DOI: https://doi.org/10.30525/2256-0742/2025-11-3-330-338

DEVELOPMENT OF CYBERSECURITY OF CRITICAL INFRASTRUCTURE IN THE CONDITIONS OF DIGITALIZATION: ECONOMIC TOOLS FOR RISKS AND INVESTMENTS ASSESSMENT

Viktoriia Chorna[1], Bohdana Bohdan[2], Oleksandr Gaponov[3]

Abstract. The article defines that cybersecurity of critical infrastructure in the context of digitalization is a set of measures, technologies and processes aimed at protecting systems, services and data that ensure the functioning of critical infrastructure facilities (energy, transport, water supply, telecommunications, etc.), in the context of their transition to digital platforms. Digitalization is understood as the gradual introduction of information and communication technologies (ICT), automated control systems (SCADA), IoT devices and cloud solutions to increase the efficiency, efficiency and scalability of management. At the same time, this transition opens up new vulnerabilities: each element of the network, from the controller of pumping stations to the sensor of a "smart" meter, becomes a potential access point for cybercriminals. Therefore, cybersecurity in this context encompasses both the protection of physical components (PLC controllers, servers, routers) and software (operating systems, SCADA applications), network protocols and data circulating within and between these systems. Taken together, technical and economic challenges form a complex context for ensuring cybersecurity of critical infrastructure during digitalization. They can only be solved through a multidisciplinary approach that combines state regulation (equipment and process certification requirements), the involvement of international standards (ISO/IEC 27001, IEC 62443), the stimulation of private investment (through partnerships with state infrastructure access fees) and the development of our own human capital through specialized educational programs and pilot routes for the integration of engineers. The *subject* of the article is the disclosure of economic tools for assessing risks and investments in the development of cybersecurity of critical infrastructure, which is caused by digitalization processes. *Research methods.* When studying economic tools for assessing risks and investments in the development of cybersecurity of critical infrastructure, which is caused by digitalization processes, classical research methods were used (dialectical materialism, abstraction, analysis and synthesis, functional, systems analysis, synergistic, comparative law, interpretation and hermeneutics, dogmatic and statistical methods). The *purpose* of the article is the disclosure of economic tools for assessing risks and investments in the development of cybersecurity of critical infrastructure, which is caused by digitalization processes. *Conclusions.* The development of cybersecurity of critical infrastructure in conditions of active digitalization requires the comprehensive application of economic tools for assessing risks and planning investments. The use of quantitative risk analysis methods, cost-benefit analysis estimates, and scenario modeling allows critical infrastructure entities to justify the amount of resources needed to implement protective technologies. Regression and economic-mathematical models allow you to project the scale of cyber threats and predict potential financial losses from incidents, while allowing you to compare the effectiveness of alternative options for measures - from upgrading legacy PLC controllers to implementing SIEM/IDS systems. Thanks to a multi-criteria approach and analysis of real options, business leaders can allocate the budget in such a way as to ensure the optimal balance between preventive investments in security and current operating costs, minimizing both direct and indirect losses from failures and reputational risks. At the same time, the success of a critical infrastructure cyber protection strategy largely depends on effective government

[1] Kyiv National Economic University named after Vadym Hetman, Ukraine *(corresponding author)*
E-mail: demidenkov@ukr.net
ORCID: https://orcid.org/0000-0002-6072-0283
[2] Kyiv National Economic University named after Vadim Hetman, Ukraine
E-mail: bvbogdan@ukr.net
ORCID: https://orcid.org/0000-0002-0422-7021
[3] Kyiv National Economic University named after Vadim Hetman, Ukraine
E-mail: alex@ecg.ua
ORCID: https://orcid.org/0000-0002-7778-673X

regulation and international harmonization of standards. In particular, the implementation of the NIS 2 Directive and approximation to the provisions of the EU DORA stimulate the development of unified audit, monitoring and operational response procedures. Tax incentives, grant mechanisms for co-financing and cyber risk insurance can become an additional tool for economic incentives for CI operators to modernize their digital systems. The development of human capital is also of key importance: investments in the training of cybersecurity specialists, the establishment of cooperation between universities, industrial enterprises and international organizations will ensure the sustainability and adaptability of protective measures. As a result, such a synergy of economic instruments, the legal environment and human resources support will allow achieving a high level of resilience of critical infrastructure to cyber threats and ensuring the uninterrupted functioning of key industries in the face of any challenges of the digital world.

Keywords: state, state functions, administrative and legal regulation, digitalization, digital technologies, state policy, legal regulation, cybersecurity, cyberspace, recovery platform, critical infrastructure, transport infrastructure, information technologies, digitalization.

JEL Classification: H11, H30, H61, I38, R50, D72

Introduction

In today's conditions of accelerated digitalization of critical facilities (energy networks, transport, telecommunications, water supply, etc.), vulnerability to cyber threats is increasing, which can lead to large-scale economic losses, disruptions in the operation of vital systems, and increased social tension. At the same time, the limited state and private resources require a reasonable allocation of investments in cyber protection measures, taking into account real risks. Therefore, the development and implementation of economic instruments that allow for quantitative assessment of the probability and consequences of cyber attacks, as well as justify the feasibility of financing specific security projects, is extremely relevant: it allows not only to reduce the probability of catastrophic incidents, but also to ensure the stability of the infrastructure with optimal use of the budget, which is especially important in conditions of limited funding and growing challenges in the digital space.

1. Research Methodology

1.1. Scientific Analysis of Work on the Topic of the Research

The issue of economic instruments for assessing risks and investments in the development of cybersecurity of critical infrastructure, which is caused by digitalization processes, is the subject of active scientific discussion, especially in view of the challenges associated with the war in Ukraine. In domestic jurisprudence, the direction of research into the transformation of state functions in conditions of a state of emergency, military operations or large-scale social crises is actively developing.

1.2. Methodological Features of the Research

When studying the issue of economic instruments for assessing risks and investments in the development of cybersecurity of critical infrastructure, which is caused by digitalization processes, various methods are used that allow comprehensively taking into account the legal, social, economic and managerial aspects of this area.

In addition to the already mentioned classical research methods, the following methods are also used in the study of economic instruments for assessing risks and investments in developing cybersecurity of critical infrastructure under digitalization conditions. A brief description of their application in the Ukrainian context is given for each:

The expert assessment method (Delphi) involves several rounds of anonymous surveys of a group of experts (cybersecurity analysts, economists, representatives of regulatory authorities), during which experts agree on their assessments of the level of risks, expected losses and necessary investments. Application: allows you to reduce the impact of individual biases, since in subsequent rounds experts adjust the assessments based on aggregated information. As a result, a consensus is formed on the probabilities of various types of cyber incidents and priority areas of investment.

SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) combines an internal assessment of an organization's strengths and weaknesses (e.g., availability of qualified cybersecurity personnel, lack of financial resources) with external opportunities and threats (e.g., the development of artificial intelligence technologies as a protection tool or as a new threat vector). Application: allows you to identify the competitive advantages of critical infrastructure (CI) owners, as well as resource gaps and regulatory challenges that need to be considered when budgeting for cybersecurity.

Cost–Benefit Analysis (cost–benefit analysis) involves quantifying the direct (equipment purchase, payments to IT specialists, licenses for antivirus products) and indirect (possible reputational losses, fines, costs of restoring services after an attack) costs of cyber security measures and comparing them with the expected benefits (impartiality of financial losses, avoidance of fines, stability of operational activities). Application: used to justify the volume of investments in SIEM systems, IDS/IPS, conducting audits and quantifying the probability of preventing incidents. The Scenario Analysis/Risk Simulation method builds several possible scenarios of events (from "baseline" to "catastrophic"), in which the indicators of the probability of cyber threats and their economic consequences change. Application: Using financial models (e.g. Monte Carlo Simulation), the range of expected losses for each scenario is estimated, allowing for the creation of an adaptive cybersecurity budget with a "case buffer" for extreme events.

The Quantitative Risk Analysis method is based on collecting statistical data on the frequency and composition of cyber incidents (DDoS, ransomware, insider threats), determining the probabilities of these events and using mathematical models (often probability distributions) to calculate expected losses. Application: used in combination with SOC (Security Operations Center) data and industry reports (e.g., CERT-UA reports) to build financial forecasts and calculate optimal insurance premiums (cyber insurance). The Multi-Criteria Decision Analysis (MCDA) method allows you to evaluate alternative investment solutions (e.g., deploying your own SOC vs. engaging a Managed Security Service Provider) using several criteria simultaneously: economic (CAPEX, OPEX), technical (response time, threat detection level), legal (GDPR, ISO/IEC 27001 compliance), social (staff trust, public image). Application: Helps critical infrastructure management select projects based on multidimensional needs; within each criterion, ranking methods (Analytic Hierarchy Process, AHP) or weighting coefficients are used.

Econometric Modeling uses panel or cross-sectional data to build regression models that assess the impact of individual variables (the amount of investment in cyber security, the level of personnel qualification, the frequency of software updates) on the financial performance of the enterprise (profitability, reduction of emergency downtime, the scale of losses). Application: Allows you to analyze large data sets from different CI enterprises and identify statistically significant determinants of the success of cybersecurity programs.

System Dynamics Modeling represents an organization or network as a set of interconnected stocks and flows (resources, incidents, costs, personnel training), which helps to study the dynamics of the development of the cybersecurity system over time, taking into account feedback loops. Application: allows you to "roll over" budget planning iterations, see how changing individual parameters (for example, increasing the frequency of employee training) will affect "security" indicators and related costs over several years.

Benchmarking analysis method – within the framework of this method, one's own CI indicators (the amount of investment in cyber security, the number of incidents, the speed of response) are compared with similar metrics of other public or private critical infrastructure operators in similar conditions (energy, gas supply, railway sectors). Application: allows you to identify "worst" and "best" practices, as well as set regulatory goals (for example, to bring the number of incident responses to the industry average), which increases competitiveness.

The case study method (Case Study Analysis) involves a detailed study of successful and unsuccessful examples of cybersecurity investments (for example, an analysis of incidents with a SCADA system hack at an energy company) allows you to learn lessons and form recommendations for similar projects. Application: ready-made cases are used as a learning and decision-making tool in specialized departments: based on specific mistakes or successes, checklists and templates for technical and financial assessment of future projects are formed.

Cohort Analysis examines groups of facilities (e.g., certain UES (united energy systems) or gas transmission network operators) that have implemented cyber security measures over a period of time and compares their economic performance (costs, reduced downtime) with a group that has not changed its security policy. Application: allows you to understand how investments in cybersecurity have affected overall operational efficiency and profitability over several years.

Economic Audit involves a detailed audit of the use of budget funds, grants, and donor contributions aimed at cybersecurity development, with a focus on compliance of expenditures with established goals and regulatory requirements. Application: the audit verifies the justification of project estimates, compliance with procurement procedures, the adequacy of contracts concluded with contractors and executors, and also analyzes the effect of the implemented measures.

The Life-Cycle Cost Analysis (LCCA) method considers the total costs of cyber security measures from the moment of their planning (concept, technical specifications) to the decommissioning of systems (equipment disposal, software updates, closure of infrastructure facilities). Application: allows you to compare long-term costs between different technical solutions (cost of maintaining your own SOC vs. subscription to MSSP services) and choose the most economically feasible option.

The Keynesian Multipliers Analysis method is used to assess the multiplier effect of investments in cybersecurity on the regional economy: how many additional jobs are created in related industries (IT development, engineering and installation work) for each hryvnia invested in the project. Application: helps to prove the feasibility of state subsidies or compensation for CI enterprises, because it shows how money "circulates" in the regional economy with an additional effect.

The Real Options Analysis method is suitable for evaluating cybersecurity investments as options with different scenarios of technological environment development: for example, the possibility of "deploying" additional cyber infrastructure if the risks of attacks increase in the next 2–3 years. Application: takes into account the uncertainty of future technological changes and allows you to make decisions taking into account the options of "postponing", "expanding" or "collapsing" the project depending on the dynamics of threats.

The “What-If” risk analysis method and Fault Tree Analysis (FTA) builds logical trees of cause-and-effect relationships that can lead to a cyber incident (for example, "what if" a SCADA controller is hacked due to the lack of network segmentation?). This allows you to identify critical nodes in the system and quantify the probability of their failures. Application: used to create a risk map of a cybersecurity investment project, where each branch of the tree is a conditional "point of vulnerability," and the sum of the probabilities gives an overall assessment of the importance of using a specific measure.

The method of standardized interviews with stakeholders, in addition to focus groups, conducts structured interviews with representatives of regulators (NKREKP, Ministry of Energy), large CI operators, insurance companies and independent auditors to collect comparative data on insurance premium rates, regulatory requirements and practical experience in budget implementation. Application: allows you to compare official requirements with the real state of affairs "on the ground", identify "blind spots" in the legislation and assess which regulatory changes have priority to increase economic efficiency.

The method of building techno-economic models (Techno-Economic Modeling) integrates technical characteristics (equipment productivity, system recovery time after an incident) with economic indicators (CAPEX, OPEX, flow costs). Models can be built in specialized software (for example, MATLAB/Simulink or Excel with macros) to assess the sensitivity of investments to basic parameters. Application: is used to select optimal equipment configurations, estimate the cost of "conditionally safe" vs. "maximum protected" mode of operation of the system.

The Value Chain Analysis method considers the entire value creation cycle of CI services (from obtaining raw materials in the form of electricity or gas to transferring them to the end consumer), determining at which stages the most vulnerable elements from the point of view of cybersecurity and what economic burden the introduction of additional technical measures (traffic tunneling, multi-level authentication) has. Application: allows the CI enterprise to identify key "control points" and calculate how much investment in protection at each stage will affect the overall cost of the service and competitiveness.

The Vulnerability Assessment method involves in-depth testing (pentest) of CI cyber systems to identify weak layers that can be exploited by attackers. The result is a list of priorities for investment (which systems, servers, controllers need to be upgraded first). Application: allows you to develop phased vulnerability budgets with a calculation of the "cost of identified vulnerability" and integrate it into the overall economic efficiency model.

Each of the listed methods is distinguished by a specific approach to collecting and processing information, justifying decisions and predicting consequences. Together, they allow you to comprehensively assess which investments in cybersecurity of critical infrastructure are economically feasible, how to allocate resources between preventive and reactive measures, as well as what managerial and regulatory support is needed for sustainable protection in conditions of rapid digitalization.

2. Theoretical and Practical Aspects of the Application of Economic Tools for Risk Assessment and Investment in the Development of Cybersecurity of Critical Infrastructure, Driven by Digitalization Processes

2.1. Theoretical and Normative Understanding of Digitalization in the Field of Critical Infrastructure

Individual issues of digitalization in the field of critical infrastructure have been the subject of research by both Ukrainian and international scientists.

A. P. Gavrys, V. V. Filippova, N. Yu. Tur carried out a comprehensive analysis of modern threats, in particular military, man-made, natural and cyber. Particular attention is paid to the issues of modernization and improvement of means of protecting infrastructure, which has become a target due to its importance for economic and social stability. The problem of the study is due to the need to ensure the reliable functioning of critical infrastructure, which has become a priority task in light of the unprecedented growth of attacks and technical vulnerability of many facilities. The authors analyzed the protection of critical infrastructure facilities in

Ukraine during a military conflict, emphasizing the complexity of modern threats and the need for an integrated approach. The work clearly emphasizes that critical infrastructure is the basis of the country's life, as it ensures the functioning of the economy, transport, communications and public services for the population. Modernization of infrastructure facilities, use of monitoring systems and strengthening of physical protection significantly increase resistance to attacks, including missile and cyber threats. The authors also prove that protection of energy facilities is a priority, since the energy sector of Ukraine is a strategically important part of the infrastructure, and the destruction or damage to energy facilities leads to power outages in large regions, which in turn paralyzes the work of enterprises, hospitals, schools and other important institutions. The defeat of these facilities can complicate logistics, equipment repair, weapons production and other defense processes. The lack of electricity and heat in cold weather conditions creates serious problems for the health of Ukrainian citizens. As a result, in conditions of an unprecedented increase in attacks and man-made threats, the proposed measures are designed not only to increase the resilience of infrastructure to destruction, but also to contribute to the stability of the state and the security of its citizens. The experience gained from the analysis of international practices allows Ukraine to adapt effective strategies for the protection of critical infrastructure, as well as to develop national approaches that take into account the specifics of the modern conflict and the need for a rapid response. These conclusions and recommendations can serve as the foundation for further scientific and applied research aimed at forming a comprehensive system for the protection of critical infrastructure facilities in the context of global and national security (A. P. Gavrys, V. V. Filippova, N. Yu. Tur, 2024). In this book, Roger Anderson examines in detail the architectural principles of building secure distributed systems, paying close attention to the issues of protecting critical infrastructure elements (SCADA controllers, network gateways). From a technical point of view, he analyzes the main attack vectors on industrial controllers (PLC) and emphasizes the need for network segmentation and minimizing the "access bandwidth" for potential attackers. From an economic perspective, the book introduces the concept of Total Cost of Ownership (TCO) for implementing security measures: the author compares the costs of adding cryptographic modules to legacy equipment with the potential losses from a breach – a cost-vs. loss assessment helps to form an economically sound investment plan for cybersecurity (Anderson R., 2008). Bruce Schneier focuses on the global aspects of collecting, processing, and protecting personal and industrial data. In the context of critical infrastructure, he analyzes how the transition to digital platforms opens up new channels for information leakage (e.g., through smart energy meter telemetry) and describes typical technical vulnerabilities (insufficient encryption, vulnerable APIs). The economic block of the book contains a discussion of how losses from hidden attacks (data theft, disruption of operations) can be many times higher than the initial investment in the implementation of anonymization and authentication tools (Schneier, 2015).

This document provides comprehensive recommendations for the technical protection of industrial controllers and networks (SCADA/ICS). The first part considers technical challenges: compatibility with legacy equipment, patch management issues, building DMZ zones, access administration and monitoring. The second part is an economic model for implementing security measures: calculating CAPEX and OPEX for IDS/IPS equipment, assessing ROI due to reducing downtime and accidents in production processes. NIST SP 800-82 also recommends the use of a Risk Management Framework, where each stage (asset identification, threat analysis, selection of protection measures) is supported by a demonstration of the financial consequences of both non-use and implementation of measures (NIST SP 800-82 Rev, 2015).

The ENISA report focuses on current and future threats to cyber-physical systems, which include critical infrastructure facilities. The technical part describes attack vectors: the use of vulnerabilities in industrial protocols (Modbus, DNP3), DDoS attacks at the telecommunications level and the vulnerability of IoT devices in "smart" networks. The economic assessment is devoted to the analysis of the average costs of recovering from incidents (with repair of physical devices and replacement of software), as well as the forecast of possible fines and reputational losses. ENISA recommends creating multi-level budgets for preventive measures, taking into account the level of maturity of cyber protection in each sector (energy, water, transport) (Threat Landscape for Cyber-Physical and SCADA Systems, 2018). In the article "The Economics of Cybersecurity: Challenges for Critical Infrastructure" by Daniel Geer, he examines how economic motivations determine the level of protection of critical infrastructure elements. The technical part describes the principles of building early warning systems (IDS/IPS), the need for a segmented network architecture and the implementation of EDR technologies. From an economic point of view, the author analyzes why CI operators often underfinance cyber protection: due to the lack of direct market signals (cybersecurity is an "invisible good"), the uncertainty of potential losses and the difficulty of assessing the effect of investments. He suggests the use of partial subsidy mechanisms and cyber risk insurance to stimulate operators to invest in protection (Geer D., 2013).

Riccardo Baldoni's work "Critical Infrastructure Protection in the Digital Age" is based on a detailed analysis of the current state of infrastructure cyber protection in different European countries. Technical challenges include the need for scalable solutions: from the implementation of industrial proxies (secure gateways) to the use of SIEM/SCADA Integration Platform for real-time event correlation. The economic part highlights the problem of "moral hazard" – when operators receive government grants or compensation but are not willing to invest their own resources in upgrading their IT infrastructure. Baldoni suggests public-private partnership (PPP) models and specific financial instruments, such as "security certificates", that allow to compensate for part of the costs of external audit and certification of systems (Baldoni R., 2017). In his article "Economic aspects of protecting a "smart" power grid", Emilius Jones focuses on the economic challenges of implementing cybersecurity within the Smart Grid. The technical part considers the architecture of secure communication between RPA (radio-based automated systems) and central dispatching. He examines how the impact of cryptographic protection on QoS (Quality of Service), additional data transmission delays and increased requirements for computing resources can lead to the need to modernize transmitters and central servers. The economic part contains LCOE (Levelized Cost of Energy) calculations taking into account investments in cybersecurity and reduction of network capacity. The author concludes that the correct balancing of "cost/efficiency" of Smart Grid protection significantly affects the final cost of electricity for consumers and the level of investment in regional energy systems (Jones, A. 2019). In this article, V. Kharchenko "Economic Challenges of Cybersecurity of Critical Infrastructure of Ukraine" analyzes the Ukrainian context: technical problems of compatibility of outdated Soviet-style equipment with new OT Security class solutions, as well as the lack of qualified engineers servicing critical systems. From an economic point of view, Kharchenko highlights the lack of funding at the state level and the low attractiveness of private investments in cyber defense: he provides calculations of budget allocations (CAPEX, OPEX) of large CI operators in Ukraine and demonstrates that the share of real costs for cyber defense in the total volume of investments is less than 5%. The author proposes to create tax incentive mechanisms (reduction of VAT on equipment, exemption from income tax of part of certification costs) and develop a system of state "Matching Funds" (co-financing) for expensive projects in critical energy networks and water supply systems (Kharchenko, 2021).

S. Golod and O. Petrenko offer mathematical models for economic risk assessment for energy enterprises. The technical part includes the development of probabilistic models taking into account different types of threats (physical access to a substation, infection of switches with MIM attacks, internal threats to employees). The economic section of the article provides formulas for calculating expected losses (Expected Annual Loss Event, EALE) and suggests mechanisms for optimizing investments in preventive measures (traffic filtering, next-generation IDS) depending on the acceptable level of risk (Risk Appetite). The authors also take into account that for state-owned enterprises, "acceptable risk" is determined by the regulatory acts of the National Commission for the Regulation of Energy and Utilities of Ukraine, and develop budget allocation algorithms with a link to tariff regulation (Holod, Petrenko, 2020).

Although Gary Becker's classic work "Human Capital: A Theoretical and Empirical Analysis with Special Reference to Education" does not directly address cybersecurity, it lays the theoretical foundations for the economic evaluation of investments in human resources, which is critical in the development of cybersecurity personnel. In the context of studying technical and economic challenges, this book justifies why investments in education and advanced training of IT specialists (cybersecurity courses, CISSP/CISM certification programs) are justified: the increase in the productivity of experts is directly correlated with the reduction of losses due to incidents, which allows the specific costs of training to be spread over a longer time horizon with increased efficiency (Becker, 1994).

2.2. Technical and Economic Challenges of Ensuring Cybersecurity of Critical Infrastructure During Digitalization

Among the technical challenges of ensuring cybersecurity of critical infrastructure in the context of digitalization, the following can be highlighted:

1) integration of old and new systems. Many critical infrastructure objects operate on outdated PLCs (programmable logic controllers) and network equipment that do not support modern cryptographic authentication and encryption methods. Combining such legacy systems with new cloud or edge solutions creates a security gap, as updating the software of old controllers is often impossible without completely replacing the equipment;

2) lack of unified standards and protocols. Different device manufacturers may use unique or unsecured communication protocols (Modbus, DNP3, OPC UA without protection). The presence of customized

implementations complicates the unified application of monitoring and anomaly detection tools, as well as the implementation of corporate security policies;

3) increasing complexity of attacks. Modern threats – from network "irrigation" (watering holes) to Advanced Persistent Threat (APT) attacks – require an integrated approach: a combination of IDS/IPS (intrusion detection and prevention systems), SIEM (event collection and analysis systems), EDR (endpoint detection and response), as well as regular pentests and configuration audits. The lack of in-house specialists with experience in industrial networks increases risks, because typical IT solutions are not always adapted for the OT segment;

4) the need for constant updating and monitoring. Each software or firmware update of devices can create new vulnerabilities. SCADA and HMI (human-machine interface) systems require 24/7 monitoring of network traffic and rapid response to abnormal behavior, which requires the deployment of specialized SOC (security operations center) or remote MSSP (managed security service provider) with a deep understanding of both the IT and OT environments.

Thus, the technical challenges of ensuring cybersecurity of critical infrastructure in the context of digitalization are a set of problems and limitations associated with the integration of legacy industrial systems (OT) with new information and communication technologies (IT), which complicate the implementation of effective protection. These include: the need for compatibility of legacy controllers with modern encryption protocols; the lack of standardized interfaces for centralized incident monitoring; limited hardware resources of industrial devices for implementing security agents; the complexity of patch management and firmware updates without stopping production processes; high vulnerability of network connections due to the use of insecure protocols; as well as the need for continuous (24/7) monitoring and operational response to threats in real time.

Among the economic challenges, the key ones, in our opinion, are:

1) high initial investments. The purchase of secure equipment (production PLCs with built-in authentication tools), licensed encryption solutions, dealing with IDS/IPS and SIEM systems, and the arrangement of segmented DMZ zones for critical nodes require significant capital expenditures. For a state or private operator, this often means a review of the budget and priorities: investing in cybersecurity may at first glance seem to be a lower priority than, say, building new power lines or pumping gas;

2) return on investment (ROI). Unlike direct investments in production or construction, the benefits of investing in cybersecurity are partially invisible: it is easier to prevent an attack than to restore lost facilities and reputation. It is necessary to calculate the economic losses from the shutdown of critical infrastructure (cost of downtime, fines, compensation to consumers, loss of trust of partners) and compare them with the costs of a modern SOC, personnel training and equipment upgrades;

3) training. The introduction of "closed" seasonal retraining programs and support for certifications (for example, CISSP, CISM, SANS courses for OT engineers) require systematic investments in the development of human capital. At the same time, the labor market stimulates the "outflow" of experienced security analysts to international projects or the banking sector with higher salaries, which leads to a shortage of qualified specialists in state-owned enterprises of critical purpose;

4) modeling of threats and losses. In order to make a reasonable investment in cyber defense, it is necessary to develop an economically sound risk assessment model (technical and financial probability of an incident), as well as a methodology for calculating expected losses. For example, to focus on the NIST SP 800-30 standard (Risk Management Guide for Information Technology Systems), but adapt it to the local regulatory environment and industry specifics. This requires a budget item for conducting audits, pentests, attack modeling with the involvement of external experts and cyber risk insurance;

5) the use of cost-effective protection methods. At the facility level: critical infrastructure operators at each critical infrastructure facility develop and ensure the implementation of a facility plan of measures to protect and ensure the resilience of critical infrastructure, which includes measures for physical protection, countering threats, effective reduction and control of security risks, ensuring information security and cybersecurity at critical infrastructure facilities (Bohdan, Kuzmenko, & Chorna, 2023).

Thus, the economic challenges of ensuring cybersecurity of critical infrastructure in the context of digitalization are a set of problems related to the appropriate allocation of limited financial and human resources for the implementation and maintenance of protective measures in digital systems. They include high initial investments (CAPEX) in the purchase of certified equipment, licensed software and the creation of a SOC with 24/7 monitoring; significant operating expenses (OPEX) for updating and maintaining security tools, patch management and staff training; uncertainty in calculating the return on investment (ROI), since the benefits of preventing cyberattacks are difficult to quantify; and the competition of such expenses with other budgeting priorities (production modernization, equipment renewal). Additional challenges include a shortage of qualified professionals with high salary expectations, exchange rate fluctuations and inflation, which increase the cost of imported solutions, and the need to create cyber risk insurance systems at adequate rates that would make investment projects cheaper. All of this makes it difficult to justify and plan estimates for sustainable protection of critical infrastructure.

2.3. Prospects for Ensuring Cybersecurity of Critical Infrastructure in the Context of Digitalization

One of the key promising areas is the gradual transition to the "zero trust" model, when no network element is automatically considered trustworthy. This means that each connected device (PLC, sensor, workstation) undergoes constant authentication and authorization before accessing sensitive resources. Network segmentation allows you to isolate critical OT networks from the general IT flow, reducing the "attack surface" and simplifying incident localization. With the implementation of the IEC 62443 standards and the recommended NIST SP 800-82 Rev. 2, unified approaches to delimiting trust zones will appear, which will increase the resilience of the CI. The next promising area, in our opinion, is the involvement of artificial intelligence systems (SIEM with UEBA/EPP/EDR modules, machine learning for analyzing anomalous traffic) will allow for predictive detection of threats in real time. Thanks to algorithms for analyzing the behavior of network flows in SCADA/ICS systems, it is possible not only to increase the accuracy of detecting "invisible" APT attacks, but also to automatically respond – by isolating vulnerable segments or changing controller configurations before a critical incident occurs. The role of cognitive platforms and “digital twins” will further increase for modeling "what if" scenarios, which will allow adapting protective policies even before changes are introduced to the production infrastructure.

The prospect of implementing quantum encryption and next-generation secure networks is interesting. Along with the development of quantum computing, there will be a need for quantum-resistant cryptographic algorithms (PQCrypto), which will preserve data confidentiality in the event of the emergence of quantum computers capable of cracking traditional RSA or ECC. The implementation of QKD (Quantum Key Distribution) protocols at the inter-node level of industrial networks will ensure that encryption keys cannot be intercepted. In parallel, 5G/6G networks with built-in security elements (network slicing, secure edge computing) will be developed, which will allow for the implementation of flexible private MEC (multi-access edge computing) for local protection of CI.

Certainly, in the conditions of obtaining the status of candidate for EU membership, the introduction of European integration standards and state regulation is promising. In the future, Ukraine will increasingly implement the NIS 2 Directive and Regulation EU 2022/2555 (On the Digital Operational Resilience for the Financial Sector, DORA), which will require critical infrastructure operators to conduct regular cybersecurity audits, test recovery plans, and provide incident reporting. It is expected that the role of the National Cybersecurity Coordination Center will be strengthened, and requirements for equipment and software certification in accordance with the European standards ISO/IEC 27001, ISO 22301 will be increased. This will create a common framework for public and private players, stimulating infrastructure modernization taking into account the best European practices. The next step is the development of human capital and institutional cooperation. Ensuring a sustainable level of cybersecurity also involves the formation of an ecosystem of professional training: the creation of master's programs in cyber-physical security, partnerships between universities and industrial enterprises for internships in SOC/CSIRT, support for CISM/CISSP certification courses. It is important to strengthen multidisciplinary interaction between IT, OT and legal experts, as well as expand cooperation with international organizations (ENISA, NIST, NATO CCDCOE) to exchange experience and respond to global threats as quickly as possible. Taken together, these perspectives form a gradual transition from fragmented "point" protection to a comprehensive, adaptive and proactive model of cybersecurity of critical infrastructure, combining technical innovations, economic feasibility and international integration.

References:

Ross Anderson (2021). Security Engineering: A Guide to Building Dependable Distributed Systems). John Wiley and Sons Ltd. 450 p.

Schneier Bruce (2016). The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. 448 p.

NIST (2015). NIST SP 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security (SP 800-82 Rev. 2). National Institute of Standards and Technology. Available at: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

ENISA (2018). Threat Landscape for Cyber-Physical and SCADA Systems (Threat Landscape for CPS/SCADA). European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-cyber-physical-systems-and-scada

Geer, D. (2013). The Economics of Cybersecurity: Challenges for Critical Infrastructure. *IEEE Security & Privacy,* 11(3), 10–17.

Baldoni, R. (2017). Critical Infrastructure Protection in the Digital Age. Springer. 250 p.

Jones, A. (2019). Economic Aspects of Securing the Smart Grid. Energy Policy, p. 1021–1030.

Kharchenko, V. (2021). Economic Challenges of Cybersecurity for Ukraine's Critical Infrastructure. *Cybernetics and Security*, 2, 45–52.

Golod, S., & Petrenko, O. (2020). Risk Assessment Models for Cybersecurity in Power Supply. *Energy and Information Technologies,* 8(1), 33–41.

Becker, G. S. (1994). Human Capital: A Theoretical and Empirical Analysis with Special Reference to Education. University of Chicago Press. 340 p.

Gavrys A. P., Filippova V. V., Tur N. Yu. (2024) Information analysis of critical infrastructure protection systems during martial law. *Bulletin of the LDUBZHD,* 30, 173–187.

Bohdan, B., Kuzmenko, O., & Chorna, V. (2023). Economic measures for managing critical infrastructure facilities in Ukraine. *Baltic Journal of Economic Studies,* 9(3), 22–32. DOI: https://doi.org/10.30525/2256-0742/2023-9-3-22-32

Received on: 19th of June, 2025
Accepted on: 14th of August, 2025
Published on: 20th of August, 2025