УДК: 658:005.934:004
DOI: 10.60022/3(4)-56S

Karmanenko Vasil
PhD in Pedagogical Sciences, Director
Separated Structural Subdivision "Professional College of Management, Economics and Law of Poltava State Agrarian University", Ukraine
Карманенко Василь Васильович
кандидат педагогічних наук, директор
Відокремлений структурний підрозділ «Фаховий коледж управління, економіки і права Полтавського державного аграрного університету», Україна
ORCID: 0009-0002-9769-3167

Sukhomlyn Larysa
PhD in Technical Sciences, Associate Professor
Associate Professor of the Management and Marketing
Kremenchuk Mykhailo Ostrohradskyi National University, Ukraine
Сухомлин Лариса Вадимівна
кандидат технічних наук, доцент
доцент кафедри менеджменту і маркетингу,
Кременчуцький національний університет імені Михайла Остроградського, Україна
ORCID: 0000-0001-9511-5932

Krakhmalova Tetiana
PhD in Economics, Associate Professor of the Department of Economics
Kyiv National University of Technologies and Design, Ukraine
Крахмальова Тетяна Андріївна
доктор філософії, доцент кафедри економіки
Київський національний університет технологій та дизайну, Україна
ORCID: 0000-0003-1578-8286

MANAGEMENT OF ECONOMIC AND INFORMATION SECURITY OF ENTERPRISES BASED ON DIGITALIZATION OF BUSINESS, RISK MANAGEMENT AND RESOURCE EFFICIENCY

Abstract. *The theoretical and methodological principles of management of economic and information security of enterprises based on a combination of business digitalization, risk management and resource efficiency are substantiated. It is determined that the deepening of digital transformation changes the nature of corporate security, since information, economic, resource, technological and operational risks are increasingly closely interconnected and are capable of forming cascading consequences for the functioning of the enterprise. The concept of the economic and information core of corporate security is proposed, which combines digital-information, risk-oriented, resource-economic contours and the contour of corporate resilience. A methodological toolkit for the integrated assessment of economic and information security has been developed based on the parameters of economic sustainability, information security, resource efficiency and digital maturity of the enterprise. The risk-oriented management logic has been improved by taking into account the cascading of corporate risks, which allows assessing not only the probability and potential losses from a separate threat, but also the possibility of its spread between the functional subsystems of the enterprise. The feasibility of determining the coefficient of safe digitalization has been substantiated and the concept of a digital security gap has been introduced, which arises in the event that the pace of digitalization outpaces the level of information security development. Based on the results of model testing, the paradox of unprotected digitalization has been formulated, according to which the increase in digital maturity without the synchronous development of security mechanisms can increase the overall vulnerability of the enterprise. The interpretation of resource efficiency as a functional determinant of economic security has been developed, which involves achieving a balance between optimizing the use of resources, their reservation and the ability to support critical business processes. The principle of digital security synchronization is formulated, according to which the expansion of the digital contour of the enterprise should be accompanied by the appropriate development of information protection, risk management, resource reservation and recovery scenarios. The practical significance of the proposed approach lies in the possibility of its use for diagnosing the security state*

© Автор(и). Ця стаття знаходиться у відкритому доступі та розповсюджується відповідно до умов ліцензії Creative Commons Attribution 4.0 (https://creativecommons.org/licenses/by/4.0/)

of enterprises, identifying critical imbalances in digital development, substantiating management decisions and forming corporate resilience in conditions of high uncertainty.

Keywords: *management, economic security, information security, business digitalization, risk management, resource efficiency, corporate resilience, digital maturity, cascading risks, digital security gap.*

МЕНЕДЖМЕНТ ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ НА ОСНОВІ ЦИФРОВІЗАЦІЇ БІЗНЕСУ, РИЗИК-МЕНЕДЖМЕНТУ ТА РЕСУРСОЕФЕКТИВНОСТІ

Анотація. *Обґрунтовано теоретико-методичні засади менеджменту економічної та інформаційної безпеки підприємств на основі поєднання цифровізації бізнесу, ризик-менеджменту та ресурсоефективності. Визначено, що поглиблення цифрової трансформації змінює природу корпоративної безпеки, оскільки інформаційні, економічні, ресурсні, технологічні та операційні ризики дедалі тісніше взаємопов'язуються та здатні формувати каскадні наслідки для функціонування підприємства. Запропоновано концепцію економіко-інформаційного ядра корпоративної безпеки, що поєднує цифрово-інформаційний, ризик-орієнтований, ресурсно-економічний контури та контур корпоративної резильєнтності. Розроблено методичний інструментарій інтегрального оцінювання економіко-інформаційної безпеки за параметрами економічної стійкості, інформаційної захищеності, ресурсоефективності та цифрової зрілості підприємства. Удосконалено ризик-орієнтовану логіку управління шляхом урахування каскадизації корпоративних ризиків, що дозволяє оцінювати не лише ймовірність та потенційні втрати від окремої загрози, а й можливість її поширення між функціональними підсистемами підприємства. Обґрунтовано доцільність визначення коефіцієнта безпечної цифровізації та введено поняття цифрового безпекового розриву, який виникає в разі випередження темпами цифровізації рівня розвитку інформаційного захисту. За результатами модельної апробації сформульовано парадокс незахищеної цифровізації, відповідно до якого нарощування цифрової зрілості без синхронного розвитку безпекових механізмів може посилювати сукупну вразливість підприємства. Розвинуто трактування ресурсоефективності як функціональної детермінанти економічної безпеки, що передбачає досягнення балансу між оптимізацією використання ресурсів, їх резервуванням та здатністю підтримувати критичні бізнес-процеси. Сформульовано принцип цифрово-безпекової синхронізації, згідно з яким розширення цифрового контуру підприємства має супроводжуватися відповідним розвитком інформаційного захисту, ризик-менеджменту, ресурсного резервування та сценаріїв відновлення. Практичне значення запропонованого підходу полягає у можливості його використання для діагностики безпекового стану підприємств, виявлення критичних дисбалансів цифрового розвитку, обґрунтування управлінських рішень та формування корпоративної резильєнтності в умовах високої невизначеності.*

Ключові слова: *менеджмент, економічна безпека, інформаційна безпека, цифровізація бізнесу, ризик-менеджмент, ресурсоефективність, корпоративна резильєнтність, цифрова зрілість, каскадні ризики, цифровий безпековий розрив.*

Formulation of the problem. A modern enterprise operates in an environment where economic and information threats are increasingly difficult to distinguish, as the digitalization of business processes simultaneously creates new sources of economic efficiency and forms additional contours of vulnerability. Automation of operational activities, the use of cloud services, corporate information systems, artificial intelligence, big data, digital platforms and remote interaction channels significantly accelerate management decision-making, but increase the dependence of enterprises on the continuity of information flows, data reliability and security of digital infrastructure. Under such conditions, a violation of information security can almost instantly transform into economic losses due to the suspension of business processes, loss of information assets, violation of contractual obligations, increased transaction costs, deterioration of business reputation and a decrease in the market value of the enterprise. This issue is particularly acute for Ukrainian business, which simultaneously operates under the influence of military, financial, energy, logistics, personnel, technological and cyber threats. In such conditions, the traditional model of economic security, focused mainly on financial stability, solvency, asset protection and counteraction to individual internal and external risks, no longer provides the necessary level of corporate resilience. The information system of the enterprise is becoming an integral part of its economic infrastructure, and the loss of data, disruption of the availability of

digital services or compromise of management information can have consequences comparable to the physical loss of part of the production resources. In this regard, the very management paradigm of enterprise security is changing. Its basis should not be a reaction to an already realized threat, but preventive identification of risks, forecasting their cascading impact and forming the organizational ability of the enterprise to maintain critical business functions under various destabilization scenarios. Economic and information security under this approach form an interconnected management circuit, within which financial, resource, information, technological and organizational decisions should be made on the basis of a single risk assessment system. At the same time, digitalization should not be considered solely as a source of new threats. With proper management, it is digital technologies that create fundamentally new opportunities for ensuring economic security. Intelligent information systems make it possible to continuously monitor business operations, detect anomalies, predict resource shortages, assess financial risks, control costs, optimize logistics flows, and timely identify deviations from regulatory parameters. Thus, there is a gradual transition from the digitalization of business processes to the digitalization of the corporate security mechanism itself.

Resource efficiency is of particular importance in this system. In conditions of shortage of financial, material, energy and human resources, the ability of an enterprise to provide a greater economic result with the optimal volume of resources used directly determines its margin of stability. Excessive resource intensity, critical dependence on individual suppliers, inefficient use of energy, insufficient asset turnover or the absence of reserve resource circuits increase the sensitivity of the enterprise to external shocks. Therefore, resource efficiency should be considered not only as a characteristic of operational performance, but also as a functional determinant of economic security. Under these circumstances, risk management performs an integrating function between digitalization, economic security, information protection and resource efficiency. Its task is to transition from fragmented management of individual risks to the formation of their holistic portfolio, taking into account interdependence. An information incident can cause an operational failure, an operational failure can cause financial losses, financial losses can cause resource constraints, and the latter, in turn, can reduce the company's ability to invest in information security. It is the emergence of such cascading risk effects that requires a revision of the traditional corporate security architecture.

Therefore, the scientific problem is the need to form an integrated management system for the economic and information security of the enterprise, in which digitalization provides information and analytical management capabilities, risk management performs a preventive and coordination function, and resource efficiency forms an economic reserve for business stability. Such a system should ensure not only the protection of the enterprise from current threats, but also its ability to anticipate risks, adapt the resource configuration, maintain the continuity of critical processes, and recover from destabilizing impacts with minimal economic losses. It is the insufficient methodological elaboration of the relationship between these four components – economic security, information security, digitalization, and resource efficiency through risk management tools – that determines the relevance of the research and the need to develop an integrated management approach to ensuring the sustainability of modern enterprises.

Analysis of recent research and publications. The issue of management of economic and information security of enterprises belongs to the interdisciplinary scientific field formed at the intersection of management theory, risk management, economic security, digital economy, resource management and strategic business sustainability. The deepening digital transformation of the business sector has significantly changed the scientific understanding of the nature of corporate security. If in traditional studies its provision was associated mainly with the protection of the economic interests of the enterprise, maintaining financial stability, solvency and preservation of material assets, then the modern scientific discourse is gradually shifting to a comprehensive study of the interdependence of economic, information, digital, technological, resource and organizational risks. An important theoretical basis for such an understanding is the development of a risk-oriented management paradigm, according to which the security of an enterprise is determined not by the absolute absence of threats, which is practically impossible in the modern economic environment, but by its ability to timely identify risks, assess the probability and scale of potential losses, form preventive response mechanisms and maintain the continuity of key business processes. Accordingly, risk management is increasingly considered not as a local control function, but as a component of strategic management, integrated into the management decision-making system (Stasyuk O., Shary V., Zos-Kior M., Kyrylyuk I., etc.) [1-4].

In parallel, the digitalization of business has formed a fundamentally new direction of research into enterprise information security. The development of cloud technologies, digital platforms, electronic document management, corporate information systems, Big Data, artificial intelligence and automated systems for supporting management decisions has increased the economic value of information and at the same time increased the dependence of enterprises on its availability, integrity and confidentiality. As a result, the information resource ceases to perform only an auxiliary function and turns into one of the strategic assets of the enterprise. It is this transformation that changes the ratio of economic and information security. Loss of

information, blocking of digital infrastructure, disruption of the corporate information system, compromise of commercial data or manipulation of management information can directly cause economic losses. At the same time, insufficient financial resources, inefficient asset management or resource constraints reduce the ability of the enterprise to invest in digital infrastructure and its protection systems. Thus, a two-way causal relationship is formed, in which information security affects the economic stability of the enterprise, and economic capacity determines the possibilities of ensuring the appropriate level of information protection (Hnatenko I., Zos-Kior M., Ilyin V., Svyryda E., etc.) [5-10].

A separate area of modern research is the issue of resource efficiency. Traditionally, it is considered through the ratio of used resources and obtained economic results, cost optimization, energy saving, material consumption and productivity. However, with high turbulence in the external environment, resource efficiency acquires a security meaning. An enterprise that has a critically high resource intensity, depends on one supplier or one energy source, does not form reserve capacities and does not have alternative logistics routes, can demonstrate high short-term economic efficiency, but at the same time remain strategically vulnerable. This allows us to distinguish between the concepts of operational efficiency and security resource efficiency. In the first case, the dominant criterion is the minimization of costs per unit of output, while in the second it is necessary to also take into account the reservation, diversification, interchangeability of resources, the speed of their redistribution and the ability of the enterprise to maintain critical functions in conditions of shortage. Therefore, resource efficiency in modern management should be studied not only as a tool for increasing profitability, but as a component of the formation of a reserve of economic stability of the enterprise [3; 4-6; 9].

The development of the concept of digital business resilience requires special attention. Its content goes beyond traditional cyber security and involves the ability of an enterprise to maintain the functioning of digital business processes during destabilizing influences, localize the consequences of an information incident, restore the digital infrastructure and adapt it after the threat is realized. With this interpretation, security moves from the logic of "protect at any cost" to the logic of "predict – counteract – localize – restore – adapt". At the same time, the analysis of scientific developments allows us to identify a certain fragmentation of existing approaches. Economic security, information security, digitalization, risk management and resource efficiency are mostly formed as related, but relatively autonomous areas of research. This complicates the explanation of situations when one primary risk triggers a chain reaction in other functional subsystems of the enterprise. For example, a cyberattack can cause the unavailability of a corporate information system, which leads to the suspension of operations, disruption of logistical connections, non-fulfillment of contracts, financial losses and a shortage of working capital. Thus, one information risk is successively transformed into operational, logistical, financial and resource risks. That is why the subject of management should be not only a separate threat, but also the trajectory of risk spread within the enterprise. On this basis, it is advisable to introduce the concept of corporate risk cascading, which is proposed to be understood as the process of sequential spread of the negative impact of the primary threat between interconnected functional subsystems of the enterprise with the emergence of secondary risks and a multiplicative increase in total economic losses. Accordingly, an integrated approach to the management of economic and information security requires scientific development, within which the digitalization of business is considered both as a source of new risks and a means of their early detection; risk management, as a mechanism for identification, assessment and preventive response; resource efficiency, as a tool for forming a reserve of economic stability; and economic and information security as interrelated resulting characteristics of corporate resilience. It is the insufficient methodological elaboration of such an interrelation that determines the need to form an integrated digital contour of the management of the economic and information security of the enterprise, capable of combining risk monitoring, resource sustainability assessment, digital analytics, preventive management and business process recovery mechanisms in a single management decision-making system.

The purpose of the article is to analyze the system of managing the economic and information security of enterprises based on business digitalization, risk management, and resource efficiency.

The main material presentation. The modern transformation of the enterprise management system is taking place under the simultaneous influence of digitalization, the growth of information dependence of business, the complication of the corporate risk structure and the need to ensure resource sustainability. Under such conditions, economic and information security cease to be autonomous functional areas of management. They form an interconnected circuit within which a violation of the stability of one subsystem can cause negative consequences for the entire system of enterprise functioning. The fundamental change is that digitalization turns information into a resource that simultaneously ensures the creation of economic value and concentrates a significant part of new corporate risks. Data about customers, suppliers, financial transactions, technological processes, inventories, logistics, production facilities and management decisions are increasingly integrated into single digital systems. Accordingly, a violation of the availability or integrity of such systems may affect

not a separate information function, but the ability of the enterprise to carry out its main economic activity. That is why it is advisable to proceed from the position of forming an economic and information core of corporate security, which is proposed to be understood as a set of interconnected managerial, economic, digital, information and resource mechanisms aimed at preserving the critical functions of the enterprise, minimizing potential losses and ensuring its ability to adapt and recover after the implementation of risk events [2; 4-6]. At the same time, the category of security itself requires a shift in emphasis from security to managed stability. A completely protected enterprise in the conditions of the digital economy is practically impossible, since the elimination of some risks is accompanied by the emergence of others. Therefore, the effectiveness of management is determined not by the number of formally neutralized threats, but by the system's ability to detect critical deviations in advance, localize their spread and restore functioning with an acceptable level of economic losses. On this basis, it is proposed to consider the management of the enterprise's economic and information security through four interconnected contours (Fig. 1).

The digital-information contour provides data generation, protection, analytical processing and use for making management decisions. The risk-oriented contour is responsible for identifying, assessing, ranking and forecasting threats. The resource-economic contour characterizes the ability of an enterprise to provide critical processes with the necessary financial, material, energy, information and human resources. The contour of corporate resilience integrates the previous components and determines the ability of a business to absorb negative impact, support critical functions, recover and transform after the risk is realized [1; 3; 7-9].

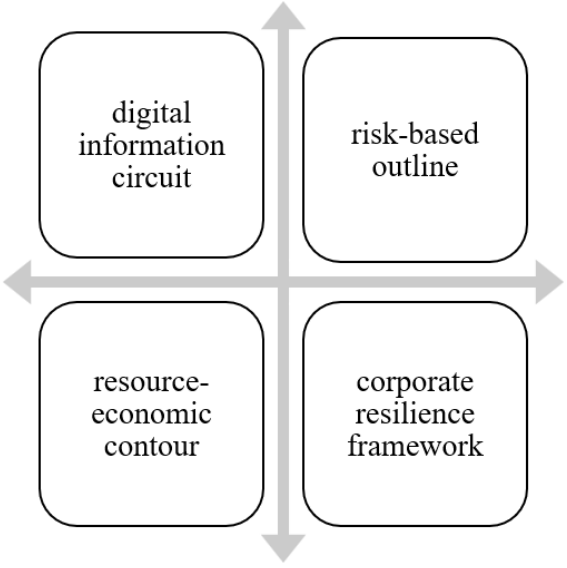


Fig. 1. Contours of economic and information security management of an enterprise
Source: proposed by the authors

Thus, a cyclical rather than linear management logic is formed: data; risk; management decision; resource provision; reaction; recovery; accumulation of new data. It is the closedness of such a cycle that creates the possibility of transition from a reactive to a preventive-adaptive security model.

For quantitative diagnostics of the proposed system, it is advisable to form an integral index of the economic and information security of the enterprise:

$$IEIS = w1E + w2I + w3R + w4D$$

where *IEIS* is the integral index of economic and information security; E is the level of economic sustainability; I is the level of information security; R is the level of resource efficiency; D is the level of digital maturity; *w1...w4* are weighting factors, and:

$$j = 1\sum 4wj = 1$$

The fundamental feature of such an index is the inclusion of digital maturity and resource efficiency not as external factors, but as direct determinants of security. A high level of digitalization without an appropriate level of information protection can not increase, but, on the contrary, reduce the overall stability of the enterprise

due to the expansion of the surface of digital risks. Therefore, it is additionally proposed to determine the coefficient of safe digitalization:

$$K_{SD} = \frac{I}{D}$$

where *KSD* is the coefficient of safe digitalization; I is the normalized level of information security; *D* is the normalized level of business process digitalization.

With KSD≥1, the development of information security does not lag behind the pace of digitalization. The value of KSD<1 signals the emergence of a digital security gap, when the enterprise increases digital dependence faster than the ability to protect it.

Such a gap is especially dangerous in the case of active implementation of cloud technologies, remote access, integrated ERP/CRM systems, automated production systems and artificial intelligence technologies. The economic efficiency of digitalization in this case may be accompanied by the accumulation of hidden information risk.

The next element is the quantitative assessment of corporate risks. For each risk, it is proposed to determine the baseline level:

$$Ri = Pi \times Li$$

where *Pi* is the probability of the *i-th* risk occurring; *Li* is the potential scale of economic losses.

However, the classical construction of "probability × consequences" is not sufficient for a digitalized enterprise, since it does not take into account the ability of the primary risk to spread between subsystems. Therefore, it is proposed to introduce a risk cascading coefficient:

$$Kcas, i = 1 + \frac{Ns, i}{N}$$

where *Ns,i* is the number of functional subsystems to which the *i-th* risk can spread; *N* is the total number of critical subsystems of the enterprise.

The adjusted risk level will be:

$$Ri^* = Pi \times Li \times Kcas,i$$

With the same initial probability, the second risk should have a much higher management priority. An important difference of the proposed approach is the inclusion of resource efficiency directly into the security management system. For its basic assessment, the ratio can be used:

$$RE = \frac{V}{Cr}$$

where *RE* is resource efficiency; *V* is the added value created or the result of the activity; *Cr* is the total cost of the resources used.

However, a high *RE* indicator does not mean high stability. An enterprise can minimize inventories, work with one supplier and abandon reserve capacities, while demonstrating high current efficiency. When an external shock occurs, such a model becomes vulnerable.

Therefore, it is advisable to supplement resource efficiency with a resource reservation coefficient:

$$Krr = \frac{Rres}{Rcrit}$$

where *Rres* is the amount of available reserve or alternative resources; *Rcrit* is the minimum amount of resources required to support critical business processes.

It is the combination of *RE* and Krr that allows us to move from the traditional logic of "minimum resources – maximum result" to the security logic of "optimal resource – maximum stability". This is a fundamental position. Excessive redundancy reduces economic efficiency, while insufficient redundancy increases the risk of business interruption. Therefore, the task of management is not to maximize reserves, but to determine their economically justified level. The integrated contour of risks of economic and information

security of the enterprise is shown in Table 1.

Table 1

Integrated contour of risks of economic and information security of the enterprise

Risk group	Key manifestation	Potential economic impact	Digital control tool	Management response
Financial	liquidity shortage, currency fluctuations	reduced solvency	BI analytics, predictive analytics	backup, scenario budgeting
Information	data loss or corruption	direct and indirect financial losses	DLP, SIEM, backup	protection, redundancy, recovery
Cyber risks	unauthorized access, attack	stopping digital processes	SOC, AI monitoring	localization and response
Resource	material or energy shortage	reduced production	ERP, digital monitoring	backup, diversification
Logistics	supply disruption	increased costs and downtime	SCM systems	alternative routes
Operational	failure of a critical process	loss of productivity	digital twins, IoT	backup scenarios
Reputational	loss of counterparty trust	reduced sales	digital monitoring	crisis communications
Management	late or erroneous decisions	multiplication of other losses	DSS, AI analytics	scenario and preventive management

Source: author's development

The presented systematization shows that modern risk rarely remains within one functional area. It is the digital interconnectedness of business processes that increases the speed of its spread. Therefore, the task of management is not only to reduce the probability of individual threats, but also to break the chains of their cascading. In this context, it is proposed to form a digital security and resource contour of the enterprise, the structural logic of which is expedient to present in this way (Fig. 2).

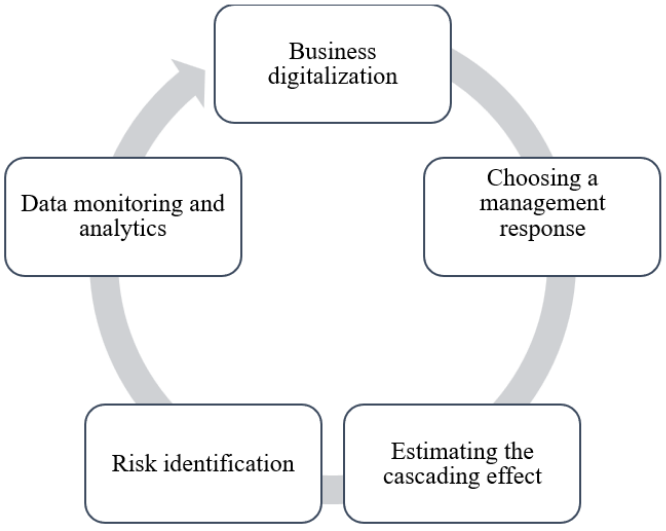


Fig. 2. Digital security and resource contour of the management of economic and information security of the enterprise
Source: author's development

The fundamental difference of the proposed contour is that the final result of management is determined not only by risk minimization. In a real business environment, complete elimination of risk is often either impossible or economically unjustified. Therefore, the result should be managed corporate resilience - the ability of the enterprise to accept an acceptable level of risk, localize its negative impact, support critical functions and ensure accelerated recovery. This is where digitalization, risk management and resource efficiency cease to be three parallel areas of management. They form a triad of ensuring the economic and informational stability of the enterprise: digitalization creates information visibility of processes, risk management turns information into a preventive management decision, and resource efficiency provides the economic ability to implement this decision.

For practical implementation of the proposed approach, it is advisable to form a diagnostic system

that allows simultaneously assessing the economic sustainability, information security, resource efficiency and digital maturity of the enterprise. The methodological complexity lies in the fact that the specified characteristics have different economic nature and are measured by different indicators. Therefore, to ensure their comparability, it is advisable to normalize the primary indicators in the interval [0;1][0;1].

For indicators-stimulators, the growth of which has a positive effect on the security of the enterprise, normalization is carried out according to the formula**:**

$$x_{ij+} = \frac{x_{ij} - x_{jmin}}{x_{jmax} - x_{jmin}}$$

and for disincentive indicators:

$$x_{ij+} = \frac{x_{jmax} - x_{ij}}{x_{jmax} - x_{jmin}}$$

where x_{ij} is the actual value of the jth indicator for the ith enterprise; xj_{min}, xj_{max} are the minimum and maximum values of the indicator in the studied population, respectively.

After normalization, the partial components of economic and information security acquire a comparable form. For the approbation calculation, it is proposed to use four blocks: *E* – economic stability; *I* – information security; *R* – resource efficiency; *D* – digital maturity. At the same time, the equivalence of the specified components does not fully correspond to the modern nature of corporate risks. Economic stability and information security directly determine the ability of the enterprise to maintain functionality, therefore it is advisable to give them a slightly greater weight. For model approbation, we will assume:

$$wE = 0{,}30;\ wI = 0{,}30;\ wR = 0{,}20;\ wD = 0{,}20$$

Therefore:

$$IEIS = 0{,}30E + 0{,}30I + 0{,}20R + 0{,}20D$$

The proposed weights in this approbation are of a model nature; in further empirical studies they can be refined by the expert evaluation method, AHP or entropy method (Table 2).

Table 2

Initial normalized parameters of the model sample of enterprises

Enterprise	Economic sustainability E	Information Security I	Resource efficiency R	Digital maturity D
П1	0,82	0,76	0,71	0,88
П2	0,68	0,61	0,79	0,84
П3	0,74	0,81	0,65	0,72
П4	0,57	0,49	0,62	0,78
П5	0,88	0,86	0,83	0,91

Source: generated by the authors for model testing of the methodology

For enterprise P1, the integral indicator will be:

$$IEIS(P1) = 0{,}30(0{,}82) + 0{,}30(0{,}76) + 0{,}20(0{,}71) + 0{,}20(0{,}88) = 0{,}792$$

Similarly, we get:

$$IEIS(P2) = 0{,}704;\ IEIS(P3) = 0{,}739;\ IEIS(P4) = 0{,}598;\ IEIS(P5) = 0{,}872$$

The following scale is proposed for interpreting the results: 0.00–0.39 – critical level; 0.40–0.59 – low; 0.60–0.74 acceptable; 0.75–0.89 – high; 0.90–1.00 – very high level of economic and information security.

So, the highest integral position is demonstrated by P5 – 0.872, while the most problematic configuration is P4 – 0.598. At the same time, the integral value itself does not yet show a structural imbalance in security. An enterprise may have an acceptable overall index, but critically lag behind one of the components.

To identify it, we will use the coefficient of safe digitalization proposed above:

$$KSD = \frac{I}{D}$$

The calculation results are (Table 3).

Table 3

Simulation calculation results

Enterprise	I	D	KSD	Diagnostic characteristic
П1	0,76	0,88	0,864	moderate gap
П2	0,61	0,84	0,726	significant gap
П3	0,81	0,72	1,125	balanced development
П4	0,49	0,78	0,628	critical gap
П5	0,86	0,91	0,945	close to balance

Source: author's calculations

The results obtained demonstrate an important pattern. A high level of digitalization in itself is not a sign of high security. This is most clearly seen for P4: digital maturity is 0.78, while information security is only 0.49. The value of KSD=0.628 means that the digital transformation of the enterprise is occurring much faster than the development of its protection systems. This allows us to formulate the concept of the paradox of unprotected digitalization: an increase in the digital maturity of the enterprise in the absence of synchronous development of information security after a certain limit does not reduce, but potentially increases its overall vulnerability.

For strategic diagnostics, it is advisable to use a two-dimensional positioning of the enterprise at levels D and I. The matrix of strategic positioning of the enterprise "digitalization – information security" is depicted in Table 4.

Table 4

Matrix of strategic positioning of the enterprise "digitalization - information security"

	Low information security	High information security
High digitalization	Zone I – digital vulnerability	Zone II – protected digitalization
Low digitalization	Zone III – systemic backwardness	Zone IV – security reserve of digital development

Source: author's development

The most dangerous of the positions of hidden risk is precisely zone I "digital vulnerability". Such an enterprise may outwardly look technologically advanced: use ERP, CRM, cloud technologies, electronic document management, artificial intelligence and automated analytics. However, the lag of information protection creates a situation where each subsequent digital integration simultaneously expands the potential risk surface. The most desirable is zone II "secure digitalization", in which digital transformation is synchronized with the development of information security. It is this state that should be defined not as an endpoint, but as a dynamic equilibrium: each technological innovation should be accompanied by an appropriate review of risks and protection mechanisms.

Separate methodological development is required to assess situations when one threat is sequentially transformed into several types of losses. For this purpose, it is proposed to determine the cascade exposure index:

$$CEIi = Pi \times Li \times Kcas,i \times Ti$$

where *Ti* is the criticality coefficient of the response time.

The introduction of *Ti* is fundamental, since for a digital business, threats of the same scale can have different consequences depending on the speed of response. For example, restoring an information system within 15 minutes and within two days creates a fundamentally different economic effect. Accordingly, it is advisable to evaluate another indicator – the business recovery coefficient:

$$Krec = \frac{Tnorm}{Tfact}$$

where *Tnorm* is the normatively permissible recovery time of a critical process; *Tfact* is the actual

recovery time.

For $Krec \geq 1$, the enterprise recovers the process within the permissible time; for $Krec < 1$, the recovery speed is insufficient.

This indicator transfers the assessment from the plane of "did an incident occur" to a much more important plane for management – "how quickly the enterprise restored the critical function". Based on the conducted research, it is proposed to consider corporate resilience as a resulting characteristic of the interaction of economic security, information security, resource sustainability and resiliency:

$$CR = IEIS \times Krec \times (1-Rc)$$

where *CR* is the level of corporate resilience; *IEIS* is the integral level of economic and information security; *Krec* is the normalized coefficient of recovery; *Rc* is the normalized residual critical risk.

The proposed dependence reflects the principle: high security without the ability to quickly recover does not mean high resilience. Similarly, rapid recovery at a critical level of residual risk can only provide a short-term return to work without eliminating the systemic causes of vulnerability. It is organizational learning after the risk is realized that completes the cycle. An incident should not end only with the restoration of the system. Its results should be transformed into new response algorithms, adjustments to the digital architecture, changes in reservation standards, revision of the risk profile and updates to management scenarios. Thus, the digitalization of business takes on a dual nature. On the one hand, it forms new points of vulnerability, on the other hand, it creates a toolkit for early warning and intelligent management of them. Therefore, the strategic task of the enterprise is not maximum digitalization, but safe digitalization, in which the pace of technological transformation does not outpace the development of information protection, risk management and resource capacity. Generalizing the results obtained allows us to propose the principle of digital-security synchronization: each significant expansion of the enterprise's digital contour should be accompanied by a proportional revision of its information protection, risk profile, resource reservation and recovery scenarios. It is such synchronization that ensures the transition from a digitalized enterprise to a digitally resilient enterprise, for which information technologies are not only a tool for increasing productivity, but also a component of the economic sustainability system.

Further development of the proposed approach should be associated with the formation of an adaptive management system capable not only of responding to already realized risks, but also of changing its own configuration depending on the nature of threats, availability of resources and the level of digital load. Such a system should operate on the principle of constant adjustment of management decisions based on new data, monitoring results and residual risk assessment. In this case, economic and information security acquire the characteristics of a dynamic management category that changes together with the enterprise and its operating environment. An important element of such a model is the formation of a single information and analytical security space. Its task is to consolidate data on the financial condition, resource provision, operational deviations, information incidents, logistical violations and the criticality of individual business processes. It is the integrated presentation of this data that allows management to assess not local risk, but its potential impact on the overall stability of the enterprise. The speed of management response is of particular importance. In a digital environment, the time lag between the emergence of a threat and the decision-making process often determines the scale of future losses. Therefore, the effectiveness of a security system should be assessed not only by the level of protection, but also by the ability of an enterprise to quickly detect deviations, make decisions and mobilize the necessary resources. In this context, digital analytics creates the prerequisites for the transition from periodic control to continuous monitoring of the security status. At the same time, the technological component cannot completely replace the management component. Automated systems are able to quickly process significant amounts of information, detect anomalies and form predictive scenarios, but the final choice of management response should take into account the strategic goals of the enterprise, the permissible level of risk, resource constraints and possible long-term consequences. Therefore, digital technologies should be considered as a tool for strengthening management capacity, and not as its replacement. An important prerequisite for the effectiveness of the proposed system is also the development of a corporate security culture. Even with a high level of digital protection, a significant part of the risks may arise due to personnel errors, neglect of procedures, low digital discipline or insufficient understanding of the consequences of information incidents. Therefore, economic and information security must be integrated into the daily management practices of the enterprise and perceived as a joint responsibility of management and employees. An equally important direction is the combination of the security system with strategic planning. Each decision to expand the digital infrastructure, enter new markets, change logistics chains, automate production or attract new technological platforms changes the configuration of the enterprise's risks. Therefore,

the assessment of economic and information threats should be carried out not after the adoption of a strategic decision, but directly during its preparation. In such a logic, risk management is transformed from a control function into a component of strategic design. Its role is to identify potential destabilization scenarios, assess critical dependencies and form alternative management solutions before the risk is realized. This allows you to minimize not only direct losses, but also indirect consequences associated with loss of time, disruption of supply chains, decline in reputation or reduction of trust from partners. In the context of resource efficiency, the balance between optimization and redundancy becomes of particular importance. The desire to minimize costs can create additional vulnerability if the company loses its stocks, backup supply channels or redundant systems. Therefore, resource efficiency should be assessed not only through savings, but also through the ability of the resource system to ensure the continuity of critical business processes under adverse conditions.

Thus, the optimal resource model is not the least expensive, but a sustainably effective one, in which the costs of reservation are economically justified from the perspective of potential losses from the suspension of activities. This approach allows you to integrate resource planning into the security system and form a reasonable margin of stability without excessive accumulation of resources. An important management tool within the proposed concept is scenario modeling. The enterprise must identify possible scenarios of information, operational or resource stability disruption in advance and establish a sequence of actions for each of them. This ensures a reduction in response time, a reduction in organizational uncertainty and an increase in the consistency of actions between functional units. The distribution of management responsibility is also of significant importance. In a digitalized enterprise, risks often cover several functional areas at the same time, so the absence of a clearly defined risk owner can lead to duplication of functions or, conversely, to management gaps. The formation of a clear responsibility system allows you to increase the speed of response and ensure personalized control over critical risks.

Therefore, the proposed economic and information security management system should be considered as an adaptive contour of strategic management, which combines digital analytics, risk management, resource planning and recovery mechanisms. Its key result is not the absolute elimination of risks, but the formation of the enterprise's ability to maintain manageability, functionality and economic sustainability under the conditions of their implementation. On this basis, we can conclude that modern security management is gradually moving from the logic of protecting individual assets to the logic of managing the integral viability of the enterprise. It is this transformation that allows us to combine economic efficiency, information security, resource flexibility and digital adaptability into a single system for forming long-term corporate resilience.

Conclusions. According to the results of the study, it was found that the digitalization of business fundamentally changes the content of the management of economic and information security of enterprises, strengthening the interdependence of financial, resource, information, technological and operational processes. Under such conditions, the traditional separation of economic security from information security loses its managerial expediency, since disruption of the functioning of the digital infrastructure can directly transform into economic losses, and resource and financial limitations, in turn, reduce the ability of the enterprise to maintain the required level of information protection. The feasibility of transitioning from a reactive model of countering threats to preventive-adaptive management focused on early detection of risks, forecasting their spread, ensuring the continuity of critical business processes and accelerated recovery of the enterprise after destabilizing influences is substantiated. In this context, the formation of an economic-information core of corporate security, which integrates digital-information, risk-oriented, resource-economic contours and the contour of corporate resilience, is proposed. A methodological approach to the integrated assessment of the economic and information security of an enterprise has been developed, which takes into account economic sustainability, information security, resource efficiency and digital maturity. The proposed toolkit allows not only to determine the overall level of security, but also to identify structural imbalances between individual components. Of particular importance is the assessment of the coefficient of safe digitalization, which determines the correspondence of the pace of development of information protection to the level of digital transformation of business processes. The provision on the cascading of corporate risks has gained scientific development, according to which the primary threat is able to spread between interconnected functional subsystems of the enterprise and generate secondary information, operational, financial, resource and reputational losses. The proposed consideration of the cascading coefficient allows assessing the risk not only by the probability of its occurrence and the scale of direct consequences, but also by the potential for systemic spread within the enterprise. It has been established that a high level of digital maturity cannot automatically be interpreted as a sign of high corporate security. The results of the model testing revealed the possibility of a digital security gap when the intensity of digitalization outpaces the development of information protection. On this basis, the paradox of unprotected digitalization was formulated, according to which further growth of digital dependence without synchronous strengthening of security systems may not reduce, but increase the overall vulnerability of the enterprise. A new place for resource efficiency in the security management system was substantiated. It

was proposed to consider it not only as a tool for minimizing costs and increasing operational efficiency, but as a factor in forming a reserve of economic stability. Accordingly, the management priority should not be the maximum reduction of resources, but the search for an economically justified balance between efficiency, redundancy, diversification and the ability to support critical functions of the enterprise. The generalization of the results made it possible to formulate the principle of digital-security synchronization, according to which the expansion of the digital contour of the enterprise should be accompanied by a proportional development of information protection, a review of the risk profile, resource redundancy and recovery scenarios. It is the observance of this principle that ensures the transition from a formally digitalized to a digitally resilient enterprise, capable of using digital technologies simultaneously as a tool for increasing economic efficiency and a mechanism for strengthening corporate resilience. Therefore, the scientific value of the proposed approach lies in the formation of a holistic logic of "digitalization – risk management – resource efficiency – economic and information security – corporate resilience". The practical use of such an approach creates opportunities for timely diagnosis of critical risks, justification of management priorities, optimization of resource provision and increasing the ability of enterprises to maintain business continuity in conditions of high uncertainty. Prospects for further research are associated with empirical testing of the proposed methodological tools at enterprises of various types of economic activity, refinement of the weight parameters of the integral index, formation of industry thresholds of digital security and development of intelligent early warning systems for cascading corporate risks.

References

1. Stasiuk O. Zmist ta peredumovy vynyknennia tsyfrovizatsii u funktsionuvanni sotsialno-ekonomichnykh system. *Naukovyi visnyk Polissia*. 2025. № 1 (30). S. 87–98.

2. Sharyi V. I., Zos-Kior M. V., Kyryliuk I. M. Instytutsiina model zemelnykh vidnosyn v Ukraini. *Visnyk Cherkaskoho natsionalnoho universytetu imeni Bohdana Khmelnytskoho. Seriia Ekonomichni nauky*. 2020. № 2. S. 107–116.

3. Hnatenko I. A., Kulikova Yu. E. Perspektyvni napriamy vdoskonalennia upravlinnia personalom v orhanizatsii. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia: Ekonomichni nauky*. 2016. № 16 (4). S. 55–58.

4. Bilyk O. I. Rozvytok systemy publichnoho upravlinnia sotsialnymy ryzykamy v umovakh tsyfrovykh transformatsii: dys. … d-ra nauk z derzh. upravl.: 25.00.02 – «Mekhanizmy derzhavnoho upravlinnia». Mykolaiv, 2021. 535 s.

5. Zos-Kior M., Iliin V., Svyryda E. Rozvytok trudovoho potentsialu v systemi efektyvnoho menedzhmentu orhanizatsii. *Ekonomika ta suspilstvo*. 2020. № 22.

6. Hnatenko I. A., Snitko Ye. O., Markov R. V., Utkin V. P. Upravlinnia proektamy klasteryzatsii innovatsiinoho pidpryiemnytstva ahroprodovolchoi sfery v umovakh realizatsii stratehii staloho rozvytku, hlobalizatsii, didzhytalizatsii, ekonomichnoi kultury suspilstva, lohistychnoho ta kadrovoho menedzhmentu. *Formuvannia rynkovykh vidnosyn v Ukraini*. 2021. № 9. S. 106–113.

7. Nikitenko V. O., Vasylchuk H. M., Merzhynskyi Ye. K. Merezheva ekonomika yak chynnyk pidvyshchennia efektyvnosti tsyfrovizatsii u konteksti evoliutsii tsyfrovoho suspilstva vid 1G do 5G. *Humanities Studies*. 2022. № 10 (87). S. 112–121.

8. Hnatenko I. A., Popova Yu. M., Bachkir I. H., Nechyporenko K. V. Stratehii derzhavnykh priorytetiv v konteksti stsenarnoho forsaitu upravlinnia innovatsiinoiu ekonomikoiu: modeliuvannia naukovo-tekhnichnoho ta intelektualnoho potentsialu. *Ahrosvit*. 2021. № 17. S. 3–9.

9. Dolhopol O., Kuznetsova K. Mistianyn i urbanizatsiia: psykholohichni transformatsii ta filosofskyi poshuk sensu. *Naukovo-teoretychnyi almanakh Hrani*. 2025. T. 28. № 5. S. 188–196.

10. Voitsitska K. M. Ekonomichnyi rozvytok urbanizovanykh terytorii yak naukove doslidzhennia v sferi publichnoho upravlinnia. *Ekonomika, upravlinnia ta administruvannia*. 2022. № 3 (101). S. 41–47.

Отримано: 30.03.2026
Прийнято до публікації: 14.04.2026
Опубліковано: 15.04.2026