https://doi.org/10.31891/2307-5732-2026-363-53
УДК 004.9

KAPITON ALLA
National University «Yuri Kondratyuk Poltava Polytechnic
https://orcid.org/0000-0002-7845-0883
E-mail: kits_seminar@ukr.net
FRANCHUK TAMARA
State University of Trade and Economics
https://orcid.org/0000-0001-7615-1276
E-mail: Tamara_Franchuk@ukr.net
TYSHCHENKO DMYTRO
State University of Trade and Economics
https://orcid.org/0000-0002-2193-9012
E-mail: tyshchenko_d@knute.edu.ua
DESIATKO ALONA
State University of Trade and Economics
https://orcid.org/0000-0002-2284-3418
E-mail: desyatko@knute.edu.ua

INTEGRATION OF CYBER PROTECTION IN THE INFRASTRUCTURE OF INNOVATION PARKS: CONCEPTUAL AND METHODOLOGICAL PRINCIPLES OF FORMING A SECURE DIGITAL ENVIRONMENT

The article considers modern directions for solving the problem of integrating cyber defense into the infrastructure of innovation parks, as well as the conceptual and methodological principles of forming a secure digital environment. This study is devoted to the analysis of issues regarding the feasibility of creating innovation parks, the very need for which arose during the development of innovative technologies, which are gaining momentum at an ever-increasing speed, using the capabilities of distributed systems. The disadvantages of virtual collaboration are analyzed, where the main point is the lack of an environment where all tasks are solved and problems are solved, as a result of which the environment encourages the search for effective solutions, where attention is paid specifically to the protection of data processing processes. The main task is the undisputed and flawless implementation of projects with a given positive result, which is the result of a correctly constructed strategy. The main concepts of this issue are studied, which are considered in the context of their interconnection and considered through the prism of a creative approach to the life of the entire ecosystem of innovative practices, its design, creation and functioning. The issue of a comprehensive approach and organization of a system of paths in the process of supporting new ideas for the development of an innovation ecosystem in Ukraine, the constant creation, implementation, promotion and regulation of new markets was studied. It has been proven that encouraging promising investors to create new products in their country is one of the levers that encourage the development of individual representatives, enterprises, and the economy of the entire country. The features of the variety of all methods of data protection from potential threats to the development of innovative packages are determined, in particular, ensuring the operation of the network due to distributed data processing and the functioning of remote resources and servers, the use of the Internet, thanks to the correct organization of work, a procedure is defined, which includes a system of actions using cyber protection of corporate confidential information, which prevents leakage, deletion and modification of data and must be inaccessible to third parties. Methods for using distributed systems and data storage, and a special data protection system in a cloud environment, are proposed. Methods of preventing and countering possible threats have been identified due to the specifics of organizing cyber protection for the entire ecosystem of innovation parks, where attention is paid to both personal data and documents, as well as the processes of their processing and transmission. Ways have been established to update special software, including antivirus programs, the use of SSL certificates, and anti-detection browsers, which are quite relevant today.

***Key words**: cyber protection, cyber defense, digital infrastructure, digital security, cyber defense models, data protection, innovation ecosystem*

КАПІТОН АЛЛА
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»
ФРАНЧУК ТАМАРА, ТИЩЕНКО ДМИТРО, ДЕСЯТКО АЛЬОНА
Державний торговельно-економічний університет

ІНТЕГРАЦІЯ КІБЕРЗАХИСТУ В ІНФРАСТРУКТУРУ ІННОВАЦІЙНИХ ПАРКІВ: КОНЦЕПТУАЛЬНО-МЕТОДИЧНІ ЗАСАДИ ФОРМУВАННЯ БЕЗПЕЧНОГО ЦИФРОВОГО СЕРЕДОВИЩА

У статті розглянуто сучасні напрями вирішення проблеми інтеграції кіберзахисту в інфраструктуру інноваційних парків, визначено концептуально-методичні засади формування безпечного цифрового середовища. Дане дослідження присвячене аналізу питань щодо доцільності створення інноваційних парків, сама потреба яких виникла в час розвитку іноваційних технологій, які набирають обертів із швидкістю, що постійно зростає, використовуючі можливості розподілених систем. Проаналізовані недоліки віртуальної співпраці, де основним параграфом є брак середовища саме того, де вирішуються усі завдання та розвязуються задачі, в наслідок чого середовище спонукає на пошук ефективних рішень, де увага приділена саме захисту процесів обробки даних. Основним із завдань є безперечна та безвідмовна реалізація проектів із заданим позитивним результатом, що є наслідком вірно побудованої стратегії. Досліджені основні поняття цієї проблематики, які розглянуті у контексті їх взаємозвязку та розглянуті через пизму креативного підходу життєдіяльності всієї екосистеми іноваційних праків, її проектування, створення та функціонування. Вивчено питання комплексного підходу та організації системи шляхів в процесі підтримки нових ідей для розвитку інноваційної екосистеми в Україні, постійного створення, впровадження, заохочення та регулювання нових ринків. Доведено, що заохочення перспективних інвесторів надає можливості

створювати нові продукти в своїй країні є одним з важелів, що спонукають до розвитку окремих представників, підприємств та економіки всієї країни. Визначені особливості розмаїття всіх способів захисту даних від потенційних загроз розвитку інноваційних паків, зокрема забезпечення роботи мережі, внаслідок розподіленої обробки даних та функціонування віддалених ресурсів та серверів, використання інтернету, завдяки правильній організації роботи, визначена процедура, що включає систему дій з використанням кіберзахисту корпоративної конфіденційної інформації, що унеможливлює виток, видалення та модифікацію даних та повинна бути недоступною для сторонніх осіб. Запропоновано методи використання розподілених систем та сховищ даних, та особлива система захисту даних у хмарному середовищі. Визначено методи попередження та протидії можливим загрозам завдякі специфіці організації кіберзахисту всієї екосистемі іноваційних парків, де увага приділена як особистими даними та документам, так і процесам їх обробки та передачі. Встановлено шляхи оновлення спеціального програмного забезпечення, зокрема програм антивірусів, застосування SSL-сертифікатів, антидетект-браузерів, що є сьогодні досить актуальними.

Ключові слова: *кіберзахист, цифрова інфраструктура, цифрова безпека, моделі кіберзахисту, захист даних, інноваційна екосистема*

Стаття надійшла до редакції / Received 12.01.2026
Прийнята до друку / Accepted 28.02.2026
Опубліковано / Published 26.03.2026

Introduction

There is no denying the urgency of creating innovation parks, the very need of which arose several dozen years ago. Today, the field of innovative technologies is gaining momentum at an ever-increasing speed, but many professionals today are forced to work remotely, using the capabilities of distributed systems. Hoping to overcome the shortcomings of virtual collaboration, where the main paragraph is the lack of an environment where all tasks are solved and problems are solved, as a result of which the environment encourages the search for effective solutions in an atmosphere where attention is paid to the protection of data processing processes. The main task is the undisputed and error-free implementation of projects with a given positive result, which is a consequence of a correctly constructed strategy. That is why we consider the main concepts of this issue in the context of their interrelationship, considering through the lens of a creative approach the vital activity of the entire system, its design, creation and functioning. Understanding the importance of such a component as information security, it should be noted that the peculiarity of the diversity of all methods of protecting data from potential threats is becoming of paramount importance today. It is not only about ensuring the operation of the network, due to distributed data processing and the functioning of remote resources and servers, the use of the Internet, thanks to the correct organization of work, the set of actions using corporate confidential information should be inaccessible to third parties. The use of distributed systems and data storage, and a special data protection system in a cloud environment requires constant updating. Prevention and counteraction to possible threats is possible thanks to the specifics of organizing cyber protection for the entire ecosystem of innovation parks, where attention is paid to both personal data and documents, as well as the processes of their processing and transmission. Updating special software, in particular antivirus programs, using SSL certificates, and anti-detection browsers are quite relevant today.

Analysis of recent research and publications

Research into current issues of optimal and effective functioning of innovation parks today requires consideration of a number of components that ensure their emergence, creation, functioning, and development. In the context of analyzing the technical component of ensuring the vital activity of the ecosystem of innovation parks, the researchers' attention was drawn to the problems of ensuring data protection and cyber security in the sphere of functioning of their digital infrastructure. A number of scientists have drawn attention to the requirements for creating a secure digital environment and digital transformation of innovation parks that will ensure the security of the innovation ecosystem. Melnyk V. It is not for nothing that he believes that innovation parks are the format of the future [1]. Tyshchenko D., Zakharov R., Moskalenko V., Desiatko A., Franchuk T., Stepashkina K., Karpunin, I. Velichko H. study the problematic issues of the effective functioning of innovation parks, consider a number of components that ensure their emergence, creation, functioning and development [2-6]. Geraskova O., Stechenko D. analyze economic efficiency of functioning of infrastructure for innovative activity in Ukraine [7]. Tarasovsky Yu. investigates problems of Ukraine's approved the Strategy for the Digital Development of Innovations until 2030 [8]. Hrynko T. considers the formation of Ukraine's innovation infrastructure as the basis for innovative activation of enterprises' activities [9]. Mazur O. investigates the state and problems of Ukrainian technoparks [10]. Nosovets O., Voloshchuk L. analyze the place of innovation infrastructure in determining the results of innovation activity [11]. Shestak Ya., Zavgorodnya Ye., Krasnoshchok V. analyze the features of technical protection of the information infrastructure of commercial enterprises [12]. Many sources indicate the interest of scholars in studying Innovations for Infrastructure Development and Sustainable Industrialization in the context of digital security transformation [13-16].

Main part

Understanding that, in essence, innovation parks represent a location for the functioning of an effective community, for the development of interesting new, innovative, well-founded solutions and a system of ideas for the improvement and development of entrepreneurship, it should be noted, that it is necessary to ensure safety in order to create a comfortable environment for the activities of specialists, directing their potential to creativity, introducing the focus of their activities from the technical component to creative ideas, startup projects and other innovations. Having ensured all the requirements for uninterrupted operation of the digital infrastructure, attention should be paid to the problem of risk management arising from non-compliance with the requirements for ensuring digital security. It is the analysis of the most effective cyber protection models that require information stability and ensure all processes related

to the protection of data directly, creating a secure digital environment, allows us to talk about the effective results of the implementation of financial and organizational mechanisms, which led to the modern processes of digital transformation, based on the active implementation of regulatory policies in various industries[1-12].

Today, there is no objection to the fact that ensuring a qualitative increase in the level of socio-economic levers of any developed state is possible under the condition of comprehensive well-founded cooperation of the system of components, which can include legal, organizational, economic, social, and others. The need for constant efficient functioning of the ecosystem and the constant development and increase of today's requirements for continuous economic growth, which is daily complicated in modern political circumstances, is indisputable. There is a constant need to create a healthy balanced modification of the economy of our and other countries from the orientation of the development of raw material industries to industries that require the development of intellectual potential with a change of focus on the development of the latest ideas and innovative activities. Despite the levers and important place of all industries in the effective growth of the country's economic indicators, it is precisely the problem in the field of intellectual potential development, implementation of ideas, innovations based on the results of scientific and technical progress, today, especially in a difficult period for our country, should be aimed at helping progressive innovative, technical, technological changes in the life of enterprises, helping to increase the competitiveness of production results, products, services, improving the service sector, provision of services and consumption of production activity results. In addition, we are talking about the possibility and preliminary procedures of increasing the efficiency of the use of natural resources, the environmental security of the state, namely the state of the energy supply of a certain country, the system for ensuring the effective operation of all mechanisms, working for national defense, ensuring the proper quality level of life of the population. Studying a number of aspects of selected scientific issues, it is quite difficult to single out the primary problems that require immediate solution, based on the features of all possible current dangers. But the statement that the analysis of innovative and digital infrastructure is of a theoretical and applied nature, namely the problem of risk management and digital security, information sustainability, data protection, namely effective activity in a secure digital environment.

Particular attention should be paid to the difficulties of work in the modern conditions of the Ukrainian market, the legislation of our state, which is constantly changing. Relying on an understanding of the needs of the citizens of the state, namely residents, it is possible to predict the wishes and expectations of other participants in the functioning of all processes that ensure the support and development of innovations. Demarcation and identification of the characteristic features of innovation parks for our country in the conditions of today's influences, both from the political and economic side, require special attention, high-tech digital with all the positive manifestations of digitization processes. You can pay attention to a sufficient number of potential investors with small capital and the desire to become a co-author, partner and co-founder of an innovative company that does not require large capital investments at the beginning and provides a start to innovations.

According to the Strategy for the Digital Development of Innovations of Ukraine (WINWIN) until 2030 approved by the Government, it can be stated that state support for innovations at the state level is planned, which will undoubtedly concern all its components, in particular, special attention will be paid to supporting its leading directions, which are directly defined in this strategy[15]. The most important of which are presented in Figure 1.

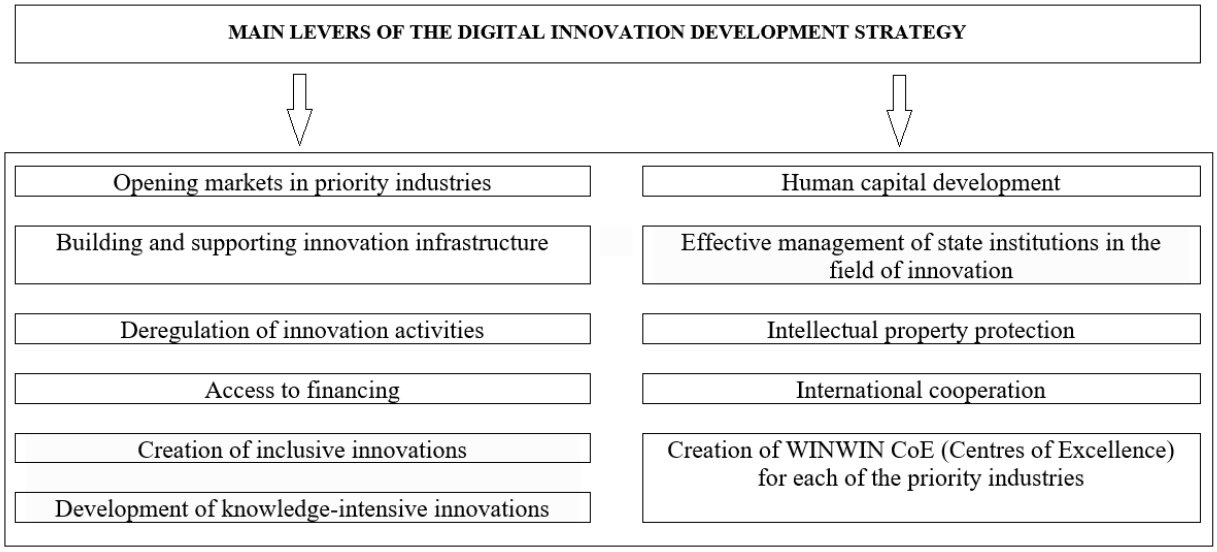

Fig. 1. Main levers of the digital innovation development Strategy

Through the prism of development, the innovation park can be considered as a set of high-quality architectural objects and landscape solutions, which are specially oriented to ensure the creation, effective development and functioning of a favorable microclimate for the implementation of innovations. The main issue is a comprehensive understanding and organization of the system of paths in the process of supporting new ideas for the development of the innovation ecosystem in Ukraine, the constant creation, implementation, promotion and regulation of new markets.

Encouraging young, promising professionals to create new products in their country is one of the levers that encourage the development of individual representatives, enterprises, and the economy of the entire country. The key industries that are the basis of the development of innovations according to the Strategy for the Digital Development of Innovations of Ukraine (WINWIN) are presented in the figure 2[15].

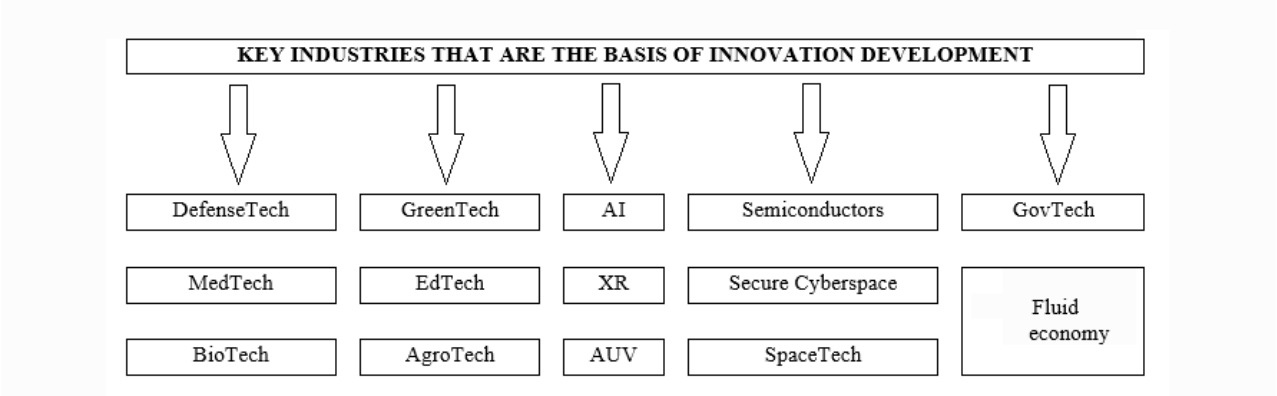

Fig. 2. Key industries that are the basis of innovation development according to the Strategy for the Digital Development of Innovations of Ukraine (WINWIN)

The main concept of innovation parks is to create a positive environment with certain conditions for high-tech ideas, projects, startups that have the potential to develop and turn into a profitable company. The very design, creation and study of the features of the functioning of the park as an ecosystem, which aims to combine all the necessary elements in one place, is the focus of our research and deserves an in-depth analysis. The main goal in the process of its development is to create an environment for the operation of high-tech business, with greater added value than traditional business. A lot of attention should be paid to the part that is responsible for its creative component, which can be conventionally called a creative cluster, which in most cases includes information, communication, telecommunication technologies, robotics and other modern technologies that have become the consequences of modern digitalization of processes. It can be considered that the concept should be flexible, that is, change and adapt to market changes, relying on changes in functioning processes. Changing external circumstances cannot help but affect the progress we strive for, but economic, political and social processes cannot stand aside and affect the development vector of innovation parks, which makes constant adjustments to the system that must function successfully, paying attention to the continuous operation of all its elements, which are constant but mutating components of the ecosystem of the park, which have the ability to change their size and fate component, adjusting the percentage of each.

Conclusions

To ensure the development of innovation parks and industries, it is necessary to ensure many components and improve quality, in essence, the transformation of existing visions of the development of innovation projects, which is becoming one of the priorities of state policy. Also a necessary condition is the creation of favorable legislation, special incentive levers, tax optimization, reduction of financial pressure, and partial or full financial support. The technical components for ensuring cyber protection in the operation of distributed systems, which are most often used effectively, also require updates and modifications. The issue of data protection, namely ensuring the security of information and production networks, consists in the constant protection of network perimeters, both their external and internal components. Modern methods of protecting specialized services are also quite relevant during the development of distributed systems that successfully operate in innovation parks. Further research in the field of protection and cyber security of technical components of innovation parks is warranted in view of the increased additional threats in the current situation.

Additional attention should be paid to problems arising from force majeure events and projects should be developed with their subsequent implementation and modification regarding threat prevention and proactive protection against them, paying attention to additional protection of users and their workplaces. An additional condition for supporting and operating innovation parks in the context of digitalization is the creation of secure communication channels and the development of a data leak prevention system. Based on the development of problems that constantly need to be solved as a result of cyberthreats, the focus of scientists should be on research on the study of cyber hygiene issues through the prism of active manifestations and implementations of cyberattacks.

References

1. Melnyk V. Innovative parks are the format of the future URL: https://interfax.com.ua/news/interview/960132.html (дата звернення: 20.01.2026).

2. Tyshchenko D., Franchuk T., Stepashkina K., Karpunin, I. System design and development corporate electronic document management *European Scientific Journal of Economic and Financial Innovations.* 2024. № *1*(13). pp. 200-207.

3. Franchuk T., Tyshchenko D., Desiatko A., Karpunin I. Features of accounting digitalization processes. *Galician economic journal,* 2025, vol. 95, no 1, pp. 61-66.

4. Tyshchenko D., Franchuk T., Zakharov R., Moskalenko V. Supporting dynamic security needswith VPN tools. *Control, Navigation and Communication Systems*. 2024. No. 3, 2024. 3 (77). pp. 149-152.

5. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A., R. Zakharov Requirements for modern processors for secure operation of information systems and networks *Control, Navigation and Communication Systems*. 2025. No. 3, 2025. 3 (77). pp. 111-117.

6. Velichko H. Elements and components of innovative infrastructure URL: http://www.spilnota.net.ua/ua/article/id-2296/ (дата звернення: 20.01.2026).

7. Geraskova O., Stechenko D. Economic efficiency of functioning of infrastructure for innovative activity in Ukraine URL: http://www.economy.nayka.com.ua/?op=1&z=3002 (дата звернення: 20.01.2026).

8. Tarasovsky Yu. Ukraine has approved the Strategy for the Digital Development of Innovations until 2030. What does it mean? URL: https://forbes.ua/news/ukraina-zatverdila-strategiyu-tsifrovogo-rozvitku-innovatsiy-do-2030-roku-shcho-vona-peredbachae-14012025-26270 (дата звернення: 20.01.2026).

9. Hrynko T. Formation of the innovative infrastructure of Ukraine as the basis of innovative activation activities of enterprises URL: https://vlp.com.ua/files/69_1.pdf (дата звернення: 20.01.2026).

10. Mazur O. Technology parks of Ukraine state and problems URL: http://www.in.ukrproject.gov.ua/files/content/mazur_techpark1131.pdf (дата звернення: 20.01.2026).

11. Nosovets O., Voloshchuk L. The place of innovation infrastructure in determining the results of innovative activity URL: https://www.problecon.com/export_pdf/problems-of-economy-2019-3_0-pages-123_132.pdf (дата звернення: 20.01.2026).

12. Shestak Ya., Zavgorodnya Ye., Krasnoshchok V. Technical protection of the information infrastructure of a commercial enterprise. *Development of Education, Science and Business: Results 2025* URL: http://www.wayscience.com/wp-content/uploads/2025/12/Conference-Proceedings-December-18-19-2025.pdf (дата звернення: 20.01.2026).

13. Digital security transformation: change that works URL: https://ohoronapraci.kiev.ua/article/news/cifrova-transformacia-bezpeki-zmini-aki-pracuut (дата звернення: 20.01.2026).

14. Digital strategy development of innovations until 2030 URL: https://winwin.gov.ua/assets/files/WINWIN_%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D0%B0%20%D0%BF%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D1%96%D1%8F.pdf (дата звернення: 20.01.2026).

15. WINWIN. Global innovation strategy of Ukraine URL: https://winwin.gov.ua/ (дата звернення: 20.01.2026).

16. Cybersecurity URL: https://amintegrator.com/cybersecurity/ (дата звернення: 20.01.2026).