Electronic scientific and practical journal

INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

#38(2026)
August '26

WWW.SMART-SCM.ORG
ISSN 2708-3195
DOI.ORG/10.46783/SMART-SCM/2026-38

ISSN 2708-3195
9772708319005

Electronic scientific and practical collection
INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

Electronic scientific and practical publication in economic sciences

Electronic scientifically and practical journal “Intellectualization of logistics and Supply Chain Management” included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): **Order of the Ministry of Education and Culture of Ukraine dated June 11, 2026 No. 928 (Appendix 13 item 205).**

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations)
D3 – Management
D5 – Marketing

ISSN 2708-3195
DOI: https://doi.org/10.46783/smart-scm/2026-38

The electronic magazine is included in the international scientometric databases:
Index Copernicus, Google Scholar

Released 6 times a year

№ 38 (2026)
August 2026

Kyiv - 2026

Founder: Viold Limited Liability Company

The electronic scientific and practical journal is registered in international scientometric data bases, repositories and search engines. The main characteristic of the edition is the index of scientometric data bases, which reflects the importance and effectiveness of scientific publications using indicators such as quotation index, h-index and factor impact (the number of quotations within two years after publishing).

In 2020, the International Center for Periodicals (ISSN International Center, Paris) included the Electronic Scientific and Practical Edition "Intellectualization of logistics and Supply Chain Management" in the international register of periodicals and provided it with a numerical code of international identification: ISSN 2708-3195 (Online).

Recommended for dissemination on the Internet by the Academic Council of the Department of Logistics NAU (No. 7 of February 26, 2020). Released 6 times a year. Editions references are required. The view of the editorial board does not always coincide with that of the authors.

Electronic scientifically and practical journal "Intellectualization of logistics and Supply Chain Management" included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): ***Order of the Ministry of Education and Culture of Ukraine dated June 11, 2026 No. 928 (Appendix 13 item 205).***

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations); D3 – Management; D5 – Marketing

facebook.com/Smart.SCM.org
DOI: https://doi.org/10.46783/smart-scm/2026-38
тел.: (063) 593-30-41
e-mail: support@smart-scm.org
https://smart-scm.org

Contents

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

148-161
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-10

UDC 351.78:004.9
JEL Classification: H83, O33, R50

Received: 2026-07-24
Accepted: 2026-08-28
Published: 2026-08-30

Sporyshev K. O. Doctor of Science in Public Administration, Associate Professor, Deputy Head of the Educational and Scientific Institute for Training of Management Personnel in Scientific Work – Head of the Scientific and Research Laboratory of Construction and Operational Application of the National Guard of Ukraine, National Academy of the National Guard of Ukraine, (Ukraine)

ORCID – 0000-0003-4737-9698
Researcher ID J-5960-2018
Scopus author id: – 59047032200
E-Mail: spor_kos@ukr.net

Bondarenko O. H. Doctor of Science in Public Administration, Associate Professor Head of the Logistics Management Department of the Educational and Scientific Institute for Management Training National Academy of the National Guard of Ukraine (Ukraine)

ORCID – 0000-0003-1755-3333
Researcher ID J-5705-2018
Scopus author id: – 57687413400
E-Mail: Alexanderbondarenko77@gmail.com

"SAFE CITY" AS A SECURITY COMPONENT OF THE SMART CITY CONCEPT: PUBLIC AND MANAGEMENT ASPECT

Sporyshev Kostyantyn, Bondarenko Oleksandr "Safe City" as a security component of the Smart City concept: public and management aspect". *The article examines the Safe City concept in the context of Smart City development and determines its public governance dimension in the conditions of digital transformation of the urban environment. It is substantiated that the contemporary understanding of Smart City is gradually moving beyond a purely technological approach and increasingly encompasses the efficiency of public governance, sustainable development, the quality of urban services, human and social capital, and the implementation of data-driven governance. The key components of Smart City – Smart Governance, Smart Economy, Smart Mobility, Smart Environment, Smart People, and Smart Living – are analyzed, with particular attention paid to their security dimension. It is established that security has a cross-cutting nature and includes the protection of information systems and data, cybersecurity, transport and public safety, economic and infrastructure resilience, prevention of environmental and technological threats, and the development of a public safety culture.*

The evolution and transformation of the Safe City concept are examined. A gradual transition is identified from local video surveillance and crime-recording systems towards the integrated use of digital technologies, intelligent video analytics, geographic information systems, Internet of Things devices, big data, and interagency information exchange tools. Particular attention is paid to the changing role of data in urban

148-161
v.38 (2026)
https://smart-scm.org

security governance and its use for monitoring, threat detection, risk assessment, forecasting, and decision-making support.

The public governance dimension of the Safe City system is determined through a combination of monitoring, information and analytical, coordination, organizational, preventive, and control functions, as well as the function of supporting managerial decision-making. It is demonstrated that the digitalization of urban security creates the prerequisites for a transition from a predominantly reactive model of responding to hazardous events towards preventive and risk-oriented governance. It is emphasized that the effectiveness of the Safe City system should be assessed not by the number of surveillance technologies deployed, but by its capacity to ensure timely threat detection, information exchange, interagency coordination, well-grounded managerial decisions, and rapid response while simultaneously respecting human rights and freedoms.

***Keywords**:* Smart City, Safe City, public governance, digitalization, urban security, digital technologies, data-driven governance, managerial decision-making, security risks, urban environment, national security

Костянтин Споришев, Олександр Бондаренко. «Безпечне місто» як безпекова складова концепції Smart City: публічно-управлінський аспект». *У статті досліджено концепцію «Безпечне місто» у контексті розвитку Smart City та визначено її публічно-управлінський зміст в умовах цифрової трансформації міського середовища. Обґрунтовано, що сучасне розуміння Smart City поступово виходить за межі технологічного підходу та охоплює питання ефективності публічного управління, сталого розвитку, якості міських послуг, використання людського і соціального капіталу та впровадження управління, заснованого на даних. Проаналізовано основні складові Smart City: Smart Governance, Smart Economy, Smart Mobility, Smart Environment, Smart People та Smart Living – та визначено їх безпековий вимір. Встановлено, що безпека має наскрізний характер та охоплює захист інформаційних систем і даних, кібербезпеку, транспортну та громадську безпеку, економічну й інфраструктурну стійкість, попередження екологічних і техногенних загроз, а також формування культури безпеки населення.*

Досліджено становлення та трансформацію концепції Safe City («Безпечне місто»). Встановлено поступовий перехід від використання локальних систем відеоспостереження та фіксації правопорушень до комплексного застосування цифрових технологій, інтелектуальної відеоаналітики, геоінформаційних систем, пристроїв Інтернету речей, великих масивів даних та засобів міжвідомчого інформаційного обміну. Особливу увагу приділено зміні ролі даних у системі забезпечення міської безпеки та їх використанню для моніторингу, виявлення загроз, оцінювання ризиків, прогнозування та підтримки прийняття управлінських рішень.

Визначено публічно-управлінський зміст системи «Безпечне місто» через сукупність моніторингової, інформаційно-аналітичної, координаційної, організаційної, превентивної, контрольної функцій та функції підтримки прийняття управлінських рішень. Доведено, що цифровізація міської безпеки створює передумови для переходу від переважно реактивної моделі реагування на небезпечні події до превентивного та ризик-орієнтованого управління. Наголошено, що ефективність системи «Безпечне місто» повинна визначатися не кількістю технічних засобів спостереження, а здатністю забезпечувати своєчасне виявлення загроз, інформаційну взаємодію, міжвідомчу координацію, обґрунтованість управлінських рішень та оперативність реагування з одночасним дотриманням прав і свобод людини.

Ключові слова: Smart City, Safe City, «Безпечне місто», публічне управління, цифровізація, міська безпека, цифрові технології, data-driven governance, управлінські рішення, безпекові ризики, національна безпека.

148-161
v.38 (2026)
https://smart-scm.org

Introduction. The rapid development of digital technologies, urbanisation processes and the increasing complexity of managing modern territorial communities are driving the transformation of traditional approaches to the organisation of urban space. Digitalisation is gradually encompassing not only the provision of administrative services and communication between public authorities and citizens but also transport, housing and communal services, energy, environmental protection, infrastructure management, public order, civil protection and emergency response. Consequently, cities increasingly function as complex information and communication systems whose management is based on the collection, integration, processing and use of large volumes of data.

The Smart City model has emerged as a conceptual reflection of these transformations. It involves the comprehensive application of digital, information and communication, and analytical technologies to improve the effectiveness of urban governance, the quality of public services, the efficient use of resources and the living conditions of the population. At the same time, the technological development of the urban environment creates new requirements for ensuring its security. The increasing number of digital systems, information flows, critical and municipal infrastructure facilities, transport networks and public spaces highlights the need to move from fragmented responses to individual threats towards integrated urban security management.

In this context, the Safe City concept is becoming particularly important. It is gradually evolving from a local video surveillance and public-order control system into an integrated information and analytical mechanism for ensuring the security of the urban environment. Modern Safe City systems may combine video surveillance networks, intelligent video analytics technologies, geographic information systems, Internet of Things (IoT) sensors and devices, automated traffic-control systems, situation centres, public warning systems, information resources of law enforcement and emergency services, as well as data analysis and risk-forecasting tools.

At the same time, the proliferation of digital security technologies is transforming not only the technological support available to public authorities but also the public governance model itself. Data obtained from different urban subsystems provide an informational basis for situational monitoring, risk identification, coordination among different actors, operational response and management decision-making. Thus, a gradual transition is taking place from a predominantly reactive urban security management model, focused on responding to events that have already occurred, towards a preventive and analytical model aimed at the early identification of potential threats and the mitigation of their consequences.

These processes are particularly relevant to Ukraine, where the digital transformation of territorial communities is taking place alongside the need to ensure the resilience of the urban environment under martial law, heightened security risks, threats to critical infrastructure and the need for the operational coordination of local self-government bodies, law enforcement agencies, emergency services and other actors within the security sector. Under such conditions, Safe City is becoming not merely a local-level technological project but also a component of the public governance system for ensuring the security and resilience of territorial communities.

Nevertheless, the Smart City and Safe City concepts are frequently examined separately in academic and practical discourse. Smart City is predominantly considered through the lens of the digitalisation of urban governance, infrastructure development, electronic services, mobility and sustainable

development, whereas Safe City is often reduced to the use of video surveillance systems, public-order control and law enforcement activities. Such an approach does not fully reflect the contemporary nature of the relationship between a city's digital development and the provision of its security.

In view of the above, it is important to develop a public governance approach according to which Safe City should be regarded as a functional security component of the Smart City concept. This component ensures the integration of digital technologies, data, institutions and management processes to prevent threats, respond to them promptly and ensure the safe and resilient functioning of the urban environment.

Analysis of recent research and publications. The development of the Smart City concept and the integration of security components into contemporary urban governance have been addressed by both international and Ukrainian scholars. A. Caragliu, C. Del Bo, and P. Nijkamp examine Smart City through the interconnection between technological infrastructure, human and social capital, and sustainable urban development. V. Albino, U. Berardi, and R. M. Dangelico systematize the main approaches to defining Smart City, its dimensions, and development criteria. The use of urban data and digital technologies in public governance has been explored by S. Barns, J. R. Gil-Garcia, M. Gasco-Hernandez, T. A. Pardo, J. Kandt, M. Batty, E. Przeybilovicz, M. A. Cunha, and others.

A separate area of research focuses on the relationship between Smart City and Safe City. M. Lacinák and J. Ristvej emphasize the importance of strengthening the safety and security dimension of Smart City and examine the potential of modern technologies for ensuring urban safety. J. Ristvej, M. Lacinák, and R. Ondrejka further develop this approach by considering Smart City and Safe City as interconnected concepts and identifying the areas in which they overlap.

Among Ukrainian scholars, particular aspects of the Safe City system have been studied by I. S. Drok, O. V. Zinchenko, T. I. Kadlubovych, and M. O. Karpenko, with a focus on transport safety, emergency response, protection of state sovereignty, and the implementation of Safe City projects at the national level. At the same time, the public governance dimension of the Safe City system and its role in Smart City development require further research, particularly regarding the use of digital data, interagency cooperation, risk prevention, and support for managerial decision-making.

The formulation of the goals of the article. The purpose of the article is to provide a theoretical substantiation of the place and functional role of the "Safe City" concept within the Smart City framework, define its public administration content, and reveal the mechanisms for integrating digital security technologies into the management system of the modern urban environment.

Presentation of the main results. The formation of the Smart City concept is a natural consequence of the transformation of the modern urban environment under the influence of urbanization, the development of information and communication technologies, the digitalization of public governance, and the growing public demand for improved quality of urban services [16]. The increasing complexity of modern cities, population growth, growing pressure on transport, energy, and utility infrastructure, as well as the need to ensure environmental sustainability and security, have created a need to search for new approaches to organizing urban development governance.

The concept of Smart City became widely used in academic and governance discourse at the beginning of the 21st century. At the same time, its formation was associated with earlier processes of urban informatization and the development of the concepts of the digital city, information city, sustainable city, and e-governance [17].

One of the important approaches to understanding Smart City is presented by A. Caragliu, C. Del Bo, and P. Nijkamp, who associate the development of a smart city not only with the availability of physical and technological infrastructure but also with human and social capital [4]. The researchers emphasize the importance of information and communication technologies for enhancing the efficiency and competitiveness of modern cities. Thus, technology is viewed not as an end in itself in Smart City development, but as one of the instruments for the comprehensive development of the urban environment.

This approach is particularly important for examining Smart City from the perspective of public governance, as it makes it possible to move beyond its narrow interpretation as merely a set of digital technologies. The availability of sensors, video surveillance cameras, digital platforms, automated transport systems, or other technological solutions does not in itself constitute a smart city. What is decisive is how these technologies are integrated into the urban governance system and used to address socially significant issues, improve the efficiency of public authorities, and enhance the quality of life of the population.

V. Albino, U. Berardi, and R. M. Dangelico emphasize the multidimensional nature of the Smart City concept. Based on an analysis of academic literature and documents issued by international institutions, the researchers draw attention to the absence of a single universal definition of Smart City and to the diversity of components used to characterize the "smartness" of a city [1]. Therefore, Smart City should be regarded not as a separate technology or a local digital project, but as a comprehensive direction of urban development encompassing various spheres of city functioning.

In this context, digital technologies primarily perform an instrumental function. Their application enables the collection and processing of data on the condition of urban infrastructure, traffic flows, energy consumption, environmental conditions, the functioning of utility systems, the state of public spaces, and other urban processes. Based on such data, public authorities are able to assess situations more promptly, identify problematic areas, forecast the needs of the territorial community, and make appropriate governance decisions.

Thus, Smart City development is directly associated with the spread of data-driven governance. Under this approach, information obtained from various urban subsystems is transformed into a resource for public governance. First and foremost, the nature of governance activities changes: alongside traditional administrative mechanisms, digital monitoring, analytical data processing, forecasting, automated data exchange, and interagency information interaction are becoming increasingly important.

Importantly, the contemporary understanding of Smart City is gradually moving beyond a purely technological approach. One of the key criteria for smart city development is becoming the ability of digital solutions to deliver tangible improvements in the functioning of urban services and the quality of life of the population. This approach is reflected, in particular, in the international standard ISO 37122:2019 "Sustainable cities and communities – Indicators for smart cities", which associates Smart City development with the improvement of urban services and quality of life and establishes a system of indicators for assessing progress in this area [8].

Currently, academic discourse demonstrates a gradual transition from a technology-oriented understanding of Smart City towards a comprehensive governance approach. While at the initial stages considerable attention was focused on the development of information and communication infrastructure and the implementation of digital technologies, Smart City is increasingly associated with governance efficiency, sustainable

148-161
v.38 (2026)
https://smart-scm.org

development, human and social capital, the quality of public services, and the capacity of public authorities to use data for managerial decision-making [18].

Table 1 – Key Components of Smart City and Their Security Dimension

Smart City Component	Content of the Component	Public Governance Aspect	Security Dimension
Smart Governance	Digitalization of governance processes, e-services, open data, and digital interaction between public authorities and citizens	Improving governance responsiveness; using data for decision-making; interagency information exchange	Protection of information systems and data; cybersecurity; rapid exchange of threat-related information; coordination among security actors
Smart Economy	Innovation, digital economy, entrepreneurship, technological development, and urban competitiveness	Creating an enabling environment for innovation; digitalization of economic processes; support for technological development	Economic resilience of the city; protection of digital economic infrastructure; ensuring the continuity of businesses and essential services
Smart Mobility	Intelligent transport systems, traffic management, and digital mobility services	Monitoring traffic flows; traffic management; optimization of transport infrastructure	Road safety; detection of accidents and hazardous situations; emergency response; monitoring and management of traffic flows
Smart Environment	Environmental monitoring, energy efficiency, resource and waste management	Collection and analysis of environmental data; management of natural and energy resources; planning of environmental policy measures	Early detection of environmental and technological hazards; monitoring of risk indicators; prevention of emergencies
Smart People	Human and social capital, digital competencies, education, and civic participation	Citizen engagement in urban governance; development of digital literacy; e-participation and communication	Development of a safety culture; public information on threats; digital channels for reporting hazardous events; citizen participation in ensuring urban safety
Smart Living	Quality of life, healthcare, culture, housing, education, social infrastructure, and safety	Ensuring the accessibility and quality of urban services; creating a comfortable and resilient urban environment	Public and personal safety; protection of public spaces; video surveillance; emergency response; civil protection; crime prevention

Source: systematized by the author based on: [1, 6].

The analysis of the Smart City components (Table 1) demonstrates that security is not limited exclusively to the Smart Living component, within which it has traditionally been associated with the quality of life of the population. In fact, the security dimension is cross-cutting and is manifested across all components of a smart city: from cybersecurity and the protection of governance data within Smart Governance, to transport safety within Smart Mobility, economic resilience within Smart Economy, the prevention of environmental and technological threats within Smart Environment, and the development of a safety culture within Smart People. Thus, the role of security within the Smart City structure is gradually expanding, creating grounds for a separate examination of Safe City as a

security-oriented dimension of the digital development of the modern city.

For the purposes of this study, the Smart Living component is of particular importance, since the quality of urban life directly depends not only on the accessibility of services, housing conditions, mobility, or the state of the environment, but also on the level of personal and public safety. At the same time, the security component is not confined to a single area of Smart City. Transport system safety is associated with Smart Mobility, the protection of digital infrastructure with Smart Governance, the resilience of energy and utility systems with Smart Environment, while the ability of public authorities to identify threats in a timely manner and coordinate response measures directly depends on the quality of digital governance.

Therefore, security should be regarded as one of the cross-cutting prerequisites for the effective functioning of Smart City. The higher the level of digital integration of the urban environment, the greater the importance of timely threat detection, protection of the population and infrastructure, coordination of relevant services, emergency response, and the use of information to prevent potential risks.

In this context, within the broader development of Smart City, a distinct security-oriented direction is gradually emerging, associated with the use of digital technologies for monitoring urban spaces, preventing offences and emergencies, protecting infrastructure, and providing information and analytical support for the activities of public authorities. Its development creates the prerequisites for the formation and expansion of the Safe City concept.

Ensuring the safety of the population is one of the fundamental prerequisites for the sustainable functioning and development of the modern city. Urban population growth, the increasing complexity of transport and utility infrastructure, the concentration of numerous economic and social facilities, the growing intensity of information flows, and the emergence of new technological risks significantly broaden the range of threats faced by the urban environment. Under these conditions, security is gradually ceasing to be regarded exclusively as the responsibility of law enforcement agencies and is acquiring a comprehensive character, encompassing public, transport, technological, information, cyber, infrastructure, and other interconnected dimensions of security.

These processes have directly influenced the development of the Smart City concept. The digitalization of the urban environment has created new opportunities not only for optimizing traffic flows, managing energy resources, or providing public services, but also for monitoring the state of urban spaces, detecting hazardous situations, preventing offences, coordinating the activities of relevant services, and ensuring rapid response to threats. As a result, security issues have gradually become one of the important areas of smart city development.

The relationship between the technological development of Smart City and the provision of urban security is reflected in the works of international researchers. In particular, K. T. Chui, P. Vasant, and R. W. Liu, examining urban monitoring and surveillance systems, draw attention to the potential of information and communication infrastructure, sensor devices, cameras, and big data analytics technologies for protecting people and property. At the same time, the use of such technologies is accompanied by a number of challenges related to data quality, privacy, information security, and relevant public policy [5]. Thus, the digitalization of urban security creates not only new governance instruments but also new objects and risks of public regulation.

The gradual emergence of a distinct security-oriented dimension of urban digital development contributed to the spread of the Safe City concept. At the initial stages, its practical implementation was largely associated with maintaining public order,

preventing crime, and using video surveillance systems. Surveillance cameras made it possible to continuously monitor specific areas of urban space, record events, and use the information obtained in law enforcement activities. However, the development of information and communication technologies has gradually expanded the capabilities of such systems.

An important direction of this transformation has been the use of data not only to record offences that have already occurred but also to prevent them. Research in the field of urban security demonstrates the potential for combining crime-related information with data on the characteristics of the urban environment, land use, population movements, and other factors. On this basis, digital systems can be used as decision-support tools in the formulation and implementation of urban security policies.

In the academic literature, Safe City is considered one of the directions for developing a secure urban environment through the application of modern technologies. In particular, a systematic review devoted to the development of a conceptual Safe City model associates a safe city with the use of technologies by public authorities, communities, and other stakeholders to reduce crime risks and create an environment in which the population can feel safe. At the same time, security is identified as one of the essential aspects of Smart City development.

At the same time, the relationship between the concepts of Smart City and Safe City is not interpreted uniformly in contemporary academic literature. Some approaches consider Safe City as a separate functional component of Smart City, primarily focused on ensuring public safety. Other studies emphasize the much broader scope of urban security, which does not allow Safe City to be fully subordinated to the Smart City concept.

The position of J. Ristvej, M. Lacinák, and R. Ondrejka is particularly illustrative in this context. The researchers note that at the early stages of their research they considered Safe City as one of the systems within Smart City; however, they subsequently concluded that such an approach did not cover the entire spectrum of urban security issues [14]. As a result, they proposed considering Smart City and Safe City as independent but partially interconnected concepts. This position demonstrates the complexity of establishing a clear hierarchy between a "smart" and a "safe" city and indicates the gradual expansion of the scope of the Safe City concept.

From a public governance perspective, this transformation in the functional content of Safe City is of particular importance. While traditional urban security systems were primarily focused on surveillance, event recording, and subsequent response by relevant services, modern digital technologies make it possible to establish a significantly more complex system of information support for governance. Video surveillance is complemented by intelligent video analytics, geographic information systems, sensors and Internet of Things devices, automated recognition of specific objects and events, big data analytics, digital public warning systems, and interagency information exchange tools.

Accordingly, the role of data in the urban security system is also changing. Data can be used not only as a source of information about events that have already occurred, but also to identify high-risk areas, detect patterns, forecast possible developments, and select the most appropriate governance measures. This creates the prerequisites for a transition from a predominantly reactive approach to urban security towards more preventive and risk-oriented governance.

Along with the technological expansion of Safe City, the range of actors involved in ensuring urban security is also broadening. While law enforcement agencies and emergency services traditionally played the primary role in this field, the functioning of a

modern digitalized city requires interaction among local self-government bodies, state authorities, police, rescue and medical services, urban infrastructure operators, transport enterprises, municipal services, and other actors. Consequently, the issue of urban security is acquiring a distinct interagency and cross-sectoral character.

At the same time, the technological advancement of security should not be equated with the unlimited expansion of surveillance systems. Contemporary research increasingly focuses on risks related to privacy, personal data protection, cybersecurity, algorithmic data analysis, and the possibility of excessive surveillance of urban spaces. Therefore, the effectiveness of Safe City is determined not only by the number of installed cameras, sensors, or other digital tools, but also by the existence of appropriate organizational, legal, and governance mechanisms regulating their use.

Thus, the development of Safe City is characterized by a gradual transition from local surveillance and monitoring technologies to the comprehensive use of digital data in urban security processes. This transformation simultaneously broadens the scope of public governance: alongside maintaining public order, it increasingly encompasses risk prevention, infrastructure protection, information exchange, coordination among relevant services, data protection, and ensuring the resilient functioning of the urban environment.

In this regard, the study of Safe City in the context of Smart City requires a shift from a purely technological interpretation towards an analysis of its governance dimension. Of particular importance is the question of how information obtained through the city's digital infrastructure is integrated into the activities of public authorities, transformed into governance decisions, and used to prevent and minimize security risks.

The development of Safe City systems highlights the need to consider them not merely as a set of technical tools for surveillance, event recording, and data analysis, but as an element of the contemporary system of public governance of urban security. Technological infrastructure alone does not ensure the security of the urban environment [2]. Its practical value is determined by the capacity of public authorities to use the data obtained to identify problems, assess risks, coordinate the activities of relevant services, make governance decisions, and organize timely responses.

This approach corresponds with contemporary research on smart urban governance. E. Przeybilovicz and M. A. Cunha consider the digital transformation of the urban environment as a factor contributing to the emergence of new dynamic models of urban governance, within which the nature of interaction among public authorities, information and communication technologies, and citizens directly influences the mechanisms through which governance functions are performed [12]. In turn, S. Ranchordás and A. Klop associate the development of data-driven governance in Smart City with the use of big data, artificial intelligence, the Internet of Things, and predictive analytics to improve the efficiency of public services and managerial decision-making. The combination of these components makes it possible to understand Safe City more broadly than traditional video surveillance systems or automated monitoring of individual areas of urban space [13].

In the traditional model of urban security, information about an offence, accident, emergency, or other hazardous event is generally received by the relevant authority or service only after the event has occurred. Subsequent governance actions are aimed at containing the event, mitigating its consequences, establishing the circumstances, and restoring the normal functioning of the affected area or facility. Such an approach is predominantly reactive,

as the governance system responds to a threat that has already materialized.

The digitalization of the urban environment creates the prerequisites for a gradual transformation of this model. The continuous flow of information from various sources enables public authorities and relevant services to obtain data on the condition of individual facilities and processes in near real time. As a result, information can be used not only to record an event but also to detect deviations, identify potentially hazardous situations, assess risks, and take appropriate measures in advance.

In this context, one of the key elements of the public governance dimension of Safe City is the information and analytical function. Large volumes of information obtained from various sources acquire governance value only when they are systematized, compared, and analyzed [3]. Therefore, what becomes fundamentally important is not the accumulation of data itself, but its transformation into information suitable for use in managerial decision-making.

At the same time, the effective use of data requires their integration. Information on the condition of public spaces, transport infrastructure, road traffic, municipal facilities, or emergencies may be generated by different authorities, services, and information systems. The isolated use of such information limits the possibilities for a comprehensive assessment of the situation. In contrast, effective information exchange makes it possible to develop a more comprehensive understanding of the state of the urban environment and the nature of existing risks.

This leads to another important function of the Safe City system – the coordination function. Ensuring the security of a modern city extends beyond the competence of any single public authority. Responding to different types of threats may simultaneously require the involvement of local self-government bodies, law enforcement agencies, civil protection authorities and units, emergency medical services, municipal enterprises, transport services, and other actors [7]. Under such conditions, governance effectiveness depends not only on the powers of each actor but also on the speed of information exchange and the coordination of joint actions.

The monitoring function also plays an important role in the operation of Safe City and involves systematic observation of the urban environment and individual processes relevant to security. Unlike the episodic receipt of information, digital monitoring makes it possible to generate continuous information flows, track changes in relevant indicators, and promptly identify developments requiring governance intervention.

The preventive function is directly related to the monitoring and information and analytical functions. The use of accumulated data and the results of their analysis creates opportunities to identify recurring patterns, determine high-risk areas or facilities, and plan measures aimed at preventing or reducing the likelihood of adverse events. Thus, governance activities gradually shift from responding to consequences towards preventing threats.

The managerial decision-support function is of particular importance. Given the large number of simultaneous information flows, an official or public authority may not always be able to process the entire volume of available information promptly. Digital analytical tools make it possible to structure data, identify priority events, reveal interrelationships, and provide an information basis for selecting appropriate governance decisions [9]. At the same time, technology should not replace the competent public authority: it performs a supporting role, while responsibility for decision-making remains with the relevant authority or official.

Today, digital technologies are changing the nature of information support for public governance. In the traditional governance

model, information was largely received through citizens' appeals, reports from relevant services, statistical reporting, and other documented sources. In the digitalized urban environment, these sources are supplemented by automated data flows that can be generated continuously and characterize the current state of particular processes. As a result, the time between the emergence of a hazardous situation, its detection, and the initiation of a governance response is reduced.

The public governance dimension of the Safe City system is also manifested through its organizational function. The integration of digital technologies into security processes requires the identification of responsible actors, the delineation of their competencies, the establishment of procedures for access to information resources, information exchange, and response algorithms. Therefore, the technological integration of information resources should be accompanied by the corresponding organizational integration of the activities of public governance actors.

Equally important is the control function, which is associated with the possibility of evaluating the outcomes of governance decisions and measures implemented. The accumulation of data makes it possible to compare the state of the urban environment before and after the implementation of relevant decisions, assess the response time of services, identify recurring problems, and adjust governance measures accordingly [11]. This creates a feedback mechanism linking information collection, decision-making, implementation, and evaluation of results.

At the same time, the digitalization of urban security governance gives rise to a number of new governance and legal challenges. The concentration of large volumes of information, including data on individuals' movements and behavior, creates risks of unlawful interference with privacy, unauthorized access to information, data leakage, or the use of data for purposes other than those for which they were originally collected [15]. The use of algorithmic analytical systems further raises issues concerning the transparency of technological solutions, non-discrimination, the limits of automated data processing, and accountability for decisions made with the use of such technologies.

Therefore, the public governance effectiveness of Safe City cannot be assessed solely by the number of installed cameras and sensors, established situation centers, or the volume of accumulated data. It should be determined by the system's capacity to ensure timely threat detection, effective information exchange, coordination among relevant actors, well-grounded governance decisions, rapid response, and respect for human rights and freedoms [10].

Thus, from a public governance perspective, the Safe City system is characterized by a combination of monitoring, information and analytical, coordination, organizational, preventive, and control functions, as well as the managerial decision-support function. Their implementation enables the transformation of digital data on the state of the urban environment into a public governance resource and creates the prerequisites for improving the responsiveness and soundness of public authorities' activities in the field of urban security.

Accordingly, the fundamental difference between the contemporary Safe City system and traditional technical surveillance systems lies not so much in the number or technological complexity of the tools employed, but rather in the integration of the data obtained through these tools into the full public governance cycle – from problem identification and risk assessment to decision-making, organization of response measures, and evaluation of their effectiveness. It is this aspect that makes it possible to consider the development of Safe City systems as part of the broader processes of the digital transformation of public governance of the urban environment.

148-161
v.38 (2026)
https://smart-scm.org

Conclusions.

In the context of the digital transformation of the urban environment, security is becoming one of the key dimensions of Smart City development. At the same time, its role cannot be limited exclusively to the Smart Living domain, since security-related objectives are, to varying degrees, integrated into all major components of a smart city. The protection of information resources, transport safety, urban infrastructure resilience, prevention of technological and environmental threats, maintenance of public order, and development of a public safety culture constitute an interconnected set of tasks that requires the coordinated use of digital and governance instruments.

The development of the Safe City concept demonstrates a gradual transformation of the approach to ensuring urban security. A Safe City can no longer be identified solely with video surveillance systems, technical recording of events, or monitoring of public spaces. Its contemporary content is primarily determined by the capacity to integrate various sources of information and use the data obtained for timely threat detection, risk assessment, forecasting of possible developments, and the organization of coordinated response measures. Accordingly, the technological development of Safe City is gradually evolving into a broader transformation of urban security governance.

A key outcome of this transformation is the changing role of information in the governance process. Data no longer serve exclusively as a means of recording events but are increasingly becoming a resource for public governance. Their systematic collection, integration, and analytical processing make it possible to reduce the time between the emergence of a threat, its detection, and the initiation of a governance response. This creates the conditions for a gradual transition from a predominantly reactive security model to preventive and risk-oriented governance of the urban environment.

The governance effectiveness of the Safe City system therefore depends not on the number of cameras, sensors, information platforms, or other technical tools, but on the extent to which they are integrated into the activities of public authorities and relevant services. Of decisive importance is the system's capacity to ensure continuous monitoring, analytical processing of information, effective interagency data exchange, coordination among relevant actors, support for managerial decision-making, and control over the results of implemented decisions. Therefore, technological integration should be accompanied by organizational and governance integration.

At the same time, the expansion of the technological capabilities of Safe City creates a new set of risks for public governance. The accumulation of large volumes of data, the increasing use of intelligent video analytics, and algorithmic data processing raise important issues related to personal data protection, privacy, cybersecurity, transparency in the use of digital technologies, and accountability for decisions made with their assistance. Therefore, the further development of Safe City should be based on a combination of technological efficiency, appropriate legal and organizational frameworks, and respect for human rights and freedoms.

Thus, the prospective development of Safe City systems should focus not on simply expanding digital infrastructure, but on establishing an integrated mechanism for urban security governance in which technologies provide the information basis for monitoring, threat prevention, coordination, and decision-making. It is precisely the capacity to transform digital data into timely and well-grounded governance actions that will determine the actual effectiveness of Safe City as a security-

oriented dimension of contemporary Smart City development.

References

1. Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. Journal of Urban Technology, 22(1), 3–21. DOI: 10.1080/10630732.2014.942092.

2. Barns, S. (2018). Smart cities and urban data platforms: Designing interfaces for smart governance. City, Culture and Society, 12, 5–12. DOI: 10.1016/j.ccs.2017.09.006.

3. Bui, M. (2025). Toward a community-driven approach to urban data-driven governance. International Communication Gazette, 87(1). DOI: 10.1177/17480485241261572.

4. Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. Journal of Urban Technology, 18(2), 65–82. DOI: 10.1080/10630732.2011.601117.

5. Chui, K. T., Vasant, P., & Liu, R. W. (2019). Smart city is a safe city: Information and communication technology-enhanced urban space monitoring and surveillance systems: The promise and limitations. In Smart Cities: Issues and Challenges (pp. 111–124). Elsevier.

6. Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N., & Meijers, E. (2007). Smart Cities: Ranking of European Medium-Sized Cities. Vienna: Centre of Regional Science, Vienna University of Technology.

7. Gil-Garcia, J. R., Gasco-Hernandez, M., & Pardo, T. A. (2022). Governance rules for managing smart city information. Urban Governance, 2(1), 221–231. DOI: 10.1016/j.ugj.2022.05.003.

8. International Organization for Standardization. (2019). ISO 37122:2019. Sustainable cities and communities Indicators for smart cities. Geneva: ISO. 95 p. https://www.iso.org/standard/69050.html.

9. Kandt, J., & Batty, M. (2021). Smart cities, big data and urban policy: Towards urban analytics for the long run. Cities, 109, Article 102992. DOI: 10.1016/j.cities.2020.102992.

10. Lacinák, M., & Ristvej, J. (2017). Smart city, safety and security. Procedia Engineering, 192, 522–527. DOI: 10.1016/j.proeng.2017.06.090.

11. OECD. (2023). Smart City Data Governance: Challenges and the Way Forward. OECD Urban Studies. Paris: OECD Publishing. 185 p. DOI: 10.1787/e57ce301-en. https://doi.org/10.1787/e57ce301-en.

12. Przeybilovicz, E., & Cunha, M. A. (2024). Governing in the digital age: The emergence of dynamic smart urban governance modes. Government Information Quarterly, 41(1), Article 101907. DOI: 10.1016/j.giq.2023.101907.

13. Ranchordás, S., & Klop, A. (2024). Data-driven regulation and governance in smart cities. In V. Mak et al. (Eds.), Research Handbook in Data Science and Law (2nd ed., pp. 251–276). Edward Elgar Publishing. DOI: 10.4337/9781035316458.00019.

14. Ristvej, J., Lacinák, M., & Ondrejka, R. (2020). On smart city and safe city concepts. Mobile Networks and Applications, 25, 836–845. DOI: 10.1007/s11036-020-01524-4.

15. Drok, I. S. (2025). The "Safe City" system as a tool for monitoring compliance with transport legislation. Analytical and Comparative Jurisprudence, 2, 244–249. [in Ukrainian].

16. Zinchenko, O. V. (2024). "Safe City" as a factor of rapid response to emergencies in the context of the development of a digital society. Collection of Scientific Works of the State Research Institute of the Ministry of Internal Affairs of Ukraine, 4(12). [in Ukrainian].

17. Kadlubovych, T. I. (2026). The "Safe City" concept as a tool for protecting state sovereignty. Forum Prava, 87(3), 190–198. DOI: 10.32631/fp.2026.3.18. [in Ukrainian].

18. Karpenko, M. O. (2023). Substantiation of the implementation of "Safe City" projects at the state level in Ukraine. Investments: Practice and Experience, 11, 45–51. [in Ukrainian].