SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

RISKS OF TRADITIONAL PASSWORD SYSTEMS IN THE CONTEXT OF ENTERPRISE DISTRIBUTED INFORMATION SYSTEMS

V. A. Dokuchaev [1,2], **I. A. Safonov** [3], **J. Rahmani** [4]

[1] Network Information Technologies and Services, MTUCI, Moscow, Russia, v.a.dokuchaev@mtuci.ru

[2] International Telecommunication Union (GCBI ITU), Geneva, Switzerland

[3] Network Information Technologies and Services, MTUCI, Moscow, Russia

[4] Network Information Technologies and Services, MTUCI, Moscow, Russia

j.rahmani@mtuci.ru

ABSTRACT

Traditional password-based authentication systems continue to be used in modern corporate distributed information systems, despite their vulnerabilities. This article examines the threats associated with traditional password systems, including the psychological aspects of their use, technical shortcomings, and regulatory gaps. Examples of real-world attacks, such as phishing campaigns and credential compromises in industrial information networks, are discussed. Particular attention is paid to password protection in industrial Internet of Things (IIoT) and smart grid systems. Practical recommendations for improving security are offered, including the use of multifactor authentication, credential rotation, the elimination of preset passwords, and the implementation of the Zero Trust concept.

DOI: 10.36724/2664-066X-2025-11-4-15-24

Received: 20.06.2025
Accepted: 23.08.2025

Citation: V. A. Dokuchaev, I. A. Safonov, J. Rahmani, "Risks of traditional password systems in the context of enterprise distributed information systems", *Synchroinfo Journal* **2025**, vol. 11, no. 4, pp. 15-24.

KEYWORDS: *authentication; vulnerabilities; password; IIoT; Smart Grid; Zero Trust; cybersecurity*

Introduction

Traditional password authentication systems remain the primary means of authentication in corporate and critical infrastructures despite growing cyber threats. In 2024, 64% of data breaches worldwide were linked to password compromise, and the average cost of a single incident for businesses reached $4.45 million [1,2]. The number of targeted attacks on industrial facilities increased by 35% over the last two years in Russian Federation. We'll examine the risks of traditional password systems, supported by research and real-world examples from energy, banking, transportation, and the Industrial Internet of Things (IIoT). We'll focus on vulnerability analysis, regulatory requirements, and innovative information security solutions.

Key factors affecting data protection

Modern information security studies unanimously indicate that the human factor remains the main weak link in data protection. According to the Verizon Data Breach Investigations Report (2022), 30% of users still choose primitive passwords such as “123456” or “qwerty,” which demonstrates the persistence of cognitive economy—the tendency to minimize mental effort when memorizing [3]. This trend is exacerbated by the practice of password reuse: 65% of employees use the same credentials for work and personal accounts, violating the principle of account segregation [4].

Phishing attacks, which account for 85% of successful intrusions, exploit fundamental psychological triggers. For example, in 2021 attackers targeted the American company Colonial Pipeline by sending an email with a fake notification from management. An employee entered the password “Colonial2021!” into a phishing form, which allowed the attackers to deploy the DarkSide ransomware and paralyze the operation of the pipeline. The damage amounted to $4.4 million, including the ransom paid in bitcoins [5]. Figure 1 shows the distribution of methods of successful attacks on organizations.

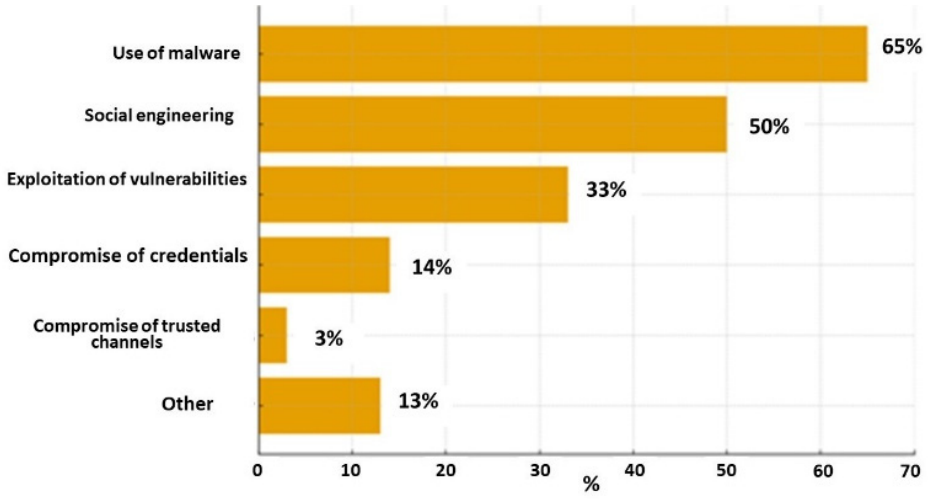

Figure 1. Distribution of Successful Attack Methods Against Organizations

Vulnerabilities of password systems are exacerbated by the technical archaism of infrastructures. According to the ENISA Report on ICS Security (2024), 40% of industrial systems in the EU still use the Telnet and FTP protocols, which transmit passwords in plaintext. This enables attackers to intercept data through sniffing attacks, as occurred in 2023 in Poland, where attackers decoded a password from unencrypted Telnet traffic of a power-grid control system [6].

Cryptographic algorithms also remain an Achilles’ heel. The MD5 and SHA-1 hash functions, used in 30% of corporate systems, are vulnerable to collisions and rainbow tables. For example, RFC 6238 (2024) estimates that cracking an MD5 hash for the password “admin123” takes only 2 seconds [7].

Organizational errors in password management often act as a catalyst for large-scale attacks. A vivid example is the Maersk incident (2017), where exploitation of the EternalBlue vulnerability in SMBv1 led to the spread of the NotPetya ransomware. The attack was made possible by the lack of network segmentation and the use of a single password for all administrative accounts. The company's losses exceeded $300 million, including the downtime of 76 port terminals [8].

A key problem remains the weak adoption of multi-factor authentication (MFA). According to NIST Special Publication 800-63B (2024), only 22% of companies use MFA for all employees, which contradicts the principles of Zero Trust – an architecture that requires verification of every request regardless of its source [9, 10].

Examples of attacks on critical information infrastructure

In the modern world, cyberattacks on critical infrastructure are becoming increasingly sophisticated, demonstrating how digital threats can transform into physical destruction and socio-economic crises (the transition of information-security incidents into industrial-safety incidents). The incidents considered below not only influenced approaches to information security but also showed that the vulnerabilities of industrial and energy systems require a global rethinking of defense strategies.

The use of the ransomware (encryptor) Stuxnet became the first cyberattack aimed at the physical sabotage of industrial equipment. The specialized malicious software was created to attack Siemens SCADA systems used at the Iranian nuclear facility in Natanz. The virus spread via infected USB drives, exploiting several zero-day vulnerabilities in Windows. Thanks to stolen digital certificates, Stuxnet remained unnoticed, gradually modifying the control parameters of centrifuges. This led to their abnormal operation, physical wear, and failure of about 1,000 units of equipment. The consequences of the attack forced the global community to revise standards for protecting critical facilities, emphasizing the need to isolate industrial networks from external threats [11].

The attack by attackers using the NotPetya encryptor quickly grew into a global cyber-pandemic. The malware used the EternalBlue vulnerability in the Windows SMB protocol, similar to the WannaCry exploit, to encrypt hard drives and block the operation of computers. Government agencies, logistics giants such as Maersk, and industrial enterprises around the world became victims. The economic damage exceeded $10 billion, and the scale of the spread showed how a local incident can trigger an international crisis. NotPetya also emphasized the importance of timely software updates and segmentation of corporate networks [12-14].

A group of attackers used the BlackEnergy malware, distributed through phishing emails, to penetrate the SCADA systems of energy companies. After gaining access, the attackers shut down several substations, leaving more than 200,000 people without electricity. Additional data-wiping methods complicated recovery, turning the attack into an example of well-planned sabotage. This incident became a starting point for the development of new standards for protecting energy facilities from cyberthreats [15].

Internet of Things (IoT) devices [16] are of significant interest to attackers. The Mirai botnet demonstrated the danger of the widespread use of unsecured IoT devices. The malware scanned the internet for gadgets with default passwords, combining them into a network for large-scale DDoS attacks. In October 2016, the attack on the DNS provider Dyn caused the collapse of services such as Twitter, Netflix, and GitHub. The event led to stricter security requirements for IoT devices and a reassessment of the role of "smart" technologies in critical infrastructure [17].

Password attack methods

Protecting credentials remains one of the key tasks of information security; however, attackers are constantly improving methods of compromising passwords. Modern attacks combine technical vulnerabilities with manipulation of the human factor, which makes them especially dangerous. Below are the main strategies used to steal or crack passwords, as well as their impact on the security of information systems.

Phishing, as a method of social engineering, is aimed at deceiving users in order to obtain their credentials. Attackers imitate trusted services by sending fake emails, SMS messages, or making voice calls. Victims are redirected to fake web pages that are visually indistinguishable from the original platforms, where they enter their logins and passwords. This method remains one of the most widespread due to its ease of implementation and high effectiveness, especially under conditions of insufficient user awareness [18].

Figure 2 shows the distribution of social-engineering channels used by attackers.

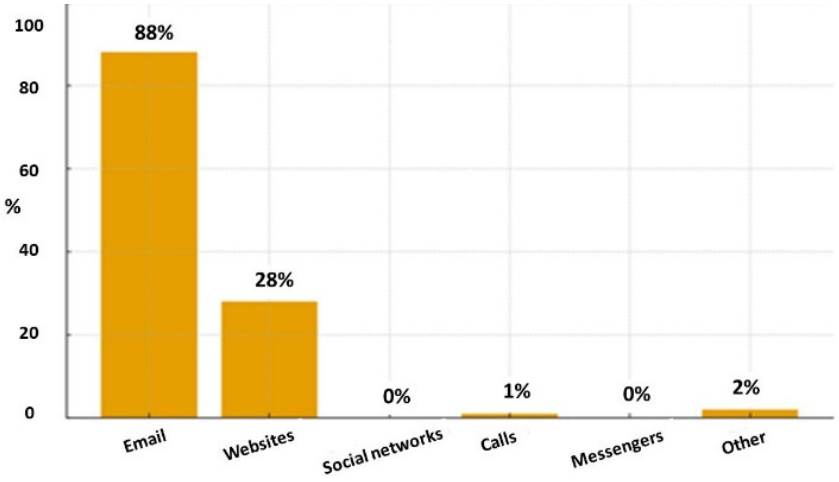

Figure 2. Distribution of Social Engineering Channels Used by Attackers

Credential stuffing attacks are based on exploiting the human habit of reusing passwords across different resources. Attackers use automated bots to test credentials that leaked in the past across numerous platforms. A login–password combination compromised as a result of a social-network breach can be used to access banking services or corporate systems. The effectiveness of this method grows due to large-scale database leaks and the weak adoption of multi-factor authentication.

Real-time data interception is another threat to password confidentiality. A Man-in-the-Middle (MitM) attack is carried out over unsecured public Wi-Fi networks, where an attacker inserts themselves into the communication channel between the user and the server. This attack technique includes substituting SSL certificates, which makes it possible to decrypt traffic, or redirecting the victim to phishing resources. This approach is especially dangerous for employees working remotely and underscores the need to use a VPN and strict certificate validation.

Direct password-guessing methods remain relevant despite the development of defensive mechanisms. Brute-force attacks involve systematically enumerating all possible character combinations, which requires significant computing resources but is effective against short or simple passwords. A dictionary attack, in turn, uses precompiled lists of popular words, phrases, or passwords from past leaks. Both methods are often combined with acceleration tools such as task parallelization on GPUs, which makes them a threat even to systems with basic protective measures.

Let us give an example of the probability of cracking a password by the brute-force method. In the modern digital world, the resistance of a password to brute-force attacks is a key aspect of data protection. Attackers use increasing computing power and optimized algorithms to crack weak combinations in a matter of hours. However, the reliability of a password depends not only on its length, but also on the diversity of characters, as well as on the strategies used to slow down attacks. We introduce the following designations:

N – total number of unique passwords;
C – size of the character set;
L – password length;
P – probability of a successful password guess;
K – number of attacker attempts;
T – time, in seconds;
R – guessing speed (attempts per second);
S – number of parallel processes;
$P(t)$ – probability of compromise within time t (in seconds);

H – entropy.

Total number of possible combinations: $N = C^L$.

Probability of a successful crack after K attempts: $P = K/N$.

Time required to crack: $T = \frac{N}{R * S}$.

Probability of a crack within time t: $P(t) = \frac{t * R * S}{N}$.

Password entropy: $H = L \cdot \log_2(C)$.

Password strength is determined by its entropy – a measure of uncertainty it creates for an attacker. According to NIST standards, the minimally acceptable entropy is 80 bits, which is achieved through a combination of password length (a minimum of 12 characters is recommended) and character diversity: letters (lowercase and uppercase), digits, and special symbols. For example, a 12-character password using 76 available symbols (Latin letters, digits, special characters) provides about 85 bits of entropy, which makes it resistant to attacks even at a high guessing speed (up to 1 billion attempts per second).

However, it is important not only to create a complex password but also to consider its lifetime: if an attacker would need years to crack it, such a password can be considered reliable. For critical systems, an additional level of protection is provided by two-factor authentication, which reduces the probability of a successful compromise to a minimum even if the password is exposed.

According to studies [18], phishing and credential stuffing occupy leading positions in terms of frequency of use, whereas brute-force attacks are gradually losing relevance due to the introduction of lockout mechanisms after multiple attempts. Thus, it can be concluded that password security depends not only on their complexity, but also on user behavior, the quality of traffic encryption, and the timely updating of security policies. A combination of technical measures – such as multi-factor authentication – and regular employee training makes it possible to reduce risks, turning the password from a weak link into a reliable barrier to attackers.

Regulatory legal documents defining password requirements

In Russia, the information security of critical infrastructures is regulated by a number of documents aimed at minimizing risks associated with vulnerabilities of password systems. FSTEC Order No. 239 establishes the mandatory use of passwords at least 12 characters long for state institutions and strategic enterprises, which is consistent with the international standards NIST SP 800-63B [19].

However, as shown by a 2024 study by Kaspersky Lab [20], 45% of Russian companies do not comply with this requirement, limiting themselves to passwords of 8-10 characters. This is due both to employees' cognitive resistance and to the absence of automated control systems.

The Decree of the President of the Russian Federation No. 250 [21] supplements these measures with a requirement for network segmentation and regular password audits at critical information infrastructure facilities. Despite this, studies by Positive Technologies show that 80% of attacks on industrial enterprises are associated with the use of default passwords such as "admin" or "1234" [22].

This indicates a systemic failure in identity and access management (IAM), especially in the segment of IoT devices, where firmware updates often require stopping production processes. Figure 3 shows the distribution of "victim organizations" by industry, which confirms the need to ensure security in the industrial sector.

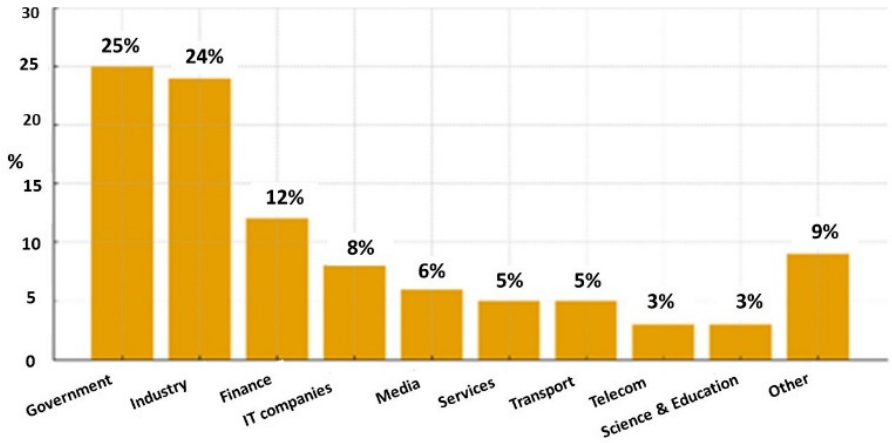

Figure 3. Victim Organizations by Industry

According to Kaspersky Lab's 2024 report [20], 60% of Russian companies do not conduct regular password audits, which contradicts the requirements of GOST R ISO/IEC 27002-2021. This creates conditions for latent threats such as unauthorized access to industrial process control systems (ACS TP).

A 2023 study by Positive Technologies [17] revealed that 55% of incidents in industry are associated with insiders abusing privileged accounts. For example, in the energy sector employees often use administrative passwords for remote access, ignoring the principle of least privilege (PoLP).

In an analysis of cyberattacks conducted by Rostelecom [23], it is noted that 30% of incidents start with employee phishing, which correlates with global trends. Targeted campaigns (spear phishing), in which attackers use social engineering to gain access to SCADA systems, are particularly dangerous.

Threats to critical information infrastructures

Critical information infrastructures (CII) around the world face a growing number of cyberthreats driven by increasing digitalization and the integration of network technologies. Among the most vulnerable areas are the Industrial Internet of Things (IIoT), smart grids (Smart Grid), and transport and logistics control systems. These domains are united by their reliance on network technologies and the need to maintain high reliability. However, these very characteristics make them targets for attackers.

The spread of industrial IIoT devices has made it possible to significantly increase production efficiency and automate many processes; however, this progress is accompanied by new threats [24,25]. One of the main problems is that a significant portion of such devices remains insufficiently protected due to the use of preinstalled passwords. A study by Positive Technologies showed that the owners of 15% of IIoT devices have never changed the default credentials, which makes them vulnerable to attacks using guessing methods [26]. In addition, industrial IIoT devices often have limited computing resources, which makes it impossible to use modern encryption algorithms and complex authentication mechanisms. As a result, attackers can intercept control commands and inject malicious commands into automated systems, which can lead to production downtime or even industrial accidents [27].

The energy industry, as one of the most important parts of critical infrastructure, also faces serious cybersecurity challenges. One key problem is the insufficient level of authentication when accessing control systems. In a number of energy companies there is no mandatory requirement to use multi-factor authentication (MFA), which increases the risk of credential compromise and unauthorized access to SCADA systems [28]. In addition, outdated software continues to be operated at many substations and distribution nodes. According to the European Union Agency for Cybersecurity (ENISA), about 40% of energy facilities in the EU run software with known vulnerabilities [29]. This creates preconditions for attacks that exploit zero-day methods, which can lead to power outages over large areas.

The transport [30,31] and logistics sector is also susceptible to cyberthreats, since traffic control systems, airports, seaports, and railway hubs actively use network technologies for coordination and process optimization. However, in many cases the security of such systems remains insufficient. One common problem is the use of default or weak passwords to access control systems. In a number of cases, the operational networks of transport hubs are not separated from corporate information and telecommunications networks, which creates an additional threat. The lack of clear segmentation allows attackers who have gained access to one system to spread the attack to other critical nodes. This can lead to transport delays, disruptions in logistics chains, and significant financial losses.

Recommendations for protecting industrial internet of things (IIoT) systems and devices

The Industrial Internet of Things (IIoT) is a rapidly evolving environment in which intelligent devices, sensors, and automated control systems interact. Under these conditions, traditional password-based authentication methods face significant risks, including brute-force attacks, phishing, and the exploitation of preinstalled credentials. In this regard, it is critically important to implement reliable mechanisms for protecting credentials.

First and foremost, it is necessary to completely abandon preinstalled passwords and apply methods of automatic password rotation. This will minimize the likelihood that attackers will successfully guess credentials. An important aspect of protection is the use of multi-factor authentication (MFA), including a combination of hardware tokens, biometric data, and cryptographic keys. This approach significantly increases the level of security and reduces the risk of account compromise.

Additionally, attention should be paid to network segmentation and access control. IIoT devices must operate in separate network segments with clearly defined routing rules and access restrictions through identity and access management (IAM) systems. This will prevent unauthorized interaction attempts between devices and increase resilience to attacks. It is also critically important to update firmware regularly and apply security patches, since software vulnerabilities can be used to bypass authentication mechanisms.

In addition, secure data-transfer protocols must be used. Outdated and insecure protocols such as Telnet and FTP should be replaced with protected alternatives. This will ensure reliable encryption of transmitted data and prevent the possibility of interception by attackers.

Smart grids are a key element of modern energy infrastructures, providing efficient management of power distribution. However, the high degree of digitalization of these systems makes them vulnerable to various attacks, including the compromise of operator credentials and the hacking of control devices. In this regard, protecting passwords and credentials in such environments requires a comprehensive approach.

The most promising authentication method in smart grids is the use of X.509 digital certificates in combination with hardware security modules (HSM). This makes it possible to eliminate dependence on traditional passwords and ensure a high level of account protection. It is also important to implement strict password-management policies, including the mandatory use of complex passwords of at least 14 characters with regular rotation.

To prevent privilege-escalation attacks, it is necessary to apply the principle of least privilege (PoLP) and use specialized privileged access management (PAM) systems. This will limit the possibility of unauthorized use of high-privilege accounts. In addition, special attention should be paid to monitoring authentication events using security information and event management (SIEM) systems. Analysis of account behavior will allow prompt detection of anomalies, such as login attempts from unusual locations or at unusual times.

Additionally, methods for encrypting communication channels should be employed. All communication between smart-grid components must be carried out through protected and certified VPN tunnels. This will prevent man-in-the-middle attacks and increase the overall resilience of the infrastructure to threats.

Control systems for critical facilities – such as water supply, transport hubs, and industrial enterprises – require strengthened protection of credentials, since their compromise can lead to catastrophic consequences. Under such conditions, it is necessary to implement the Zero Trust concept, in which trust in a user is formed on the basis of multi-factor identification regardless of their location.

One of the key aspects of protection is the regular auditing of accounts. All inactive and obsolete accounts must be removed in a timely manner, and access rights must be reviewed regularly using role-based models (RBAC). This will minimize risks associated with inherited or forgotten accounts that could be used by attackers.

The use of hardware authentication means – including PKI tokens and WebAuthn technologies – plays an important role. These methods eliminate dependence on static passwords and significantly complicate the possibility of account attacks. In addition, strict control over remote access must be ensured. Control systems must be completely isolated from external networks, and remote access must be carried out exclusively through protected gateways with additional verification.

Finally, increasing staff awareness remains an important element of protection. Regular training and testing will help employees promptly recognize phishing attacks and handle credentials safely, which will significantly reduce the likelihood of account compromise.

Prospective authentication methods

Biometric authentication is becoming increasingly popular due to its high reliability and ease of use. Modern methods include fingerprint recognition, iris scanning, facial recognition, and even gait or heartbeat analysis. These technologies significantly reduce risks associated with theft or leakage of credentials, since biometric data are difficult to forge or transfer to third parties. However, biometric authentication also faces challenges related to data privacy and the possibility of compromise in the event of leaks. It is important to use secure methods for storing biometric templates.

The FIDO2 and WebAuthn protocols offer a fundamentally new approach to authentication that eliminates the need for passwords. Instead, cryptographic keys stored on hardware tokens or in special device modules are used. This approach removes risks associated with phishing and password interception, because authentication is tied to a specific device and does not require transmitting secret data over the network. The development of this area promotes a transition to fully passwordless authentication, increasing the security level of corporate and critical systems.

The concept of decentralized identification systems (Decentralized Identifiers, DID) is based on the use of blockchain and distributed ledgers to store and verify digital identity credentials. Unlike traditional centralized systems, DID allows users to manage their own digital identifiers, removing the need to trust third parties. This is especially important in the context of protecting personal data and preventing information leaks. However, large-scale adoption is still limited by a lack of regulatory standards and the need to refine infrastructure to support decentralized solutions.

Artificial intelligence (AI) and machine learning play an increasing role in authentication systems. User-behavior analysis algorithms make it possible to detect suspicious activity and adapt authentication mechanisms in real time. Systems can track typing speed, geolocation, login time, and other parameters to automatically request additional authentication when anomalies are detected. This approach can significantly reduce the likelihood of compromise even if credentials are exposed. In addition, AI is used to improve biometric systems, increasing recognition accuracy and reducing false positives. In the future, artificial intelligence may become a key element of adaptive authentication, providing a balance between security and user convenience.

Conclusion

The analysis has shown that traditional password systems remain a vulnerable link in the protection of corporate distributed systems and critical infrastructures such as the Industrial Internet of Things, smart grids, and infrastructure control systems.

The main problems include the human factor, outdated protocols, shortcomings in access management, and non-compliance with regulatory requirements. The implementation of Big Data and Artificial Intelligence technologies, while being powerful drivers of economic development, simultaneously gives rise to new potential risks of unauthorized access to confidential information. To minimize risks, it is necessary to apply a comprehensive approach that includes strengthened authentication, strict password management policies, the use of hardware security measures, and continuous monitoring of security events. The implementation of the Zero Trust concept and multi-factor authentication will significantly reduce the likelihood of successful attacks and increase the resilience of the infrastructure to information security threats.

REFERENCES

[1] Verizon Data Breach Investigations Report [Online], 2022. Available: https://www.verizon.com/business/resources/reports/dbir (accessed 03.01.2025).

[2] V. A. Dokuchaev, “Digital transformation: New drivers and new risks,” *2020 International Conference on Engineering Management of Communication and Technology (EMCTECH 2020): Proceedings*, Vienna, October 20-22, 2020. New York: Institute of Electrical and Electronics Engineers (IEEE), 2020, p. 9261544. DOI: 10.1109/EMCTECH49634.2020.9261544.

[3] OWASP Authentication Cheat Sheet [Online]. Available: https://cheatsheetseries.owasp.org (accessed 17.01.2025).

[4] Google Security Blog [Online], 2019. Available: https://security.googleblog.com (accessed 12.02.2025).

[5] NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63b (accessed 07.01.2025).

[6] ENISA Report on ICS Security [Online]. Available: https://www.enisa.europa.eu (accessed 10.01.2025).

[7] RFC 6238 (TOTP): Time-Based One-Time Password Algorithm [Online]. Available: https://tools.ietf.org/html/rfc6238 (accessed 13.01.2025).

[8] Zero-Trust Network Architecture [Online] / Forrester Research, 2020. Available: https://www.forrester.com/zero-trust/ (accessed 15.02.2025).

[9] NIST Special Publication 1108R3. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: NIST, 2020.

[10] E. S. Yusifov, V. A. Dokuchaev, “Why Kubernetes security problems require a zero-trust strategy,” *Information Society Technologies: Proceedings of the XVII International Industry Scientific and Technical Conference*, Moscow, March 2-3, 2023. Moscow: Media Publisher, 2023, pp. 116-118.

[11] J. Rahmani, “Study of risk-management methods in the infocommunication system of an energy-producing company of the Islamic Republic of Iran,” *T-Comm*, 2022, vol. 16, no. 8, pp. 30-37. DOI: 10.36724/2072-8735-2022-16-8-30-37.

[12] V. A. Dokuchaev, N. S. Kalmykov, “Aspects of applying segment routing in software-defined networks,” *Prospective Technologies in Information Transmission Media: Proceedings of the 14th International Scientific and Technical Conference*, Vladimir, October 6-7, 2021. Vladimir: Vladimir State University named after A. G. and N. G. Stoletovs, 2021, pp. 164-168.

[13] J. Rahmani, “The main approaches to evaluating the effectiveness of applying the risk analysis and management methodology at energy company,” *T-Comm*, 2022, vol. 16, no. 9, pp. 46-55. DOI: 10.36724/2072-8735-2022-16-9-46-55.

[14] N. S. Kalmykov, V. A. Dokuchaev, “Analysis of the main methods for ensuring network security in software-defined networks,” *Telecommunication and Computing Systems 2020: Proceedings of the International Scientific and Technical Conference*, Moscow, December 14-17, 2020. Moscow Technical University of Communications and Informatics. Moscow: Goryachaya Liniya – Telecom, 2020, pp. 63-70.

[15] V. A. Dokuchaev, A. A. Kalfa, J. Rahmani, “Typical structure of the corporate infocommunication system of an energy-producing company (IRI),” *III Scientific Forum “Telecommunications: Theory and Technology” TTT-2019: Proceedings of the XXI International Scientific and Technical Conference*, Kazan, November 18-22, 2019. Vol. 1. Kazan: Kazan National Research Technical University named after A. N. Tupolev, 2019, pp. 298-299.

[16] V. A. Dokuchaev, A. V. Shvedov, A. V. Ermalovich, “The “Internet of Things” concept as the basis for the development of information and communication technologies (ICT),” *Current Problems and Prospects for Economic Development: Proceedings of the Jubilee XV International Scientific and Practical Conference*, Gurzuf, November 17-19, 2016 / Crimean Federal University named after V. I. Vernadsky. Gurzuf: IP Brovko A. A., 2016, p. 298.
[17] J. Rahmani, V. A. Dokuchaev, “Analysis of trends in the development of the communications industry in the Islamic Republic of Iran,” *Information Society Technologies: Proceedings of the XIV International Industry Scientific and Technical Conference*, Moscow, March 18-19, 2020. Moscow: Media Publisher, 2020, pp. 300-301.
[18] E. A. Petinova, N. Kh. Odinaev, “Phishing analysis: statistics, methods and solutions in cybersecurity,” *Youth. Science. Future. 2024: Collection of Papers of the II International Scientific and Practical Conference*, Petrozavodsk, April 22, 2024. Petrozavodsk: IP Ivanovskaya I. I., 2024, pp. 143-153. DOI: 10.46916/24042024-3-978-5-00215-361-9.
[19] Order of the FSTEC of Russia of December 25, 2017 No. 239 “On the approval of requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation” [Online]. Available: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed 21.04.2025).
[20] Kaspersky. Kaspersky Lab analytical reports 2024 [Online]. Available: https://securelist.ru/kaspersky-incident-response-report-2024/112080/ (accessed 21.04.2025).
[21] Decree of the President of the Russian Federation No. 250 of 01.05.2022 “On additional measures to ensure the information security of the Russian Federation” [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001202205010023 (accessed 21.04.2025).
[22] Positive Technologies. Outcomes of IS incident investigations in 2021–2023 [Online], 2023. Available: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years (accessed 02.02.2025).
[23] Solar. Attacks on Russian companies in Q2 2023 [Online], 2023. Available: https://rt-solar.ru/analytics/reports/3610/ (accessed 13.02.2025).
[24] V. Yu. Statyev, V. A. Dokuchaev, V. V. Maklachkova, “Information security in the Big Data space,” *T-Comm*, 2022, vol. 16, no. 4, pp. 21–28. DOI: 10.36724/2072-8735-2022-16-4-21-28.
[25] V. A. Dokuchaev, “The impact of new information and communication technologies on the privacy of personal data,” *Current Problems and Prospects for Economic Development: Proceedings of the XXIII International Scientific and Practical Conference*, Simferopol–Gurzuf, October 17-19, 2024. Simferopol: IP Zueva T. V., 2024, pp. 12-15.
[26] Positive Technologies. Owners of 15% of IoT devices have never changed the default password — Xakep [Online]. Available: https://xakep.ru/2017/06/20/iot-stats/ (accessed 04.03.2025).
[27] Threats to IoT devices in 2023 | Securelist [Online]. Available: https://securelist.ru/iot-threat-report-2023/108088/ (accessed 10.03.2025).
[28] European Union Agency for Cybersecurity (ENISA). EU Cybersecurity in 2024: Insights from ENISA Latest Report [Online]. Available: https://cyble.com/blog/eu-cybersecurity-in-2024-insights-from-enisa-latest-report/ (accessed 14.02.2025).
[29] Threats to the energy sector. Analytical report. CISA, 2023 [Online]. Available: https://www.cisa.gov/sites/default/files/2024-09/FY23_RVA_Analysis_508.pdf (accessed 13.02.2025).
[30] V. A. Dokuchaev, “Analysis of international recommendations on transport security under digital transformation,” *Trends in the Development of the Internet and Digital Economy: Proceedings of the VI International Scientific and Practical Conference*, Simferopol–Alushta, June 1–3, 2023. Simferopol: IP Zueva, 2023, pp. 15-17.
[31] V. A. Dokuchaev, “Some aspects of transport security under digital transformation,” *Theory and Practice of Economics and Entrepreneurship: Proceedings of the XX International Scientific and Practical Conference*, Simferopol–Gurzuf, April 20-22, 2023 / Edited by N. V. Apatova. Simferopol: Crimean Federal University named after V. I. Vernadsky, 2023, pp. 31-34.