MEST Journal
DOI: 10.12709/mest.14.14.01.13

CASE STUDY
MEST Journal

THE LABOR MARKET IN TERMS OF THE SHADOW DIGITAL ECONOMY

Serghei Ohrimenco
Laboratory of Information Security at the Academy of Economic Studies of Moldova, Chisinau. Moldova
https://orcid.org/0000-0002-6734-4321

Tatiana Manasterska
University of Kalisz, Faculty of Social Sciences, Department of Social Research and Communication, Poland
https://orcid.org/0000-0003-3567-1667

Lucia Gujuman
Department of Information Technology and Information Management, Academy of Economic Studies of Moldova, Chisinau. Moldova
https://orcid.org/0000-0001-7940-4291

ARTICLE INFO

Open access

JEL Category:
E26, J46, O17

Keywords:

Labor market

Shadow digital economy

Products and services

Dark market

Computer crime

Cybersecurity.

ABSTRACT

This article examines the shadow digital economy (SDE), a growing phenomenon amid digital transformation and rising information costs. We review technical and economic definitions and propose an integrated definition of the SDE. The study offers the first systematic analysis of labor markets and the qualitative traits of participants in this criminal ecosystem. We identify a structured set of labor-market roles within the SDE model. We analyze institutional traps that sustain shadow employment and show how the SDE perpetuates informal and illicit labor arrangements. The paper proposes a clear classification of criminally oriented products and services. We introduce a concise conceptual model of a "shadow" project for designing SDE products or services organized by criminal groups, detailing participant roles and project composition. Specialized services that require further study are grouped and highlighted. Our findings indicate that SDE activity extends beyond direct financial loss, eroding consumer trust, damaging brand reputation through data breaches, fraud, and counterfeiting, and posing risks to national security. The study ends with policy implications and recommendations for periodic evaluation and integration of AI-related risks into financial governance.

Address of the author:
Serghei Ohrimenco
osal@ase.md

Received: 04.12.2025
Revised: 25.12.2025
Accepted: 02.01.2026
Available online: 15.01.2026

1 INTRODUCTION

In the mid-20th century, interest in the shadow economy began to grow in various countries. Various studies conducted during this period led to the emergence of a new field in economics and the development of government initiatives aimed at combating the shadow economy and its integration into the legal sphere.

This paper examines the phenomenon of the shadow digital economy (SDE) as a form of latent but escalating digital warfare operating at the intersection of informal economic activity and cybercrime.

The authors analyze key practices within the digital economy, encompassing cyberattacks, labor-market distortions, transnational data trading, cyberextortion and monetized attacks, platform-based informal labor exploitation, money laundering, and tax evasion, enabled by anonymity and digital payment systems. These processes not only operate "outside the law" but also actively transform the institutional environment, exploiting its vulnerabilities and creating a parallel system of value chains where legal and illegal practices are intertwined.

Based on comprehensive studies of the digital economy, the authors propose an analytical framework that allows us to consider the digital economy as a systemic challenge requiring comprehensive strategies for digital sovereignty, institutional sustainability, and international regulation.

Table 1. Definitions of Technological Risks

Adverse outcomes of AI technologies	Intended or unintended negative consequences of advances in AI and related technological capabilities (including Generative AI) on individuals, businesses, ecosystems and/or economies
Adverse outcomes of frontier technologies (quantum, biotech, geoengineering)	Intended or unintended negative consequences of advances in frontier technologies on individuals, businesses, ecosystems and/or economies. Includes, but is not limited to brain-computer interfaces, biotechnology, geoengineering and quantum computing.
Censorship and surveillance	Broad and pervasive observation of a place or person and/or suppression of communication, information and ideas, physically or digitally, to the extent that it significantly infringes on human and civil rights (e. g. privacy, freedom of speech and freedom of expression).
Cyber espionage and warfare	Use of cyber weapons and tools by state and non-state actors to gain control over a digital presence, cause operational disruption, and/or compromise or damage an entity's technological and information networks and infrastructure. Includes: defensive and offensive cyber operations that occur during or trigger armed conflict, and cyberattacks that steal classified, sensitive data or intellectual property to gain an advantage.
Misinformation and disinformation	Persistent false information (deliberate or otherwise) widely spread through media networks, shifting public opinion in a significant way towards distrust in facts and authority. Includes, but is not limited to: false, imposter, manipulated and fabricated content.
Online harms	Erosion of protection from and/or prevalence of harmful behaviour that poses a digital threat to the emotional or mental health and well-being of individuals. Includes, but is not limited to: online child sexual abuse, online harassment and cyber bullying.

Source: (World Economic Forum, 2025, p. 76)

The Global Risks Report 2025 (World Economic Forum, 2025) confirms the seriousness of the problems and challenges. It outlines the current global risk landscape in five key dimensions: economic, environmental, geopolitical, social, and technological. The latter group includes Adverse

Outcomes of AI Technologies and Cyber Espionage and Warfare. Global risks ranked by short- and long-term severity include Misinformation and Disinformation, Cyber Espionage and Warfare, Online Harms, Censorship and Surveillance, and Adverse Outcomes of Frontier Technologies (ranked 1st, 5th, 14th, 16th, 31st, and 33rd in the short term) and Misinformation and Disinformation, and Adverse Outcomes of AI Technologies (ranked 5th, 6th, and 5th in the long term, respectively). A detailed description of the technological risks is provided in Table 1.

These categories expand our understanding of the SDE, but they don't answer the question of how technological risks influence the situation.

We also review key literature to deepen understanding of the SDE. These include the works of renowned Austrian economist Friedrich Schneider (Medina & Schneider, 2019; Medina & Schneider, 2021), and his co-authors, scholars Ligita Gaspareniene and Rita Remeikiene (Gaspareniene et al., 2016), and Dinara Orlova (Ohrimenco et al., 2025), whose publications focus on the shadow economy and the digital economy, as well as its various variants, the SDE. Of the recent works, it is worth mentioning (Berdiev et al., 2024), in which the authors highlight “new” features of the SDE, such as the connection between corruption and digital currencies.

Austrian scholar Friedrich Schneider made a significant contribution to the development of the scientific field of measuring the shadow economy. His works examine in detail various aspects of the shadow economy in both developed and developing countries. Schneider (2017) argues that the shadow economy represents the informal sector of a national economy that is not recorded in official statistics.

In addition to “shadow economy,” the literature commonly employs terms such as alternative economy, hidden, concealed, twilight, invisible, autonomous, black, cash, secret, illegal, parallel, and unofficial.

2 RESEARCH METHODOLOGY

This article is based on an analysis of available literature and a structural synthesis of data aimed at identifying and addressing problems associated with SDE.

The methodological approach includes:

- *a research framework*. This framework derives from the problem being studied and a set of key questions, including characteristics and definitions of SDE, assessments of the labor market and institutional traps, criminally oriented products and services, and specialized services.
- *literature review*. This study employs a systematic review of scholarly and practitioner literature and reports from research firms specializing in information security and its economic aspects. We use these sources to synthesize existing knowledge and identify emerging trends related to the shadow digital economy. The study included a review of scientific databases, including Google Scholar, IEEE Xplore, and Scopus (for the period 2019-2024), except for a few publications. Keywords for identifying sources included terms such as Labor Market, Shadow Digital Economy, Product and Services, Dark Market, Computer Crime, and Cybersecurity.
- *categorization of problems and solutions*. Several security-related issues were identified, including the finding that SDE activities extend far beyond financial losses by undermining consumer trust, damaging brand reputation (notably via data breaches, fraud, and counterfeiting), and threatening regional and national security.
- *data analysis and synthesis*. All collected data was systematized by thematic areas: technological risks, the digital economy and its definitions, labor markets, as well as categories such as the shadow, non-observed, and criminal economies.

A significant obstacle hinders the development of a unified methodology for defining the SDE, its structural components and sectors, and for assessing their economic impact. This primarily relates to the lack of statistical data on SDE. The available data characterizing individual aspects of SDE manifestations are based on surveys conducted by individual researchers and research firms. Evidence indicates that government and commercial organizations are reluctant to report computer incidents and the damage they cause.

This, according to the authors, is precisely what hinders the development of a methodology for studying SDE.

3 DEFINITION OF THE DIGITAL ECONOMY

Let's begin by defining the digital economy:

“The digital economy represents the pervasive use of IT (hardware, software, applications and telecommunications) in all aspects of the economy, including internal operations of organizations (business, government and non-profit); transactions between organizations; and transactions between individuals, acting both as consumers and citizens, and organizations. The technologies underlying the digital economy also go far beyond the Internet and personal computers. IT is embedded in a vast array of products, and not just technology products like cell phones, GPS units, PDAs, MP3 players, and digital cameras” (Malecki & Moriset, 2007).

We will attempt to analyze categories such as the shadow, non-observed, and criminal economies. The methodology proposed by the Organization for Economic Co-operation and Development (OECD) (2017) should be adopted as a starting point. Specifically, the following categories are identified:

- *Underground production* - activities that are productive and legal but intentionally concealed by government authorities to avoid paying taxes or complying with laws (regulations).
- *Illegal production* - production activities that result in the creation of goods and services prohibited by law or that are illegal, through the implementation of unauthorized procedures.
- *Informal sector production* - production activities carried out by unincorporated enterprises in the household sector or other units that are not registered and/or smaller than a specified size in terms of employment and have a market production.
- *Production of households for own-final use* - production activities that result in goods or services being consumed or capitalized by the households that produced them.
- *Statistical underground* - defined as all productive activities that should be recorded in core data collection programs but are omitted due to deficiencies in the statistical system.

Based on the research conducted, the authors propose the following definitions of the shadow digital economy (Ohrimenco et al., 2024; Ohrimenco et al., 2019; Ohrimenco et al., 2021B):

- The shadow digital economy is a specific sphere of economic activity with its own structure and system of economic relations. This specificity is determined by the illegality, informality, and criminal nature of economic activity and the concealment of income.
- From an economic perspective, it is a sphere of economic relations encompassing all types of production and business activities that, in their direction, content, nature, and form, contradict the requirements of current legislation and are carried out contrary to state regulation of the economy and bypassing oversight.
- From a technological perspective, it is an individual and/or collective activity that is illegal, related to the design, development, distribution, support, and use of information and communication technology components hidden from society and of a criminal nature.

Thus, the shadow digital economy (SDE) is understood as a sector of economic relations where production and economic activity, regardless of its direction, content, nature and form, do not comply with the norms of current legislation and is carried out through digital technologies outside the framework of state regulation and control.

Shadow entrepreneurship lies at the core of the SDE and is characterized by the following common features: first, it is a hidden, latent activity that is not recorded by government agencies and is not reflected in official reporting; second, it encompasses all stages of social reproduction: production, distribution, exchange, and consumption; third, all processes, from the analysis of software source code to the monetization of botnet rentals, are criminal and parasitic in nature.

4 LABOR MARKETS

Academic debate surrounds the qualitative characteristics of participants engaged in the shadow digital economy. The model of the shadow digital economy identifies a unique system of labor market participants (Clayton, 2019).

The first group consists of researchers whose work focuses on identifying and studying weaknesses in information systems. Based on the data obtained, new exploitation techniques are developed. The next group consists of developers who create software, including malware designed for extortion or data theft. These developers also create tools for infiltrating systems to gain unauthorized access to information.

After software development comes the distribution stage, where vendors-the final link in the software development process-play a particularly important role. They not only sell malware and stolen data but also provide feedback between developers and end users, allowing for improvements in the quality and functionality of the software being developed. Ensuring the functioning of the entire system infrastructure also requires IT technicians who build and maintain networks, servers, and databases. These specialists create conditions for all other groups to operate. Hackers are also a key element, searching for vulnerabilities in various information systems, applications, and networks that allow criminals to access protected data.

Fraudsters play a key role in the functioning of the SDE system, analyzing vulnerabilities and developing new schemes to deceive and manipulate potential victims. Additionally, there is a category of hosting service specialists who provide hosting services to criminals, supporting fraudulent content and associated websites.

Finally, managers oversee the organization, recruit and onboard participants, assemble teams for specific functions, and coordinate day operations.

It's worth noting that the SDE blurs the lines between employment and individual entrepreneurship. A successful specialist can be employed by a large IT company and simultaneously hire their own contractors, typically working online, who can therefore be located anywhere in the world with internet access.

The IT labor market model demonstrates a new approach, where specialists are both employees and employers. They work for several companies, delegating some of their responsibilities to a team of assistants hired through platforms like Upwork. This allows them to significantly increase their income without formal employment, creating a multi-tasking system in which they coordinate the team's work while their assistants perform their duties. This model gives flexibility and financial stability but is also fraught with risks due to the difficulty of monitoring by employers and the potential for breaches of employment agreements.

One of the key characteristics of the shadow IT labor market is its secrecy. Programmers working on large projects are often unaware that their labor is being used to create illegal products or implement criminal schemes. This creates conditions for the functional isolation of individual workers from the overall functioning of the underground economy. In some cases, such workers believe their activities are limited exclusively to legal operations, making it difficult for law enforcement to track criminal projects.

Shadow labor markets in the information sphere are characterized by a high level of organizational complexity. Unlike traditional forms of criminal activity, such as drug trafficking or smuggling, which employ more overt and transparent schemes, the use of hired labor in the digital sphere requires much more sophisticated methods of disguise. This allows criminal groups to operate effectively within the framework of legitimate enterprises, concealing the true nature of their activities.

A key feature of such projects is not only the lack of direct worker awareness of the illegality of their work, but also the control structure that minimizes the risk of detection. Organizational mechanisms in shadow-economy projects commonly restrict workers' access to information about the true purpose of their work, thereby lowering the probability that they will perceive their involvement as criminal.

The system of criminal labor organization described above can be examined through the lens of institutional traps, allowing for a deeper understanding of its operating dynamics and parallels with formal systems.

In the context of the SDE criminal organization, developers, traders, hackers, fraudsters, and other participants operate within a specific institutional environment, where their activities are not only subject to criminal "norms" and "rules" but also create conditions for the emergence of institutional traps. Such traps include:

The Legalization Trap. In a traditional labor system, market participants may face a situation where the uncontrolled growth of informal or semi-legal professions leads to the formation of a shadow market where rules are not properly regulated. In a criminal organization, this is analogous to a situation where criminals begin to operate according to established criminal patterns, and such actions become the norm. This leads to the stabilization of criminal practices, making them more difficult to suppress. Participants in the system adapt to these conditions and, in a sense, become dependent on them.

The Trust Trap. Within a criminal network, interactions between developers, traders, and hackers can lead to the formation of a specific trust between participants, which in turn gives rise to institutions that support criminal activity. This creates a vicious circle in which the criminal organization becomes resilient to external interference, and its participants, using existing channels, develop and maintain their activities. In the official economy, a similar situation can arise in shadow labor markets when workers begin to collaborate with informal structures, thereby strengthening illegal schemes. Another example of a “trust trap” is the establishment of arbitration tribunals to resolve disputes between individual and group interests among participants in the energy market.

Corruption trap. Participation in criminal schemes—by fraudsters and managers alike—creates a system in which each participant becomes, to some extent, dependent on corrupt relationships to achieve their objectives. Internal networks of loyalty and dependency hinder potential change, as any violation of established rules can lead to a breakdown of the entire structure. Similarly, in legitimate markets, when institutional problems (such as ineffective legislation or corruption) lead to ineffective functioning, this creates a vicious cycle in which the system becomes incapable of reform.

Automatism trap. In criminal organizations, as in ordinary institutions, situations can arise where participants begin to act out of habit, automatically following established patterns and routine processes. This can lead to the stabilization of existing practices, even if they become less effective or dangerous. This automatism in actions can be compared to institutional traps in the economy, when the labor market experiences difficulties due to outdated practices or a lack of receptivity to innovation.

These institutional traps in the context of the SDE criminal organization are not only a consequence of certain norms and processes but also a factor that sustains its existence. Participants in the SDE system frequently find themselves trapped: adherence to current rules and norms consolidates the criminal structure. This mirrors formal labour markets, where legacy institutions can restrict development and maintain unstable or ineffective practices.

Shadow employment negatively impacts the labour market in the following ways: informal employment represents a serious distortion of labour relations. The lack of proper employment registration leads to employers' disregard for labour laws and for workers a lack of rights, social guarantees, and legal protection. This opens the door to predatory exploitation of the labor force, particularly through underpaying, noncompliance with labor safety requirements and standards, and the use of labor (high-intensity and excessive working hours, lack of days off, paid vacations, etc.). Underpaying informal workers, in turn, reduces incentives to improve production and implement new technologies. All this leads to poor health among workers, a deskilled workforce, a decline in the quality of labor and the products produced, and ultimately, a decline in the country's and region's labor quality potential. Finally, paying wages in unaccounted cash leads to the concealment of income and the loss of social and tax payments. The latter, in turn, limits the potential for wage increases in the public sector. The lack of control over employment processes, coupled with various law violations, leads to the criminalization of the labor market.

The education system, which also plays a significant role in participation in the informal sector, deserves close attention. Authors Görksány and Cichocki (Gërxhani & Cichocki, 2023) show that highly educated individuals are less likely to engage in the informal sector, not only because they have a more stable income but also because they are more susceptible to social norms of tax compliance. However, in conditions

of economic instability, even highly educated individuals may resort to informal employment methods if the formal labor market does not provide sufficient jobs.

5 PRODUCTS AND SERVICES

It should be noted that the rapid development of new technologies for processing, transmitting, and storing information, as well as mobile devices and applications, ensures a relatively rapid turnover of hardware and software platforms and ecosystems, making products and services constantly fluid. As soon as manufacturers introduce a product or service to the market, they immediately become the subject of intense scrutiny by cybercriminals and the criminal underworld for potential use in crimes (Ohrimenco et al., 2021B), (PMBOK, 2000).

Due to its specific nature, tangible goods in the digital economy are extremely rare and typically involve hardware, while most products are intangible software.

It's important to note one crucial fact: as in the real economy, all goods and services in the digital economy are produced rationally and using a project-based approach (Heldman, 2018). Most "shadow" projects stem from the strategic need to overcome external environmental complexities and the challenges of managing the project as a dynamic system. Using the fundamental principles of a systems approach, project activity can be characterized as managing the relationships between project elements to achieve the project's defined goals.

Let us consider a conceptual model (basic structure) of a “shadow” project for designing a product or service in the sphere of fuel and energy efficiency, organized by a criminal group.

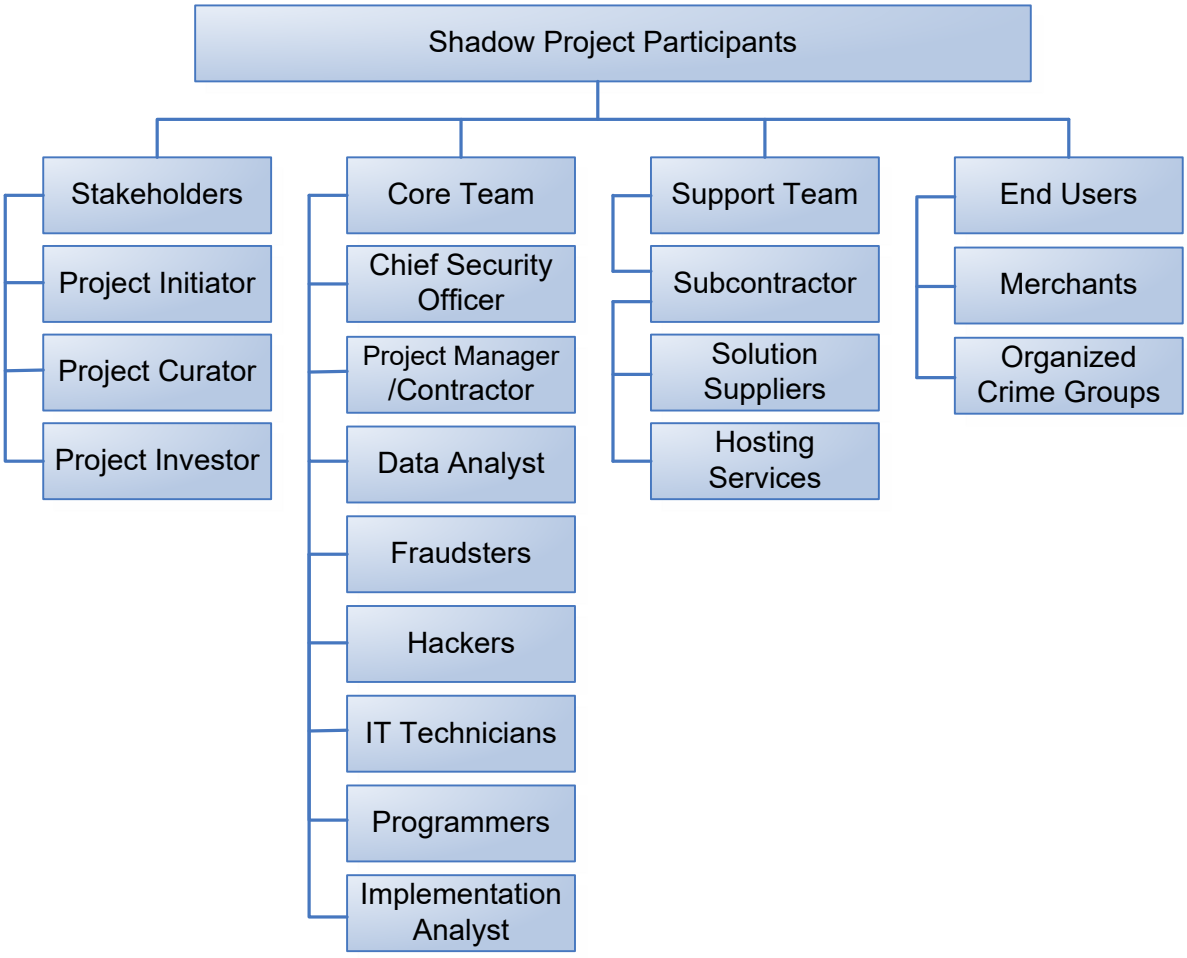

***Figure 1**: Conceptual model of a project to create a product or service in the SDE*
Source: Original work by authors

Based on their level of involvement in a "shadow" project, four groups of participants can be distinguished:

1. *Stakeholders*. These are groups pursuing their own interests and exerting some influence on the members of the core and support teams, as well as on the progress of the project. It is important to note that stakeholder groups do not directly interact with the teams.
2. *Core Team*. A group of specialists working directly on the project in close collaboration.
3. *Support Team*. Larger in size and quality than other project teams. It brings together diverse specialists and relevant structures that provide indirect assistance and influence to members of the core team. It should be noted that support team members are not directly involved in achieving project goals.
4. *End Users*. These are primarily individuals, as well as informal organizations, interested in using the created product or service for their own purposes (individually or collectively) in accordance with its purpose and technical parameters.

Let's consider the project's key participants, which include representatives of the stakeholders:

- *Project initiator*. This is the party with an interest in the successful implementation of the project and the achievement of its primary objectives and is the future owner of the project's outcome. The initiator formulates the key requirements for the project's outcomes, secures project financing from its own or borrowed funds, searches for potential investors, and enters contracts with the project's primary contractors.
- *Project Curator*. This is a senior representative of the organizational structure implementing the project. This person oversees the project's implementation on behalf of the initiator, providing overall control and operational support for the project, including sourcing financial, logistical, human, and other resources. The curator is directly responsible to the initiator for ensuring the project achieves its final goals.
- *Investor*. The party is investing in the project, for example, through loans or borrowed funds. In most cases, the initiator and investor in the project may be criminal organizations.

The following members should be identified within the core team of a "shadow" project:

- *Project Security Manager* – the individual responsible for overseeing the entire range of security and safety functions within the project. Their responsibilities include: preventing the unauthorized collection, processing, and transfer of confidential information about the project and its participants to competing organizations and law enforcement agencies; identifying informants (insiders); exposing agents of influence and undercover law enforcement officers; preventing and countering attempts at infiltration and recruitment of agents from project employees; monitoring the loyalty of project employees, combined with measures to protect them from law enforcement.
- *Project Manager/Contractor* – the specific individual responsible for project management within the project office. They are accountable to the project manager for achieving project objectives within the budget, on time, and to the specified quality level, and ensure operational management of the core project team within the context of key management functions (deadlines, costs, risks, etc.). The project manager is responsible for the overall implementation of the project, as well as for the execution of all work and services under the contract.
- *Data Analyst*, a versatile specialist with knowledge in various fields like mathematics and economic-mathematical methods, programming languages, statistics, information and communications technology, economics, and business. Their responsibilities include collecting and processing analytical data and interpreting it for project management.
- *Expert Analysts*. This is a diverse group of fraud experts with extensive experience in developing new fraud schemes and manipulating victims.
- *Hackers*. A large group of cybersecurity experts with the knowledge and skills to overcome information security systems, software protection tools, organize attacks on information systems, and search for and exploit vulnerabilities in networks, products, and applications.

- *IT Specialists*. A group of specialists who create, maintain, and expand the project's technological infrastructure – networks, systems, servers, databases, etc.
- *Programmers*. Specialists involved in developing algorithms and source code for programs designed to implement various types of software exploits for project implementation.
- *Implementation Analyst*. A specialist who provides assistance and consultations to end users through implementation services. They may also prepare source documentation, coordinate final customer requirements, and fine-tune the product or service being implemented.

Support team members may act as auxiliary participants in a "shadow" project:

- *Subcontractor.* An individual or small organization that provides liaison with the contractor and is responsible for the implementation of specific work and services in accordance with the contract.
- *Supplier*. This is a subcontractor that supplies various goods and services within the project on a contractual basis-equipment, consumables, intangible assets, etc. An example would be a "shadow" service providing hosting services as part of a criminal infrastructure.

The final, but not the least, links in the structure of a "shadow" project, organized and managed by a criminal enterprise, are:

- *Traders*. Individuals or commercial entities that sell and resell the developed product or service in the SDE sector to representatives of organized crime groups and hackers. At the same time, through the feedback function, they provide project office developers with information about user issues to improve the quality of product or service development, as well as support services.
- *Organized criminal group*. This is a stable group of individuals who have united in advance to commit one or more crimes, using a product or service in the shadow digital economy to improve the "quality and effectiveness" of their crime.

It should be noted that the project-based nature of all "shadow" processes for creating products and services in the digital economy allows them to be implemented "effectively and reliably" and controlled throughout the entire project lifecycle. It should be noted that such a project does not have a highly rigid structure, as such structures are highly unstable.

Criminal services include the deployment of malware, unauthorized system intrusion (hacking), attacks conducted via social networks, acquisition of insider information and abuse of privileges, physical theft or loss of valuable assets, and the exploitation of system vulnerabilities and malicious environments.

The information incidents generated by shadow services are shown in Figure 2 and include the following categories: malware infection, malware distribution, disruption or slowdown of an information resource, unauthorized access, information gathering using ICT, security breach, dissemination of information with inappropriate content, and vulnerabilities.

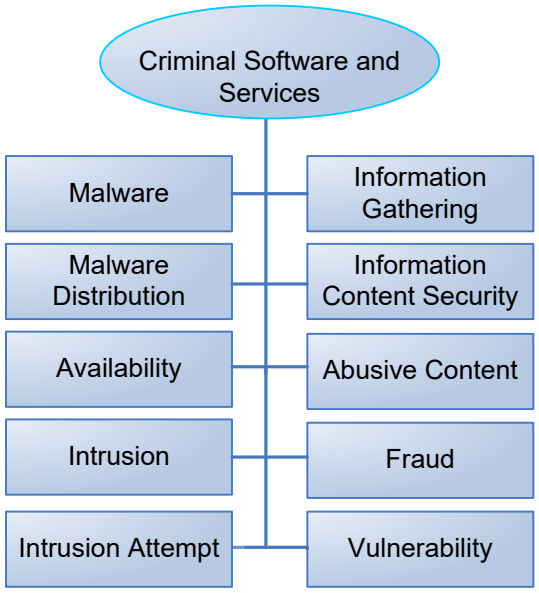

***Figure 2**: Composition of SDE services*
Source: Original work by authors

6 SPECIALIZED SERVICES

The main services in the SDE are the following:

- *Cybercrime-as-a-Service (CaaS)* – is the provision of services to others to facilitate their commission of cybercrime. This service is also called by names such as Attacks-as-a-Service, Malware-as-a-Service, and Fraud-as-a-Service. This is a set of models for developing criminal functions that cybercriminals supply to

their clients (customers) in exchange for payment for their services and products. A logical extension of this is the following services:

- *Ransomware as a Service (RaaS)* – Cybercriminals offer ransomware packages that other individuals or groups can use to infect and encrypt their targets' data. The attackers then demand a ransom from the victim to decrypt the data. Ransomware is constantly evolving through the development of additional features and is becoming a sophisticated mechanism for targeted and successful attacks.
- *Phishing-as-a-Service (PhaaS).* PhaaS vendors sell phishing kits for a fee. These packages include the tools and documentation required to carry out phishing attacks. Buyers obtain ready-made phishing pages and message templates, lists of potential victims, and other resources. User-friendly interfaces enable nontechnical actors to create and manage campaigns, and the services typically provide prebuilt templates, hosting for fraudulent sites, and data-collection mechanisms designed to harvest victims' credentials and personal information.
- *Distributed Denial of Service-as-a-Service (DDoSaaS).* In this service, cybercriminals provide tools and infrastructure for launching distributed denial of service (DDoS) attacks on websites or online services, causing them to become unavailable to legitimate users.
- *Botnets-for-hire (BfH).* Cybercriminals may rent out their botnets, which are networks of compromised computers or devices controlled by a central entity (the botmaster). Cybercriminals can use these botnets to send spam, conduct DDoS attacks, or spread malware.
- *Credential-theft-services (CTS).* Some cybercriminals offer services to steal login credentials (e.g., usernames and passwords) from individuals, companies, and other cybercriminals.
- *Research-as-a-Service (RaaS),* delivered via application programming interfaces (APIs), enables digital-era companies to integrate timely research into customer interactions. Information instability also compels cybercriminals to analyze complex events in real time to adapt their activities

7 CONCLUSION

The shadow digital economy, which fuels and scales cybercrime activities, is a crucial element of modern cyberthreats (Olejnik & Kurasiński, 2023). The study confirmed that such processes as the formation of parallel illegal markets (forums, darknet marketplaces), the creation of 'service' models (Crime-as-a-Service, Ransomware-as-a-Service), and the spread of illegal financial flows through cryptocurrencies and mixers are forming a stable and increasingly professional cybercrime ecosystem. A special place here is occupied by the affiliate programme model, where malware and infrastructure developers profit from each ransomware or successfully executed attack. Thus, the threshold of entry for new attackers is significantly lowered, leading to an increase in the total number of attacks worldwide.

A comprehensive assessment shows that, along with the emergence of criminal 'digital corporations, there is a trend toward diversifying forms of illegal online activity, from DDoS attacks to cyber espionage and compromised business communications. The latest technological advances (artificial intelligence, quantum computing, 5G networks) will inevitably become targets of further attacks, as it is in the area of advanced developments that vulnerabilities appear that have not yet been adequately protected. Consequently, cyber threats are becoming truly global in nature and pose serious risks to government institutions, businesses and individuals.

The situation requires a systemic approach to cybersecurity organization, which should include legal and regulatory aspects for current and potential threats, cooperation between different states in prosecuting cybercriminals (given the cross-border nature of cyberattacks), and the development of multi-layered defence systems covering the personal level, the corporate environment and critical infrastructures. As attackers evolve their means and methods of attack, traditional forms of anti-virus and firewall defences need to be supported by more flexible and intelligent technologies, including machine learning and real-time anomaly detection.

Thus, this study not only underscores the historical significance of computer security but also identifies new avenues for countering threats that

arise from the evolving shadow digital economy (Priyadarshini & Cotton, 2022). The scale and complexity of contemporary cyberattacks call for strengthened international cooperation, the development of integrated methods to anticipate future attack scenarios, and the cultivation of a shared cybersecurity culture (Abd El-Latif et al., 2023). Only coordinated efforts by government, the private sector, research and development organizations, and civil society can curb the exponential growth of cybercriminal activity and ensure the long-term security of the digital environment.

WORKS CITED

Abd El-Latif, A. A., Maleh, Y. E.-A., & Ahmad, S. (2023). *Cybersecurity management in education technologies: Risks and countermeasures for advancements in e-learning.* CRC Press. https://doi.org/10.1201/9781003369042

Berdiev, A. N., Goel, R. K., & Saunoris, J. W. (2024). Global cryptocurrency use, corruption, and the shadow economy: New insights into the underlying linkages. *American Journal of Economics and Sociology*, *83*(3), 609-629. https://doi.org/10.1111/ajes.12566

Clayton, R. (2019, 02 6). Report: Under the hood of cyber crime. Retrieved from https://blog.checkpoint.com/research/report-under-the-hood-of-cyber-crime/

Gaspareniene, L., Remeikiene, R., Ginevicius, R., & Skuka, A. (2016). Critical attitude towards the theory of digital shadow economy: Literature review and new foundations. *Terra Economicus*, 156-172. https://doi.org/10.18522/2073-6606-2016-14-4-156-172

Gërxhani, K., & Cichocki, S. (2023). Formal and informal institutions: understanding the shadow economy in transition countries. *Journal of Institutional Economics*, *19*(5), 656-672. https://doi.org/10.1017/S1744137422000522

Heldman, K. (2018). *Project management jumpstart.* John Wiley & Sons. ISBN: 978-1-119-47222-3

Malecki, E. J., & Moriset, B. (2007). *The digital economy: Business organization, production processes and regional developments.* Routledge. ISBN 9780415396967

Medina, L., & Schneider, F. (2019, December 12). *Shedding light on the shadow economy.* CESifo Working Paper No. 7981. https://dx.doi.org/10.2139/ssrn.3502028

Medina, L., & Schneider, F. (2021). *The evolution of shadow economies through the 21st century.* Retrieved from https://elibrary.imf.org

OECD. (2017). *Shining light on the shadow economy: Opportunities and threats.* Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/09/shining-light-on-the-shadow-economy-opportunities-and-threats_a9a92285/e0a5771f-en.pdf

Ohrimenco, S., Borta, G., & Cernei, V. (2021). Estimation of the key segments of the cyber crime economics. In *Proceedings of the 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 103–107). IEEE. https://doi.org/10.1109/PICST54195.2021.9772165

Ohrimenco, S., Borta, G., & Cernei, V. (2024). The digital world has a long shadow. In *The Elgar Companion to Information Economics* (pp. 481-504). Edward Elgar Publishing. https://doi.org/10.4337/9781802203967.00035 eISBN: 9781802203967

Ohrimenco, S., Borta, G., & Tetiana, B. (2019). Shadow of digital economics. *Problems of Infocommunications, Science and Technology (PIC S&T).* (pp. 776-780). Harkiv: IEEE. https://doi.org/10.1109/PICST47496.2019.9061545

Ohrimenco, S., Borta, G., Bazhenov, S., Bazhenova, Y., & Abrosimov, D. (2021B). Tovary i uslugi v tenevoy tsifrovoy ekonomike. *Studii naționale de securitate*, 37-55. https://doi.org/10.5281/zenodo.5236346

Ohrimenco, S., Orlova, D., & Cernei, V. (2025). Commercial secret management in terms of shadow digital economy. *Business Management, 35*(2), 64–85. https://doi.org/10.58861/tae.bm.2025.2.04

Olejnik, L., & Kurasiński, A. (2023). *Philosophy of Cybersecurity*. http://doi.org/10.1201/9781003408260

PMBOK. (2000). *Project management body of knowledge.* PMBOK. ISBN: 1-880410-25-7

Priyadarshini, I., & Cotton, C. (2022). *Cybersecurity: Ethics, legal, risks, and policies.* Apple Academic Press. ISBN 9781003187127

Schneider, Friedrich (2017) : Implausible large differences in the sizes of underground economies in highly developed European countries? A comparison of different estimation methods, Working Paper, No. 1709, Johannes Kepler University of Linz, Department of Economics, Linz. Retrieved from https://www.econstor.eu/bitstream/10419/167508/1/cesifo1_wp6522.pdf

World Economic Forum. (2025). *The Global Risks Report 2025*. Retrieved from World Economic Forum. Retrieved from https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

How to cite this article?

Style – **APA** *Seventh Edition:*

Ohrimenco, S., Manasterska, T., & Gujuman, L. (2026, January 15). The labor market in terms of the shadow digital economy. *MEST Journal, 14*(1), 191-202. https://doi.org/10.12709/mest.14.14.01.13

Style – **Chicago** *17th Edition:*

Ohrimenco, Serghei, Tatiana Manasterska, and Lucia Gujuman. "The labor market in terms of the shadow digital economy." *MEST Journal (MESTE) 14*, no. 1 (January 2026): 191-202. https://doi.org/10.12709/mest.14.14.01.13.

Style – **GOST** *R 7.0.100-2018, Name Sort:*

Ohrimenco, S., Manasterska, T., Gujuman, L. The labor market in terms of the shadow digital economy // *MEST Journal* / ed. Z. Čekerevac. – Belgrade – Toronto : MESTE, 15 Jan. 2026. – Vol. 14, No. 1. – pp. 191-202. – DOI: https://doi.org/10.12709/mest.14.14.01.13.

Style – **Harvard** *Anglia Ruskin:*

Ohrimenco, S., Manasterska, T. & Gujuman, L., 2026. The labor market in terms of the shadow digital economy. *MEST Journal*, 14(1), pp. 191-202. Available at: https://doi.org/10.12709/mest.14.14.01.13 [Accessed dd Month yyyy].

Style – **ISO 690** *Numerical Reference:*

Ohrimenco, S., Manasterska, T. & Gujuman, L. The labor market in terms of the shadow digital economy. *MEST Journal.* 2026 Jan 15;14(1): 191-202. DOI: 10.12709/mest.14.14.01.13