Baltic J. Modern Computing, Vol. 14 (2026), No. 4, 764-782
https://doi.org/10.22364/bjmc.2026.14.4.03

Cost-Effectiveness of AI Implementation in Information Security: A Systematic Review

Vladyslava LIUBARETS[1], Anhelina SPITSYNA[2], Oleksandra TERESHCHENKO[3], Dmytro ZAHORODNII[4], Serhii BREZETSKYI[1]

[1]Department of Intellectual Systems and Digital Technologies, Academy of Labor, Social Relations and Tourism, 03187, 3-A Kiltseva Road Str., Kyiv, Ukraine
[2]Department of Economics, National Transport University
01010, 1 Mykhaila Omelianovycha-Pavlenka Str., Kyiv, Ukraine
[4]DataArt Solutions Inc, 10016, 475 Park South Ave., New York, USA
[4]Department of Economics and Business Management, Interregional Academy of Personnel Management, 03039, 2 Frometivska Str., Kyiv, Ukraine

v.v.lubarets@ukr.net, angel7a@ukr.net, tereshchenko_oleksandra@edu-iosa.org, saintdexter777@gmail.com, Sergey.brezetskiy@gmail.com

ORCID 0000-0001-8238-1289, ORCID 0000-0001-9730-6249, ORCID 0009-0008-2422-155X, ORCID 0009-0000-6039-7503, ORCID 0000-0002-8709-6951

Abstract. The modern global economy has become so interconnected and digitalized that cybersecurity is now a key condition for a company's survival. Information security is no longer an exclusive IT task but a key part of competitiveness. This encourages businesses to actively use AI-based applications as a strategic asset. AI automates repetitive tasks while enabling security systems to learn, predict threats before they occur, and respond without the intervention of qualified IT specialists. This article conducted a systematic review of investments in artificial intelligence for cybersecurity, focusing on comparing costs with expected benefits, changes after automation, and long-term financial and reputational impact. The review shows that AI and machine learning can reduce response time to cyberattacks, decrease false alarms, and lower operating costs. Therefore, integrating AI into cybersecurity is not only a security upgrade but also an economic necessity, increasing reliability, user trust, and long-term business sustainability.

Keywords: cybersecurity; digital economy; digital transformation; economic efficiency; economics of cybersecurity; risk management.

Introduction

The digitalization of the global economy and the increasing scale and complexity of cyber threats require a shift in the focus of modern information security (Liubarets et al., 2024). Private businesses and governments are constantly faced with threats that require carefully balanced defense strategies to effectively respond to. Morgan (2020) estimates that global

losses from cybercrime could reach $10.5 trillion annually by 2025, making cyberattacks one of the biggest economic threats of the decade. The percentage increase in cyberattacks in Australia alone in 2024 was 73% compared to the previous year, 2023. These figures demonstrate the growing financial impact of cybercrime and the urgent need for organizations to enhance their cyber defenses (Zandi et al., 2024; Kryvovyazyuk et al., 2025).

Cyber threats have thus become a top concern for organizations and governments worldwide, as the frequency, complexity, and impact of cyberattacks continue to increase (Yamin et al., 2021). In recent years, the evolution of cyber threats has exposed vulnerabilities across sectors, resulting in significant financial, operational, and reputational damage. The growing reliance on digital infrastructure has increased the potential for cyberattacks to disrupt critical services and business operations, underscoring the urgent need for robust cybersecurity measures (Turk et al., 2022).

A striking example of the danger of cyberattacks is the NotPetya attack of 2017, which was primarily directed against Ukraine. NotPetya quickly spread around the world, affecting numerous international companies. For example, in Europe, the Danish shipping giant Maersk was affected by it, suffering losses of approximately $300 million due to operational disruptions and the need to restore its IT systems. The German-based pharmaceutical company Merck also suffered significant losses during the cyberattack. Its financial losses are estimated at approximately $870 million (Ren et al., 2020; Dwyer, 2021).

All this emphasizes the transnational nature of cyberthreats and confirms that they are capable of causing significant economic damage even to large international corporations. Given this, the financial and operational consequences of the aforementioned cyberattack underscore the critical need for improved cybersecurity strategies and cooperation between international institutions to effectively confront current cyber threats (Valkenburg and Bongiovanni, 2024). At the same time, traditional cybersecurity tools can no longer provide the necessary flexibility and resilience, as their use is dependent on people and requires a lot of time and resources. Therefore, the integration of artificial intelligence (AI) algorithms is now seen as an economic imperative (Buczak and Guven, 2015).

The use of AI in the processes of detecting, predicting, and countering cyber threats is already showing its value. Thus, special machine and deep learning systems can autonomously detect anomalies in network traffic, predict attack vectors and reduce the impact of human errors, which, according to IBM Security (2025), account for over 95% of all cybersecurity incidents. This helps reduce employee costs, increase the efficiency of processing large volumes of data, reduce financial losses from downtime or data leaks and generally increase the productivity of security operations centers (SOCs).

However, the implementation of AI in cybersecurity is a complex process with difficulties. The most significant of them are high initial investment requirements, the need for specialized infrastructure, lack of qualified personnel, and limited empirical data to demonstrate economic results. For example, according to Capgemini Research Institute (2019), although 61% of organizations recognize AI as a critical tool for increasing their cyber resilience, only 23% of them actually use it in their activities. This discrepancy highlights the combination of economic, organizational, and institutional barriers that slow down the implementation of AI in private business activities. This slowdown occurs even though the global trend shows an increase in the integration of AI technologies into economic activities.

At the international level, efforts to support and regulate AI in information security are constantly increasing. The European Commission presented the EU Law on AI, which regulates the use of AI in critical sectors, including cybersecurity (European Commission, 2021). A preliminary review of the scientific literature shows that most studies on the use of AI in cybersecurity focus exclusively on technological issues, while the economic dimension of this process remains understudied (Govea et al., 2024). Therefore, a gap in existing research is the lack of a comprehensive assessment of the economic feasibility of implementing AI-based information security systems in resource-constrained environments and developing countries. The relevance of the article is determined by the need to respond to cyber threats using separate applications and automated systems built on the basis of the use of new technologies based on AI algorithms.

It should be noted that the main gaps in previous research related to the issue of cost-effectiveness of integrating AI into cybersecurity systems are the dominance of exclusively quantitative methods and ignoring PRISMA. Also among the critical gaps can be mentioned the formation of conclusions based on insufficient data and the obsolescence of the theoretical basis of many studies. This leads to a gap between the theoretical and practical components of the aforementioned studies. The purpose of this study was to conduct a systematic review of the impact of the implementation of AI on the cost-effectiveness of the information security system and identify the economic benefits derived from the development, implementation, and support of solutions based on AI. The novelty of the study lies in the actualization of the issues of economic benefits from the development, implementation and support of solutions based on AI in the economic activities of companies.

Materials and methods

A systematic literature review was conducted in accordance with this PRISMA 2020 recommendation (Page et al., 2021). The review was guided by the following research questions: Question (Q1): How does the implementation of AI affect the cost-effectiveness of the information security system? Question (Q2): Do the economic benefits generated by AI-based solutions justify the initial investment in their development, implementation, and support?

The formulation of the above research questions allows author to focus the research on assessing the economic potential of AI in information security and on developing practical recommendations for businesses and policymakers in the broader digital transformation landscape. The strategy for searching for relevant scientific articles was based on the use of specific terms related to the economic potential of AI and economic benefits (Table 1).

Table 1. Specific terms and concepts used in the search

Concepts (C)	C1: Economic potential of AI	C2: Economic benefits
Terms	productivity growth, cost reduction, Return on Investment (ROI), scalability	cost efficiency, payback period, investment justification, operational efficiency

Data for this review were collected in several stages, during the first half of 2025. This systematic review was conducted in accordance with the PRISMA 2020 guidelines to ensure transparency and reproducibility of the study selection process (Page et al., 2021). A number of international interdisciplinary and specialized databases with online access were selected to search for relevant literature, such as: ScienceDirect, SAGE Journals, arXiv and OpenAlex. The selection of these databases is based on the fact that some of them provide open access to individual publications, while others provide free subscription access to the author.

The necessary publications were found using the specific terms listed in Table 1. All publications found are logically related to the concepts of "economic potential of AI" and "economic benefits". This approach to selecting search phrases eliminates the need for additional consultations with content specialists and data analysts. The guiding criteria for selecting publications for the literature review process were: articles are full-text; publications are written in English language and published between 2017–2025. Accordingly, the criteria for excluding publications included the factors of lack of access to the full text, language of writing other than English, and publication date before 2017.

The start date for the publication study was 2017, as that was when one of the first peer-reviewed scientific articles appeared that directly analyzed the ROI and delayed economic effect of AI. The argument for the publication study in subsequent years can be traced back to the fact that the same research team, in their subsequent paper in 2021, found that the use of AI initially reduces measured productivity, but only then has a sharp positive effect, forming a J-curve of productivity (Brynjolfsson et al., 2021).

The first stage of selection of publications for the systematic review led to the retrieval of 228 records in the electronic databases ScienceDirect, SAGE Journals, arXiv and OpenAlex. During this stage, 92 duplicate records were identified, which the author manually removed. During the screening stage, all publications were checked for compliance of their titles, abstracts and keywords with the inclusion criteria specified by the author. During the initial screening, 136 publications were identified as relevant for this review, but in addition, 64 publications were found not to meet the inclusion criteria specified by the author.

Also, the author was unable to obtain the full text of 21 articles in open sources, electronic libraries or by contacting their authors. Thus, the stages of identification and screening of publications allowed to obtain 51 publications. In turn, the third stage of selecting publications for the systematic review allowed author to identify 11 articles with incomplete text, 8 articles written in a language other than English, and 12 articles published before 2017. As a result, the data collection carried out by the author resulted in 20 articles (Figure 1).

The VOSviewer was used to analyze the scientific landscape of the study. The keyword co-occurrence analysis was based on author keywords extracted from selected bibliographic records. Another important method of bibliometric analysis is co-authorship analysis, which shows the relationship between authors and the degree of organization of cooperation between them. The quality assessment of the publications included in the review was conducted using an adapted version of the Critical Assessment Skills Program (CASP) checklist (CASP, 2018). The original criteria were modified to reflect the specificities of AI and cybersecurity research, including assessment of data quality, methodological rigor, and model validation.

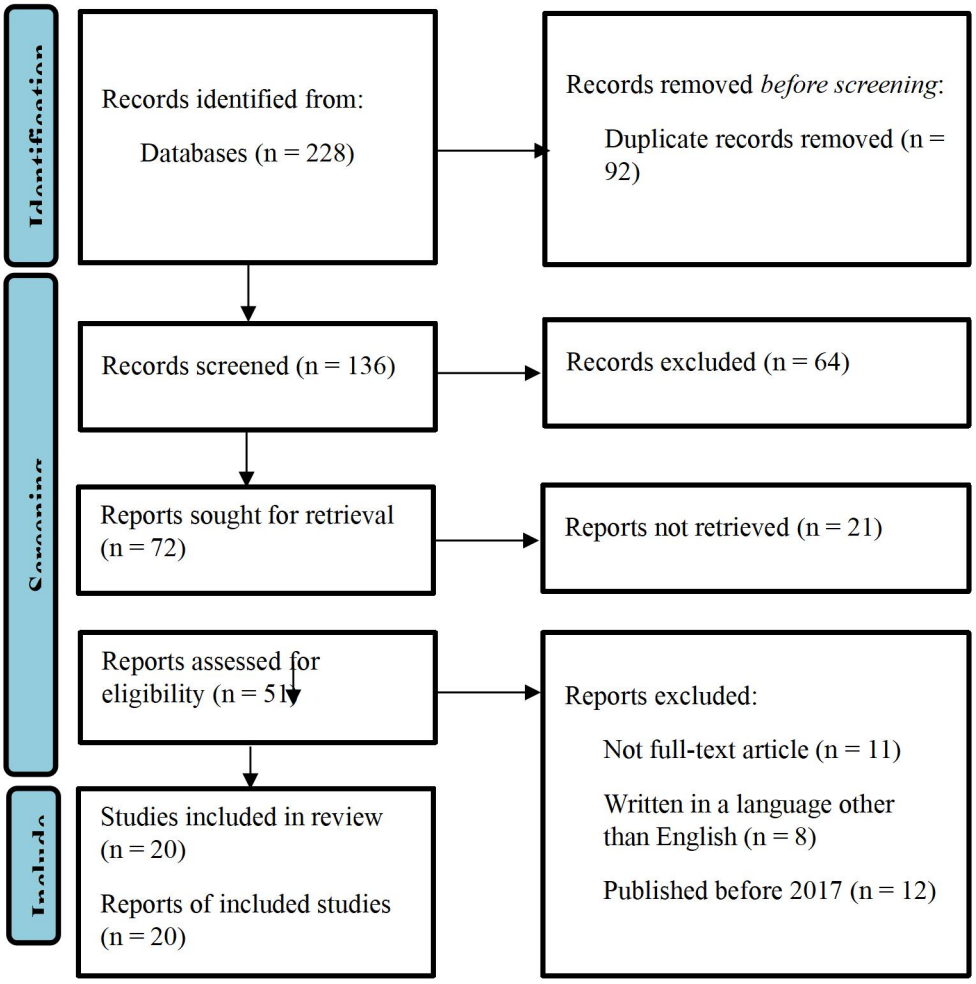

Figure 1. Search strategy flow diagram based on PRISMA 2020 guideline for systematic review

The final interpretation of the selected publications (n = 20) was conducted over a week in the second half of 2025. It was based on the use of a predominantly deductive method: from the general to the specific. This allowed author to verify the compliance of the selected publications with the main criteria of scientificity and to answer the research questions, as shown in the next section.

Results

The bibliometric analysis included keyword co-occurrence and co-authorship analysis. This allowed author to identify the main research areas and scientific clusters in the field of AI applications in information security. Besides co-citation and co-authorship analyses,

the citation analysis has been performed in order to discover the most significant papers among those chosen for the investigation, using VOSviewer. The number of citations was collected and analyzed in order to estimate the significance of each paper in terms of its effect on the research conducted in the area where artificial intelligence, cybersecurity, and economic evaluation intersect. It appears that the distribution of citations is not uniform enough, meaning that some papers have made a greater contribution to the advancement of research in the mentioned area compared to other ones. Papers highly cited often contain key concepts related to AI adoption and its economic effects. However, less cited papers tend to be newer, which is quite expected. The view of the analysis of the co-occurrence of keywords is shown in Figure 2.

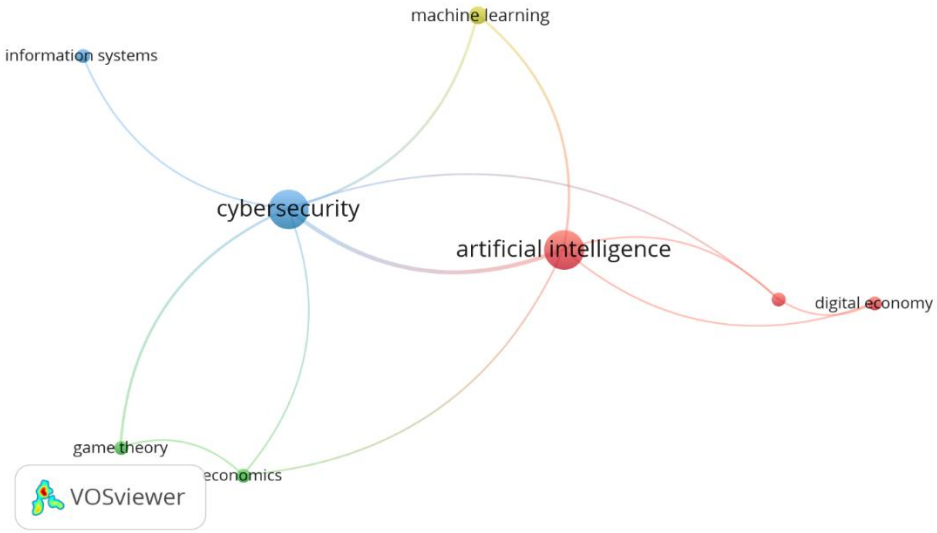

Figure 2. VOSviewer keyword co-occurrence clustering view

A minimum occurrence threshold was applied to filter infrequent terms, ensuring the stability of the network. It should be noted that the area of the node and the font size depend on the weight of the keyword. The larger the weight value, the more times the keyword appears, and the larger the corresponding node and font will be. The line between the nodes indicates that the keyword occurs together with another keyword. The thickness of the connecting line indicates the strength of the co-occurrence between the two keywords. The thickness of the connecting line is proportional to the strength of the co-occurrence, that is, the thicker the connecting line, the more times the two keywords occur together. The results of the keyword co-occurrence analysis revealed relatively weak relationships between individual components of economic assessment and technical cybersecurity mechanisms (Table 2).

Table 2. The results of the keyword co-occurrence analysis

List of keywords	Cluster	Links	Total link strength	Occur-rences	Avg. pub. year
artificial intelligence	1	5	11	11	2023.2727
Cybersecurity	3	6	13	11	2022.6364
digital economy	1	2	2	2	2023
Economics	2	3	3	2	2023
game theory	2	2	3	2	2022.5
information systems	3	1	1	2	2020
machine learning	4	2	4	3	2023.6667
Sustainability	1	3	3	2	2022.5

The results of Table 2 show that the selected publications were classified into four clusters, and the keywords "artificial intelligence" and "cybersecurity" have the greatest number of connections with other elements. They are the most important elements of the network and are found most often in the analyzed publications. In addition, all topics are determined to be new, as the average year of their publication is five years or less.

The next bibliometric analysis method was co-authorship analysis. The view of the co-authorship analysis conducted using VOSviewer are shown in Figure 3.

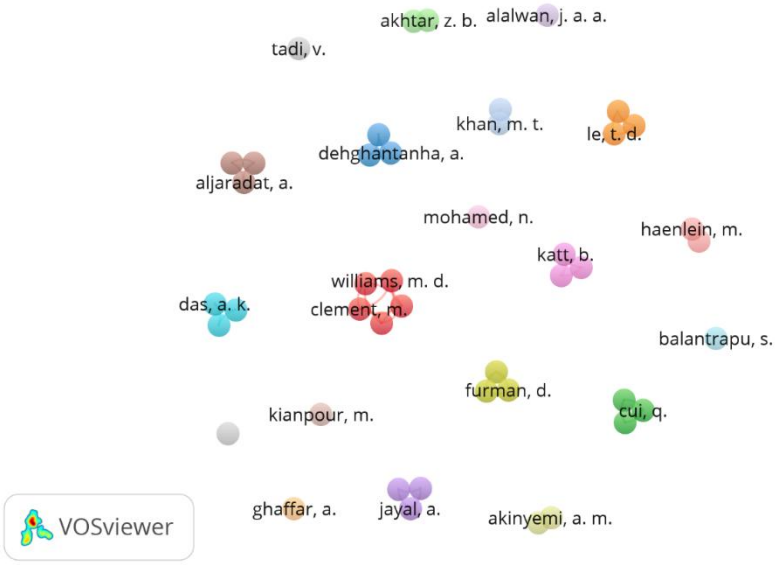

Figure 3. VOSviewer co-authorship clustering view

The results of the co-authorship analysis showed that the authors of 7 publications, which are further considered in the review, are individual researchers. In addition, 4 publications were written by scientific groups of two authors, 8 – by groups of three and one group of five authors (Table 3).

Table 3. The results of the keyword co-authorship analysis

List of authors	Cluster	Links	Documents	Avg. pub. year
akhtar, z. b.	11	1	1	2024
akinyemi, a. m.	13	1	1	2025
alalwan, j. a. a.	14	0	1	2022
aljaradat, a.	8	2	1	2024
balantrapu, s.	15	0	1	2022
clement, m.	1	4	1	2017
cui, q.	2	2	1	2021
das, a. k.	6	2	1	2019
dehghantanha, a.	3	2	1	2023
dwivedi, y. k.	1	4	1	2017
furman, d.	4	2	1	2023
ghaffar, a.	16	0	1	2025
govea, j.	9	2	1	2024
haenlein, m.	10	1	1	2019
hasani, t.	3	2	1	2023
jayal, a.	5	2	1	2021
jeyaraj, a.	1	4	1	2017
kaplan, a.	10	1	1	2019
kayes, a.	9	2	1	2019
khan, m. t.	12	1	1	2024
kianpour, m.	17	0	1	2021
kubitskyi, s.	4	2	1	2023
kumar, n.	6	2	1	2019
le, t. d.	7	2	1	2025
le-dinh, t.	7	2	1	2025
ma, x.	2	2	1	2021
mohamed, n.	18	0	1	2025
o'reilly, n.	3	2	1	2023

prakash, e.	5	2	1	2021
rana, n. p.	1	4	1	2017
rawindaran, n.	5	2	1	2021
rawol, a. t.	11	1	1	2024
sarkar, g.	8	2	1	2024
shchokin, r.	4	2	1	2023
shoukat, d.	12	1	1	2024
shukla, s. k.	8	2	1	2024
sims, s.	13	1	1	2025
singh, r. p.	19	0	1	2025
srinivas, j.	6	2	1	2019
tadi, v.	20	0	1	2024
uwizeyemungu, s.	7	2	1	2025
watters, p.	9	2	1	2019
williams, m. d.	1	4	1	2017
zhang, s.	2	2	1	2021

The results of Table 3 show that the number of publications of each author selected for this review is the same and equals one. Also, during the analysis, it was found that the maximum number of author connections is four, and the minimum is zero. Twenty groups of authors were identified, which corresponds to the number of publications. The latter means that each publication considered during the review was written by a separate group of authors.

An important part of the systematic review is the CASP checklist. Using this approach to assessing quality and risk of bias made it possible to understand whether the study design was appropriate for its purpose, whether the data set was described, whether the methodology was rigorous, whether the results were validated or verified, and whether the results obtained could be applied without bias (Table 4). The quality and risk of bias rating scale used the values "high", "medium" and "low".

Table 4. The results of CASP checklist using for assessing quality and risk of bias

Study	Design	Data Quality	Methodology	Validity	Bias risk	Overall
Zhang et al. (2021)	Medium	Medium	Medium	Medium	Medium	Medium
Balantrapu (2022)	Medium	Low	Medium	Low	Medium	Medium
Akhtar and Rawol (2024)	High	Medium	High	Medium	Low	High

Akinyemi and Sims (2025)	High	High	High	High	Low	High
Kaplan and Haenlein (2019)	High	Medium	Medium	Medium	Low	Medium
Alalwan (2022)	Medium	Medium	Medium	Medium	Medium	Medium
Hasani et al. (2023)	High	High	High	High	Low	High
Rawindaran et al. (2021)	High	Medium	High	Medium	Low	High
Shoukat et al. (2024)	Medium	Medium	Medium	Medium	Medium	Medium
Mohamed (2025)	High	High	High	High	Low	High
Singh (2025)	Medium	Low	Medium	Low	Medium	Medium
Srinivas et al. (2019)	High	High	High	High	Low	High
Govea et al. (2024)	High	High	High	Medium	Low	High
Ghaffar (2025)	Low	Medium	Medium	Low	High	Low
Le et al. (2025)	High	High	High	High	Low	High
Sarika et al. (2023)	Medium	Medium	Medium	Medium	Medium	Medium
Dwivedi et al. (2017)	High	High	High	High	Low	High
Kianpour (2021)	High	High	High	Medium	Low	High
Aljaradat et al. (2024)	High	High	High	Medium	Low	High
Furman et al. (2023)	Medium	Low	Medium	Low	Medium	Medium

Analysis of Table 4 shows that the majority of the assessed publications demonstrate medium or high quality. Thus, the quality assessment of the selected publications found that 50% of them demonstrate high overall quality, 45% are classified as medium and only 5% as low. In addition, 50% of the publications demonstrate low risk of bias, 45% moderate risk and 5% high. The methodological rigor of 55% of the publications is also high. However, the quality of the data remains variable, as only 30% of the publications are based on high-quality data, while 50% rely on moderately reliable data sets and 20% rely on limited data sources.

Those of these publications that were found to be of high quality tend to be empirical or analytical works with a strong methodological foundation and verified results.

At the same time, medium-quality publications often lack comprehensive data sets or empirical validation, while conceptual studies tend to exhibit a higher risk of bias.

The study shows that integrating AI into information security systems brings clear and measurable economic benefits. This effect is noticeable both in the reduction of direct costs associated with incident response and in the reduction of indirect losses, such as reputational damage, regulatory fines, or customer churn. Globally, organizations that rely on machine learning to monitor network activity and detect intrusions report a 70-80% faster incident detection rate compared to traditional security tools, and this improvement directly translates into reduced financial losses. With the average cost of a data breach reaching $4.35 million, response time becomes a critical factor in containing losses.

Companies that use AI-based automated security systems report incident costs that are approximately $1.5 million lower than those that rely solely on manual operations (IBM Security, 2025). This finding supports the assumption that automation significantly increases the cost-effectiveness of cybersecurity efforts, and that AI is superior to manual methods in detecting and responding to threats (Zhang et al., 2021). According to Capgemini Research Institute (2019), 69% of organizations admit that they cannot adequately counter advanced cyberattacks without AI. In several European countries, notably Germany and France, the number of critical incidents decreased by almost 50% after implementing AI-based predictive analytics, while security operations center (SOC) operating costs fell by 20-25% (European Commission, 2021).

It is also worth noting that cost-effectiveness includes not only measurable financial benefits, but also intangible benefits: higher user trust in digital services, stricter compliance with regulatory requirements such as GDPR, and the ability to scale operations without a proportional increase in security budgets. Morgan (2020) predicts that global losses from cybercrime will reach US$10.5 trillion annually by 2025, and even a small reduction achieved through the integration of AI will have a significant macroeconomic impact. The best results are achieved by organizations that use comprehensive AI solutions that combine machine learning with behavioral analytics. For example, banks in the UK that implemented AI-based fraud detection methods reduced the number of successful fraud cases by 42% in the first year. In Scandinavian countries, the widespread implementation of AI to ensure the security of financial transactions led to a 30% reduction in customer compensation costs, a strong indicator of cost-effectiveness (OECD, 2022).

The implementation of AI also helps minimize the financial burden associated with the costs of maintaining the equipment and infrastructure necessary to protect the organization. This is achieved by intelligently notifying organizations of scheduled maintenance or predicting potential failures of certain hardware components, allowing for proactive replacement before a complete failure occurs. Ultimately, the integration of AI technologies with equipment and infrastructure maintenance can provide financial savings for organizations and reduce the overall energy consumption of hardware components (Kaplan and Haenlein, 2019; Mazaraki et al., 2021).

However, the adoption of AI for cybersecurity in small and medium-sized enterprises is hampered by cost factors, while their vulnerability to cyberattacks increases due to limited expertise and funding (Rawindaran et al, 2021). Using AI in corporate cybersecurity provides them with predictive and proactive security, which in the long term can reduce costs and increase their cost-effectiveness (Le et al., 2025). A study of an AI-based cybersecurity system using Cuda-based deep neural networks demonstrated its high detection accuracy (99,60%), outperforming traditional solutions. Therefore, integrating

AI into cybersecurity systems offers a cost-effective and highly adaptive solution for enterprise-grade network applications (Shoukat et al., 2024).

Another study shows that integrating AI into security systems provides adaptive and automated protection mechanisms that can reduce the burden on human resources (Akhtar and Rawol, 2024). Thus, the freed up human resources can be used more efficiently, which contributes to reducing staffing levels and reducing personnel costs for companies. It should also be noted that the high false positive rate generated by cybersecurity systems that use traditional intrusion detection methods can lead to fatigue among security personnel. When security teams are overwhelmed with false positives, they can become desensitized to warnings, potentially ignoring real threats, which compromise security and contribute to burnout and employee dissatisfaction (Srinivas et al., 2019; Furman et al., 2023).

The latter leads to long-term increased costs and reduced profits due to the need to constantly replace and train new security personnel. Therefore, the transformative impact of AI on cybersecurity is that AI technologies help to overcome the limitations of traditional security measures. Existing research confirms that AI-based solutions have already outperformed traditional methods in various real-world scenarios of countering cyber threats (Balantrapu, 2022). Also, an analysis of the experience of real-world implementation of AI in security systems shows that AI-based security systems demonstrate impressive prospects in reducing costs and increasing operational efficiency of companies. For example, Amazon's AWS DeepLens uses AI and computer vision to improve the security and protection of its warehouses. In these conditions, the created security system optimizes cyber security processes and protects companies from theft through constant monitoring and detection of anomalies in security (Sarika et al., 2023).

Thus, the considered example of AWS DeepLens from Amazon demonstrates that in order to reduce costs and increase the operational efficiency of companies, it is possible to integrate not only AI into the security system, but also to supplement it with the use of other digital technologies (computer vision). Unfortunately, the aforementioned study does not provide practical data on the effectiveness of such a dual integration of digital technologies into the security system of companies. The cost-effectiveness of AI-based security measures is evident through both immediate and long-term financial benefits. While the initial costs of setting up AI systems can be high, these costs are offset by the reduction in manual labor, minimizing human error, and the ability to scale effectively.

Long-term savings come from reduced operational costs, fewer security incidents, and reduced downtime (Tadi, 2024). Another important area of cybersecurity is AI-based predictive analytics. Its use resulted in an estimated 76% reduction in incident costs in the same year, and the organization participating in the project earned 4.3 times its cost in one year (Akinyemi and Sims, 2025). While the public sector’s performance is generally lower, AI implementation still yields positive results, reducing risks to critical infrastructure that has significant societal value. However, not all researchers are unanimous on this issue, for example, Alalwan (2022) believes that one of the main problems faced by AI-based cybersecurity is additional financial costs.

AI-based cybersecurity systems require significant computing resources and data availability to function effectively in real-world environments. Smaller enterprises do not have the infrastructure to deploy these systems on a large scale (Mohamed, 2025). Thus, integrating AI into small enterprise security systems and their subsequent support is often impossible for economic and technical reasons, or even undesirable due to the economic inexpediency of this process. This negatively affects the scalability of AI-based

cybersecurity systems. The process of obtaining economic benefits from the integration of AI is complicated by the fact that it depends not only on technological readiness, but also on investment opportunities, the availability of qualified personnel and regulatory conditions (Hasani et al., 2023). Also, investments in AI often require significant upfront costs, including technology acquisition, infrastructure upgrades, and staffing. As a result, many companies face a delayed return on investment, with benefits taking months or even years to materialize (Ghaffar, 2025).

The study by Dwivedi et al. (2017) confirmed the relevance of classic innovation adoption models – TAM (Technology Acceptance Model) and UTAUT (Unified Theory of Technology Adoption and Use) – for interpreting behavioral aspects of technology adoption. At the same time, scholars such as Aljaradat et al. (2024) have advocated expanding this framework to include economic and organizational variables. As a result, literature increasingly relies on hybrid theoretical models, where behavioral, financial, and technological factors are considered together rather than separately. This evolution is further reflected in studies that apply the TOE (Technological-Organizational-Environmental) framework to information security. Kianpour (2021) have proposed integrating technological elements (infrastructure, automation, analytics), organizational factors (resources, personnel, managerial support), and external influences (regulation, market environment) to develop a more holistic understanding of digital security. Further empirical research (Hasani et al., 2023; Singh, 2025) has shown that organizations with higher security process maturity and stable investment flows tend to reap much greater economic benefits from AI than those operating with limited resources.

In the context of developing countries, researchers such as Govea et al. (2024) emphasize the need to develop economic models of AI implementation that reflect resource constraints, market characteristics, and the role of government support. These studies highlight that without public-private partnerships and external financing instruments; AI technologies remain out of reach for many organizations working in the security sector. The results also show that the success of AI implementation depends not only on the technological maturity of the organization, but also on how well-structured investment and management decisions are.

The analysis showed that companies that integrate cost-benefit analysis into their AI strategies achieve, on average, 25-30% higher resource efficiency and 20% faster incident response. Behavioral factors described by the TAM and UTAUT models strongly influence user acceptance of AI tools, while organizational and institutional elements of the TOE framework help maintain long-term system stability. Together, these factors form the basis for developing a comprehensive methodology for assessing the cost-effectiveness of AI investments in the face of market and regulatory constraints. The conducted systematic literature review allowed author to create a comparative table of the approaches of the authors of the analyzed scientific papers to the integration of AI into information security systems (Table 5).

Table 5. Comparison of approaches to integrating AI into information security systems

The essence of the approach	List of authors	Number of articles	General assessment of the integration of artificial intelligence into information security systems
Based on a comparison with manual or traditional methods	(Zhang et al., 2021; Balantrapu, 2022; Akhtar and Rawol, 2024; Akinyemi and Sims, 2025)	4	Compared to traditional cybersecurity methods, AI-based information security systems reduce the need for human resources, reduce the costs of cyberattacks, and increase the cost-effectiveness of cybersecurity measures
Based on equipment and infrastructure maintenance costs	(Kaplan and Haenlein, 2019; Alalwan, 2022; Hasani et al., 2023)	3	Although integrating AI technologies into security systems can reduce overall energy consumption by hardware components, it requires additional costs for equipment and infrastructure maintenance, which exacerbates the issues of investment affordability, availability of qualified personnel, and regulatory conditions
Based on the scale of the enterprise or company	(Rawindaran et al., 2021; Shoukat et al., 2024; Mohamed, 2025; Singh, 2025)	4	Integrating AI technologies into security systems is always beneficial for large companies and corporations, but in small and medium-sized enterprises this process is often hampered by cost factors
Based on long-term prospects	(Srinivas et al., 2019; Ghaffar, 2025; Le et al., 2025)	5	The long-term savings from integrating AI into security are reduced operating costs, fewer incidents, and reduced downtime, but many companies face a delayed return on investment, with the benefits of such modernization being realized over months or even years
Based on integration with other digital technologies	(Sarika et al., 2023)	1	A security system created by combining AI and other digital technologies optimizes cybersecurity processes and protects companies from theft
Based on the implementation model	(Dwivedi et al., 2017; Kianpour, 2021; Aljaradat et al., 2024)	3	Although classical models of innovation implementation still remain relevant, their framework needs to be expanded to include economic and organizational variables, adjusting for external influences

In conclusion, the study confirms that the implementation of artificial intelligence in cybersecurity has proven to be economically justified across industries and regions. From direct financial benefits to long-term strategic advantages, AI technologies generate a multiplier effect, enhanced by scalability and sustainable performance. Given the rapidly increasing cost of cybercrime, the failure to integrate artificial intelligence into cybersecurity strategies poses significant financial risks for both private companies and government agencies. It is precisely because of the rapid growth of financial risks from cyberattacks that companies with limited resources need to join forces to develop and support AI-based information security systems, using hybrid AI implementation models that immediately calculate the economic factors of this process.

This will allow not only to obtain a holistic understanding of digital security for employees of such enterprises, but also to pre-calculate the amount of investment required to develop and support AI-based information security systems. Given the numerous small business development programs that are typical for many regions and developing countries, a promising direction for the development and support of AI-based information security systems may be the involvement of state institutions in financing and regulating their unification and distribution among national companies with limited resources.

During this process, the development of AI-based information security systems can take place on the basis of state higher education institutions, using the skills and abilities of young specialists in the field of information technology and entrepreneurship economics. This will not only contribute to the growth of the geo-economic power of states with a developed education system, but will also provide a unique experience for graduates of their higher education institutions, allowing for the scaling up of the integration of AI-based information security systems into all spheres of life.

Discussion

The results of the study show that the cost-effectiveness of implementing AI in information security cannot be reduced to a single indicator. Instead, it is a complex, multidimensional phenomenon shaped by technological, organizational, and economic factors. First, the results of the review demonstrate that AI generates tangible economic benefits. This is reflected in faster detection and response to security incidents, lower costs of mitigating cyberattack, and more efficient allocation of organizational resources. These observations support previous findings by Eling and Schnell (2016) and Fotis (2024), who showed that even small improvements in threat detection can lead to significant financial benefits. The results also correlate with the theoretical principles of the TOE (Technology-Organization-Environment) and UTAUT (Unified Theory of Technology Implementation and Use) models, which are commonly used to explain how organizations adopt new technologies (Kianpour, 2021; Aljaradat et al., 2024).

Like these studies, this review confirms that the cost-effectiveness of AI implementation directly depends on organizational readiness, financial capacity, and managerial support. These findings suggest that existing behavioral models should be expanded to include economic variables that shape the real financial outcomes of implementing advanced security technologies. It should also be noted that AI models require modern central processors, which leads to increased costs for their implementation (Wilkins, 2018). At the same time, the review's findings challenge the common belief that

AI is universally profitable. As Rawindaran et al. (2021) point out, SMEs often face delayed or reduced profitability due to high initial investments, limited internal resources, and a lack of skilled personnel. The results of this study confirm this asymmetry: economic efficiency varies significantly depending on the size and resource base of the organization. This nuance extends traditional approaches to the economics of cybersecurity, emphasizing that the economic returns from AI-based security solutions are highly context-dependent.

From the perspective of technology adoption theories (Dwivedi et al., 2017), the study also deepens the understanding of how organizations perceive and implement intelligent systems. The results show that perceived usefulness and perceived risk have not only psychological but also economic dimensions. Higher trust in AI correlates with improved investment attractiveness and reduced operational costs, indicating that organizational attitudes directly impact financial performance. Overall, the results of the review support the findings of recent studies (Eling and Schnell, 2016; Hasani et al., 2023; Singh, 2025) on the significant economic impact of implementing AI in cybersecurity. The results also challenge the belief that AI provides equal benefits to all organizations, showing that economic outcomes depend largely on available resources.

Conclusion

The study shows that integrating AI into information security systems is much more than just a technical upgrade. It has become a significant economic driver of the digital economy and a practical necessity to maintain the resilience of modern information infrastructures. The study results demonstrate that intelligent threat analysis systems can reduce the financial impact of cyberattacks and the costs of resolving security incidents and strengthen the trust of users and business partners in digital services. One of the central findings is that there is a sustainable ROI associated with AI-based cybersecurity solutions. Across industries, the economic benefits are manifested both in the direct reduction in the average cost of cyber incidents and in long-term strategic advantages. Organizations that implement AI are better able to remain competitive, avoid fines and reputational damage, and thrive in an increasingly volatile digital environment.

Another important finding is the observation that the strongest economic impact of AI is observed in sectors that deal with large amounts of dynamic data. In these industries, AI allows for the rapid detection of sophisticated attacks and the timely adaptation of defenses. However, the study notes that the implementation of AI technologies often requires significant upfront investments, which can limit the ability of small and medium-sized enterprises to implement them. This highlights the importance of flexible AI implementation models, such as hybrid ones, which can make access to advanced technologies more financially feasible and inclusive. The practical conclusion of the study is that cybersecurity spending should not be viewed as an operational expense, but as an investment that can generate economic returns. This reframes the approach of decision-makers to cybersecurity: from a cost-driven necessity to a strategic area of development that improves risk management effectiveness and supports long-term economic growth. The practical value of the study is that it offers a basis for developing investment strategies in the field of cybersecurity.

Further research should clarify how AI affects the broader economic environment – its role in strengthening macroeconomic stability, shaping national investment

attractiveness, and increasing the resilience of international digital markets. It is also important to identify how AI interacts with other emerging technologies, as combined solutions can significantly improve the effectiveness of information protection systems.

References

Akhtar, Z. B., Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. *IT Journal Research and Development*, *9*(1), 50–67. https://doi.org/10.25299/itjrd.2024.16852

Akinyemi, A. M., Sims, S. (2025). AI-enhanced predictive analytics for identifying and mitigating critical cybersecurity vulnerabilities. *World Journal of Advanced Research and Reviews, 26*(2), 1585–1606. https://doi.org/10.30574/wjarr.2025.26.2.1654

Alalwan, J. A. A. (2022). Roles and challenges of AI-based cybersecurity: A case study. *Jordan Journal of Business Administration*, *18*(3), 437–456. https://doi.org/10.35516/jjba.v18i3.196

Aljaradat, A., Sarkar, G., Shukla, S. K. (2024). Modelling cybersecurity impacts on digital payment adoption: a game theoretic approach. *Journal of Economic Criminology*, *5*, 100089. https://doi.org/10.1016/j.jeconc.2024.100089

Balantrapu, S. (2022). Evaluating AI-enhanced cybersecurity solutions versus traditional methods: A comparative study. *International Journal of Sustainable Development Through AI, ML and IoT*, *1*(1), 1–15.

Brynjolfsson, E., Rock, D., Syverson, C. (2021). The productivity J-curve: How intangibles complement general purpose technologies. *American Economic Journal: Macroeconomics*, *13*(1), 333–372. https://doi.org/10.1257/mac.20180386

Buczak, A. L., Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Capgemini Research Institute. (2019). Reinventing cybersecurity with artificial intelligence: The new frontier in digital security. Retrieved from https://www.capgemini.com/gb-en/wp-content/uploads/sites/5/2022/05/AI-in-Cybersecurity_Report_20190710_V05.pdf

CASP. (2018). CASP checklist. Retrieved from https://casp-uk.net/casp-tools-checklists/

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., Williams, M. D. (2017). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers*, *21*(3), 719–734. https://doi.org/10.1007/s10796-017-9774-y

Dwyer, A. C. (2021). Cybersecurity's grammars: A more-than-human geopolitics of computation. *Area, 55*(1), 10–17. https://doi.org/10.1111/area.12728

Eling, M., Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

European Commission (2021). Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

Fotis, F. (2024). Economic impact of cyber attacks and effective cyber risk management strategies: A light literature review and case study analysis. *Procedia Computer Science*, *251*, 471–478. https://doi.org/10.1016/j.procs.2024.11.135

Furman, D., Shchokin, R., Kubitskyi, S., Chaplinskyi, V., Strochenko, N., Dorosh, I. (2023). Motivation and incentives for employees of domestic enterprises. *Journal of Law and Sustainable Development, 11*(3), e0815. https://doi.org/10.55908/sdgs.v11i3.815

Ghaffar, A. (2025). The ROI of AI: Why companies invest billions in artificial intelligence. *Iconic Research and Engineering Journals, 9*(4), 1361–1365.

Govea, J., Gaibor-Naranjo, W., Villegas-Ch, W. (2024). Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems*, *12*(5), 165. https://doi.org/10.3390/systems12050165

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5), 1–38. https://doi.org/10.1007/s43546-023-00477-6

IBM Security. (2025). Cost of a data breach report 2025. Retrieved from https://www.ibm.com/security/data-breach

Kaplan, A., Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Kianpour, M. (2021). Heterogeneous preferences and patterns of contribution in cybersecurity as a public good. In *Proceedings of the 13th International Conference on Agents and Artificial Intelligence*, 414–421. https://doi.org/10.5220/0010336204140421

Kryvovyazyuk, I., Britchenko, I., Lipych, L., Kravchuk, P., Galaziuk, N., Burban, O. (2025). Impact of global risks on economic downturn in countries worldwide: Analysis of the causes of the situation and opportunities for growth recovery. *Economic Studies (Ikonomicheski Izsledvania), 34*(6), pp. 66-86.

Le, T. D., Le-Dinh, T., Uwizeyemungu, S. (2025). Cybersecurity analytics for the enterprise environment: A systematic literature review. *Electronics, 14*(11), 2252. https://doi.org/10.3390/electronics14112252

Liubarets, V., Kashyna, G., Kachan, Y., Brezetskyi, S., Ostrovershenko, A. (2024). Adapting professional development to the digital transformation of today's job market. *Multidisciplinary Science Journal, 6*, 2024ss0713. https://doi.org/10.31893/multiscience.2024ss0713

Mazaraki, A., Melnyk, T., Melnychenko, S., Kudyrko, L., Lositska, T., Pugachevska, K. (2021). *Import substitution potential in the conditions of digital transformation.* Kharkiv: Pc Technology Center.

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, *67*, 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

Morgan, S. (2020). Special report: Cyberwarfare in the C-suite. Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

OECD (2022). *The economic impact of artificial intelligence in cybersecurity: Policy perspectives.* Paris: OECD Publishing.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Rawindaran, N., Jayal, A., Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers, 10*(11), 150. https://doi.org/10.3390/computers10110150

Ren, A. L. Y., Liang, C. T., Hyug, I. J., Brohi, S. N., Jhanjhi, N. Z. (2020). A three-level ransomware detection and prevention mechanism. *EAI Endorsed Transactions on Energy Web, 7(*26), 1–7. https://doi.org/10.4108/eai.13-7-2018.162691

Sarika, D. M. N., Jain, A., Bajeja, N., Rawat, P., Joseph, C. (2023). Use of enhanced artificial intelligence in security business management in the digital economy era. *Journal of Informatics Education and Research, 3*(2), 1484–1494.

Shoukat, D., Khan, M. T., Sajjad, S. M., Akhunzada, A. (2024). Smart and sustainable threat intelligence. In *Innovation and Technological Advances for Sustainability* (pp. 268–278). CRC Press. https://doi.org/10.1201/9781003496724-26

Singh, R. P. (2025). Emerging impacts of AI on Black entrepreneurship: A conceptual discussion. *Journal of the International Council for Small Business*, 1–16. https://doi.org/10.1080/26437015.2025.2549445

Srinivas, J., Das, A. K., Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Tadi, V. (2024). Quantitative Analysis of AI-driven security measures: Evaluating effectiveness, cost-efficiency, and user satisfaction across diverse sectors. *Journal of Scientific and Engineering Research*, *11*(4), 328–343. https://doi.org/10.5281/zenodo.13347873

Turk, Ž., Sonkor, M. S., Klinc, R. (2022). Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework. *Journal of Civil Engineering and Management, 28*(5), 349–364. https://doi.org/10.3846/jcem.2022.16682

Valkenburg, B., Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. *Computers & Security*, *139,* 103708. https://doi.org/10.1016/j.cose.2024.103708

Wilkins, J. (2018). Is artificial intelligence a help or hindrance? *Network Security*, (5), 18–19. https://doi.org/10.1016/S1353-4858(18)30046-1

Yamin, M. M., Ullah, M., Ullah, H., Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, *57*, 102722. https://doi.org/10.1016/j.jisa.2020.102722

Zandi, G., Yaacob, N. A., Tajuddin, M., Nik Abdul Rahman, N. K. (2024). Artificial intelligence and the evolving cybercrime paradigm: current threats to businesses. *Journal of Information Technology Management*, *16*(4), 162–170. https://doi.org/10.22059/jitm.2024.99505

Zhang, S., Ma, X., Cui, Q. (2021). Assessing the impact of the digital economy on green total factor energy efficiency in the post-COVID-19 era. *Frontiers in Energy Research*, *9*, 798922. https://doi.org/10.3389/fenrg.2021.798922

Received March 13, 2026, revised September 24, 2026, accepted September 24, 2026