

Journal Scientific and Applied Research, Vol. 30, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

FINANCING DIGITAL ADMINISTRATIVE SECURITY IN THE PUBLIC SECTOR: CHALLENGES AND PROSPECTS

Iliana K. Simeonova

Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: i.simeonova@shu.bg

Abstract: *The digital transformation of the public sector is changing the way state and local institutions provide administrative services, manage information and interact with citizens and businesses. At the same time, the importance of administrative security in the electronic environment and the need for sustainable financial provision of measures for the protection of information resources, digital infrastructure and administrative processes are growing. This report examines the financing of digital administrative security as an essential component of the modernization and sustainability of the public sector. The main sources of funding, the directions of investment, financial, administrative and technological challenges, as well as the opportunities for more efficient use of public resources are analyzed. Current European and national policies related to digital transformation, cybersecurity and data protection are considered. The need to move from project and reactive financing to a long-term investment model based on risk assessment, performance measurement and ensuring institutional sustainability is argued.*

Key words: ***D****igitalization, Administrative security, Public sector, Cybersecurity, Financing, Risk management, E-government, Digital transformation, Public spending, Institutional resilience.*

1. Introduction

Digital transformation has become one of the main factors for changing public governance. The development of e-government, digital administrative services, cloud technologies, data analytics and artificial intelligence creates opportunities to increase the efficiency, transparency and accessibility of public services. At the same time, however, the dependence of public institutions on information systems, digital infrastructures and electronic communications is growing. This makes the security of the digital administrative environment a strategic issue.

The European Digital Transformation Policy places security, resilience and the development of digital competences among the main prerequisites for successful digital development. Decision (EU) 2022/2481 establishes the Digital Decade Policy Programme until 2030, which provides for the development of secure and resilient digital infrastructures,

digital skills and digitalization of public services. The document explicitly underlines the need to increase resilience against cyber-attacks and investments that combine public and private funding. [9]

In Bulgaria, this policy is specified in the updated National Strategic Document "Digital Transformation of Bulgaria for the Period 2024-2030", adopted by Decision No. 264 of the Council of Ministers of April 4, 2024. [10]

Current data show that Bulgaria continues to invest significant resources in the digital transformation. According to the European Commission's report on Bulgaria for the Digital Decade in 2026, EUR 1.17 billion. of the National Recovery and Resilience Plan is related to the progress of the digital transformation. At the same time, the European Commission reports ongoing challenges in cybersecurity and the deployment of advanced digital technologies.

This shows that the issue is not limited to the availability of financial resources. Its **distribution, prioritization, efficiency and sustainability over time** are essential.

In this context, administrative security should be seen as a state of security of administrative processes, information resources, digital systems and organisational capabilities that ensure the proper functioning of a public institution.

The subject of the study is the digital administrative environment of the public sector.

The subject of the study is the mechanisms and sources for financing digital administrative security, as well as the main challenges to their effectiveness.

The purpose of the report is to analyze the main sources and areas of funding for digital administrative security and to outline opportunities for improving the financial sustainability of the public sector.

2. Theoretical aspects of digital administrative security

2.1. Nature and characteristics of administrative security

Administrative security can be defined as a state and system of organizational, regulatory, informational, personnel and technological measures aimed at protecting administrative processes and resources of the public organization from threats and vulnerabilities.

In the traditional administrative environment, security is mainly associated with the physical protection of documents, premises and tangible assets, access control and compliance with established procedures. Digitalization significantly expands this content.

In an electronic environment, administrative security includes the protection of information systems, databases, electronic documents, digital identity, communication channels and automated processes.

Therefore, four interrelated components can be distinguished: **organizational security** – rules, procedures, distribution of responsibilities and control; **information security** – protection of information from unauthorized access, alteration, destruction or loss; **personnel security** – competence; **security of the work process** – the ability of administrative processes to continue functioning in the event of technical or other violations.

The protection of personal data is of particular importance. Article 32 of Regulation (EU) 2016/679 requires the implementation of appropriate technical and organizational risk-appropriate measures, including ensuring the confidentiality, integrity, availability and resilience of systems and the possibility of timely recovery after an incident.

An important conclusion follows from this: **the financing of digital administrative security is not only an expense for technical infrastructure, but an investment in the ability of the public organization to perform its functions.[6]**

2.2. Digitalisation of the public sector

The digitalization of the public sector includes the implementation of electronic administrative services, automated information systems, cloud technologies, digital registers, electronic identification and tools for big data analysis. The next stage of the transformation is the use of artificial intelligence to support administrative decisions, forecasting workload, anomaly detection and risk management. The European Digital Decade programme places the digitalization of public services among the main measurable goals by 2030 and connects digital governance with secure and interoperable technologies. In Bulgaria, the national roadmap for digital transformation includes the strand of "digital governance", which covers the digitalization of public services. However, digitalization creates a paradox: the more administrative processes are transferred to a digital environment, the greater the need for investment in security becomes. This means that the digitalization budget must include not only funds for the development and deployment of systems, but also fixed costs for their protection, updating, monitoring, redundancy and restoration.

2.3. Risks to the digital administration

Among the main risks, cyberattacks, malware, phishing, compromise of user profiles and leakage of sensitive information stand out. Directive (EU) 2022/2555 – NIS2 – establishes a European framework for a high common level of cybersecurity and introduces stricter requirements for cyber risk management and incident reporting. [7]

Another risk is **insufficient administrative capacity**. The purchase of technological infrastructure does not guarantee security if the institution does not have enough qualified employees to manage it. There is also **technological dependence** on external suppliers. When using cloud services, specialized software or external platforms, the public organization must manage not only its own risks, but also the risks along the supply chain.

Funding should therefore be focused on a comprehensive security system and not on individual technological products.

3. Financing of digital administrative security

3.1. Sources of funding

The main source of funding for digital administrative security is the **state budget**. It ensures the sustainability of the main administrative structures and allows financing of fixed costs – maintenance, updating, personnel and monitoring.

The second significant source is **European funds and programs**. European policy provides for the use of cohesion funds, digitalization programs and other financial instruments to support the digital transition. Decision (EU) 2022/2481 explicitly refers to the possibility of using European and national funds, including resources under Regulation (EU) 2021/241 on the Recovery and Resilience Facility.[9]

A third source is the **National Recovery and Resilience Plan**, through which Bulgaria finances a significant volume of digital investments. According to the European Commission, EUR 1.17 billion of the total resource of the plan is related to the digital transformation.

Another possible tool is **public-private partnerships**, especially in the construction of digital infrastructure and specialized technology services.

In certain areas, resources from international financial institutions and technical assistance can also be used. This is how a multi-channel model is formed:

State budget + European funding + NRRPs + public-private partnerships + international instruments

The main problem is how to coordinate these sources so that one-off projects are not financed without subsequent support.

3.2. Main areas of investment

Funding for digital administrative security can be grouped into several areas.

1. **hardware and communication infrastructure**
2. **software security**
3. **the reservation and restoration of the information**
4. **employee training**
5. **Cybersecurity Monitoring Centers and Systems**
6. **the protection of personal data and digital identity**

Therefore, the optimal investment policy must allocate resources between technologies, people and organizational processes.

3.3. Efficiency of public expenditure – author's model for financing

In the context of limited public resources, the question arises not only how much is invested in security, but also **what result is obtained against the funds spent.** The application of a traditional approach to the assessment of public expenditures on digitalization, based mainly on the size of the investment and the immediate financial result, is insufficient in the financing of administrative security. The reason is that a significant part of the benefits of investments in security are preventive in nature and are manifested by preventing or limiting negative events. In this regard**, an author's risk-based model for financing digital administrative security (BBMF-DAC) is proposed**.

The model is based on the understanding that the amount and priority of the financial resource should be determined not only by the available budget, but by **the criticality of the administrative resource, the probability of the threat materializing, the potential impact and the ability of the institution to prevent, detect and overcome the incident**.

The model is **cyclical**, not linear. After the performance assessment, the results return to the initial stage of risk identification and assessment, thus adapting the financial decision to changes in the technological environment.

First stage: risk identification identify digital assets and administrative processes, the disruption of which would have a significant impact on the functioning of the institution. This may include: information systems; electronic registers; systems for electronic administrative services; databases; digital identity; communication infrastructure; electronic document management systems; critical administrative services.

Second stage: risk assessment - it is proposed that the risk be assessed by a combination of: **probability of the threat and potential impact**

A third indicator can be added to this assessment – **the criticality of the administrative process** and here the following author's formula can be used:

Investment Priority Index (EEI) = B × W × K where:

1. **C** – probability of risk realization;
2. **VD** – potential impact;
3. **K** – criticality of the administrative process.

Each indicator can be evaluated on a five-point scale from 1 to 5.

The obtained value allows the classification of investment needs:

Index	Priority level	Financial action
1–20	Low	Current funding
21–50	Medium	Planned investment
51–80	High	Priority funding
81–125	Critical	immediate/strategic funding



Fig. 1. Author's model for risk-based financing of digital administrative security

Stage three: prioritization of investments - not every digital investment should be financed with the same priority.

For example, an investment in a system that ensures the continuity of a critical administrative service should have a higher priority than an investment in a system of limited importance for the core functions of the institution.

In this way, it is proposed to go from: **"What technology can we buy?"**

to: **"Which risk should we reduce and what investment is needed for this?"**

This is a significant change in the philosophy of budget management.

Fourth stage: determination of the financial resource At this stage, the investment is associated with a specific financial need, divided into:

1. initial investment;
2. implementation costs;
3. training costs;
4. maintenance costs;
5. update costs;
6. monitoring costs;
7. accident recovery costs.

This avoids one of the main problems in public digital investment – the financing of acquisitions without sufficient funds for subsequent exploitation.

4. Main challenges

4.1. Financial constraints: The first major challenge is the limited public resources. Digital security requires not a one-time investment, but **a constant financial resource**. After the purchase of a system, there are costs for licenses, updates, maintenance, training and monitoring. This creates a risk that project financing will lead to the construction of systems whose subsequent maintenance is not sufficiently secured. Smaller public organizations and municipalities, which often have limited human and financial capacity, are particularly vulnerable. Therefore, it is necessary to plan financing at **the life cycle of the investment**, and not only at the stage of its construction.

4.2. Administrative and management problems: Procedural difficulties in public procurement, insufficient number of specialists and poor coordination between institutions are a serious problem. Another problem is the insufficient link between **financial and strategic planning**. Cybersecurity costs must be linked to a specific risk assessment and to the criticality of the administrative service concerned.

4.3. Technological challenges: The technological environment is changing significantly faster than budgetary and administrative cycles. The development of cloud technologies, artificial intelligence and automation creates new opportunities, but also new risks. It is particularly important to avoid fragmentation of information systems. If different institutions use incompatible solutions, data exchange and security control are difficult.

5. Good practices and international experience

International experience shows that successful digital transformation is not based solely on the deployment of technologies; it requires a combination of a political vision, sustainable funding, institutional capacity and high security standards. **Estonia** is one of the most frequently cited examples of comprehensive e-government. A key feature of the Estonian model is the integration of digital services, e-identity and data exchange between institutions. **Denmark** also demonstrates high potential in the field of digital governance and the provision of public services. Sustainable institutional planning of digital investments and consumer orientation are an essential element. **The Finnish** approach is particularly interesting in terms of resilience and cybersecurity, with digital security seen as part of the overall resilience of society.

For Bulgaria, the applicable conclusion is not the mechanical reproduction of foreign models, but the adaptation of their principles to the national administrative structure. The European Commission recognizes that Bulgaria has well-developed connectivity and continues to improve digital public services, but at the same time points to ongoing challenges in cybersecurity and digital skills.

Therefore, future funding should not only focus on scaling up digital services, but at their **security, resilience and long-term functionality**.

6. Perspectives and recommendations

Based on the analysis, several main directions can be formulated for improving the financing of digital administrative security.

First, there is a need for a gradual shift from short-term project financing to **long-term budgetary planning**, which includes the entire lifecycle of the digital system.

Second, funding must be based on **a risk assessment**. Critical administrative systems should receive priority funding according to the potential impact of a possible incident.

Third, there is a need to increase investment in **human capital**. Technology cannot replace a qualified employee; the public sector needs experts in cybersecurity, data management, artificial intelligence and digital project management.

Such investment should also support anticipatory technological preparation, enabling personnel to develop competencies not only for currently deployed systems but also for the critical and secure use of emerging digital technologies [21]

Fourthly, there is a need to develop **interinstitutional and shared infrastructures**, which would allow smaller administrative structures to use common services and expertise.

Fifth, investments in artificial intelligence and predictive analytics should be linked to clear risk management rules. Regulation (EU) 2024/1689 – The Artificial Intelligence Act – establishes a harmonized European framework for artificial intelligence and sets requirements related to the safety, fundamental rights and reliability of certain systems.[8]

Sixth, it is necessary to increase **the transparency of public investments** in digital security. Citizens and institutions must be able to track not only the amount of funds, but also the results achieved.

Seventh, uniform indicators should be introduced to assess the effectiveness of investments, this will allow for comparison of different projects and institutions and will support future budgetary decisions.

3. Conclusion

The digital transformation of the public sector is an irreversible process that changes the organization, the provision of administrative services and the interaction between institutions, citizens and businesses. At the same time, the dependence of public administration on digital technologies is growing, which makes administrative security a basic condition for sustainable e-government.

The analysis shows that the financing of digital administrative security should not be seen as a secondary expense to digitalization. It is an **investment in the institutional sustainability and ability of the public sector to perform its functions**.

European and national policies already create a significant financial and regulatory framework. The national strategic document "Digital Transformation of Bulgaria for the period 2024-2030" provides for specific measures, deadlines and sources of funding, while the European Digital Decade program places digital public services and cybersecurity in a common strategic framework.

At the same time, the availability of significant resources does not automatically guarantee security. The main challenges relate to the sustainability of funding, insufficient administrative capacity, rapid technological developments, dependence on external suppliers and the need for continuous maintenance of digital systems.

Therefore, the future approach should be based on **long-term, risk-based and performance-oriented financing**. It is necessary to move from financing individual digital projects to building a comprehensive system of administrative security. In this system, financial resources, digital technologies, human capital, the regulatory framework and risk management must function as interrelated elements.

In conclusion, it can be assumed that **sustainable financing of digital administrative security is a prerequisite and not a consequence of a successful digital transformation**. Without adequate and long-term planned investments, digitalization can increase not only the effectiveness of public administration, but also its vulnerability.

References

[1] Administration Act. Promulgated SG No. 130 of 05.11.1998, last amended. and supplemented.

[2] Electronic Government Act. Promulgated SG No. 46 of 12.06.2007, last amended and supplemented.

[3] Cybersecurity Act. Promulgated SG No. 94 of 13.11.2018, last amended and supplemented.

[4] Public Finance Act. Promulgated SG No. 15 of 15.02.2013, last amended and supplemented.

[5] Public Sector Internal Audit Act. Promulgated SG No. 27 of 31.03.2006, last amended and supplemented.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. OJ L 119, 4.5.2016.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022. on measures for a high common level of cybersecurity across the Union (NIS2). OJ L 333, 27.12.2022.

[8] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. establishing harmonised rules on artificial intelligence (Artificial Intelligence Act). OJ L, 12.7.2024.

[9] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022. establishing the 2030 Digital Decade Policy Programme OJ L 323, 19.12.2022.

[10] Council of Ministers of the Republic of Bulgaria. Digital transformation of Bulgaria for the period 2024-2030 Decision No 264 of 04.04.2024

[11] Council of Ministers of the Republic of Bulgaria. Strategy for Development of Internal Control in the Public Sector of the Republic of Bulgaria for the period 2023-2026 Decision No 993 of 08.12.2022

[12] European Commission. Bulgaria 2026 Digital Decade Country Report. Brussels, 2026.

[13] European Commission. Bulgaria 2025 Digital Decade Country Report. Brussels, 2025.

[14] OECD. Digital Government Review of Bulgaria: Towards the Digital Transformation of the Public Sector. Paris: OECD Publishing.
[15] OECD. Digital Government Index: 2023 Results. Paris: OECD Publishing.
[16] World Bank. GovTech Maturity Index 2022 Update: Trends in Public Sector Digital Transformation. Washington, D.C.: World Bank.
[17] European Commission. eGovernment Benchmark. Brussels: European Commission.
[18] NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, 2024.
[19] ENISA. ENISA Threat Landscape. European Union Agency for Cybersecurity.
[20] Ministry of e-Government, Republic of Bulgaria. National Roadmap for Digital Transformation of Bulgaria until 2030
[21] Tasinov, T. Y., Toncheva, S. K. Anticipatory Technological Preparation and Digital Health Competencies in Nursing and Midwifery Education. In: Conference Proceedings, XIX National Forum of Health Care Specialists and Poster Session for Students „Fair Access to Quality Health Care“, Shumen, 24–25 October 2025, pp. 97–103.