the development of the digital economy in the Russian Federation. Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy. Yekaterinburg, Russia. https://doi.org/10.2991/aebmr.k.201205.042

Monoscalco, L., Simeoni, R., Maccioni, G., & Giansanti, D. (2022). Information Security in Medical Robotics: A Survey on the Level of Training, Awareness and Use of the Physiotherapist. ***Healthcare (Basel, Switzerland)***, ***10***(1), 159. https://doi.org/10.3390/healthcare10010159

Parandoush, P., Zhou, C., & Lin, D. (2019). 3D printing of ultrahigh strength continuous carbon fiber composites. ***Advanced Engineering Materials, 21***(2). http://dx.doi.org/10.1002/adem.201800622

Pitelinskii, K. V., Makovei, S. O., & Buikin, A. Iu. (2024). Intellektualnye sistemy v sfere obrazovaniia: Avatary epokhi kiberpanka. Proceedings of the XX International Congress with elements of scientific school for young scientists. Moscow, Russia.

Pitelinskii, K. V., Makovei, S. O., & Sigida, M. P. (2021). Robotizirovannye bionicheskie apparaty kak sredstvo effektivnoi realizatsii upravlencheskikh reshenii v VUCA-mire — Izuchenie zarubezhnogo voennogo opyta. ***Defense Industry Achievements — Russian Scientific and Technical Progress, 2***(150), 49-57. https://doi.org/10.52190/1729-6552_2021_2_49

Pitelinskii, K. V., Makovei, S. O., & Sigida, M. P. (2022). Robotizirovannye sistemy v usloviiakh pandemii COVID-19: Tendentsii i znachimost primeneniia. Proceedings of the 10th Scientific conference. Moscow, Russia. https://doi.org/10.36535/2022-9785945770829-54

Robai, M. P. (2024). Extensive review of security and privacy issues in heterogeneous networks. ***World Journal of Advanced Research and Reviews, 23***(1), 2955-2984. https://doi.org/10.30574/wjarr.2024.23.1.2308

Sadkhan, S. B., & Abbas, N. A. (2016). Privacy and security of wireless communication networks. In: Information Resources Management Association, Mobile computing and wireless networks: Concepts, methodologies, tools, and applications***. IGI Global,*** 2016, 1798-1818. https://doi.org/10.4018/978-1-4666-8751-6.ch080

Seleman, Y. (2016). Security threats to wireless networks and modern methods of information security. ***Global Journal of Computer Science and Technology, 16***(E2), 1–4. https://computerresearch.org/index.php/computer/article/view/1358

Sun, R., & Zhou, Y. (2022). Application and development of nano material technology in archives protection technology. ***Integrated Ferroelectrics, 228***(1), 17-34. http://dx.doi.org/10.1080/10584587.2022.2072119

Tang, C. (2024). Research on the structure and materials of 3D printing technology. ***Applied and Computational Engineering, 89***(1), 93-96. https://doi.org/10.54254/2755-2721/89/20241089

Tomo Licardo, J., Domjan, M., & Orehovački, T. (2024). Intelligent robotics—A systematic review of emerging technologies and trends. ***Electronics, 13***(3), 542. https://doi.org/10.3390/electronics13030542