Practice of the implementation cyber security and financial inclusion at the micro-, macro- and global levels of the economy

Kateryna Kraus [*A]; Nataliia Kraus [B]; Olena Shtepa [C]

[A, B, C] Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska St., Kyiv, 04053 Ukraine

Received: May 10, 2022 | Revised: May 18, 2022 | Accepted: June 27, 2022

JEL Classification: H56, L86, O16.

DOI: 10.38188/2534-9228.22.2.03

Abstract

Authors presented main aspects of cybersecurity in the current context of global challenges in terms of password protection Wi-Fi network, hacking detection, external cyber threats, complex mechanisms of hacking IT systems, cyberattacks that are complex and widespread. The opinion is expressed that one of the tendencies of development of cybersecurity of Ukraine is creation of the concept and introduction of technologies of Smart Information Systems. Main results achieved should be the ability to monitor, controllable, intelligent control of the decision-making system of digital asset management, which provides high reliability and high economic performance. Authors expressed the opinion that Enabling Financial and Digital Inclusion takes place through the implementation of the following chain type: "Financial identity – Secure electronic account – Ability to save, borrow, insure – Access to global economy". Main threats to national security are named, including the inconsistency of infrastructure and modern requirements; Insufficient efficiency and level of coordination of the security and defense sector of Ukraine. Pursuing the goal of successful implementation of the Cyber Security Strategy of Ukraine, it is proposed to move on to the following steps, namely: to follow the path of creating a national cybersecurity system; increasing the effectiveness of combating threats in the military sphere; cyber protection of state electronic information resources, as well as information infrastructure; protection of the interests of the citizen, society and the state in cyberspace. Authors presented a practical example of licensing DigitalLab by businesses to enhance cybersecurity through the use of DigitalLab-Light, DigitalLab-Express, DigitalLab-Standart, DigitelLab-PRO.

Keywords: cybersecurity, financial inclusion, cyber-attacks, digitalization, financial institutions, financial technologies.

Introduction

Information, as a set of knowledge about the facts and the relationships between them, has become a strategic resource, the basis for any decision. Information systems created in public authorities and commercial structures circulate information containing classified information about the achieved potential in the field of economics, defense, science and technology, confidential information about management, economic, commercial, financial and other activities. Accordingly, information protection is a complex, knowledge-intensive and multifaceted problem in the conditions of introduction of modern information technologies, creation of distributed computer systems and communication networks, which becomes especially acute (Desyatko, 2020).

For example, in February 2017, the votes of

[*] **Corresponding author:**

[A] Cand. Sc. (Economics), Associate Professor, Department of Management, e-mail: k23k@ukr.net, ORCID: 0000-0003-4910-8330

[B] Dr. Sc. (Economics), Professor, Department of Finance and Economics, e-mail: k2205n@ukr.net, ORCID: 0000-0001-8610-3980

[C] Cand. Sc. (Economics), Associate Professor, Department of Management, e-mail: o.shtepa@kubg.edu.ua, ORCID: 0000-0003-2220-2052

more than 2 million children became public, as a result of a leak from the database of "smart toys". The records were stored in the database of the manufacturer of "smart" toys CloudPets. These toys can record and transmit messages, allowing parents to stay in touch with their children. Passwords for online access to toys were encrypted, however, in most cases they were so simple that they could be easily picked up.

In the UK, personal information of children in Aberdeen was also compromised. The data was stored on paper and was stolen from the car along with an unencrypted laptop. So, from these examples it becomes clear that today, in the first place are the problems associated with the formation and development of cybersecurity of digital entrepreneurship, using modern information and communication technologies for economic development at micro and macro levels and stabilizing social development in in general.

The World Bank, other leading financial institutions, G-20 member states, and members of the Bank for International Settlements' working groups attribute the quality and availability of financial services to financial inclusion. At the same time, main results of financial inclusion programs are not only the possibility of obtaining a wide range of financial (settlement, credit and other related) services in the digitalization of the economy by the vast majority of citizens who need and / or want to consume them, but also competitive development of new quality of digital economy, inflation (price) stability, financial system stability, poverty reduction and long-term economic growth.

The National Bank is committed to protecting consumers of financial services and is setting up a special unit to take care of these issues. This will regulate the system of disclosure of information about financial products and services.

Material and methods

Valuable in the scientific sense of the problem of financial inclusion in the digitalization of the economy are scientific works and practical research and development of such well-known scientists and inventors as V. Isaacson, N. Andrusiak (Kraus, 2019), N. Brand, J. Wales, E. Williams, O. Verniy, B. Gates, S. Didenko (Didenko, 2019), A. Desyatko (Desyatko, 2020), L. Dydinets (Dudynets, 2019), B. Elbrecht, V. Efimushkin (Yefimushkin, 2017), O. Zerniuk, A. Chaikina (Kraus, 2020), M. Iavich, N. Kraus (Kraus, 2018), T. Ledovskyi, A. Poghosyan (Pohosyan, 2017), M. Swan (Svon, 2017), A. Tapscott (Tapscott, 1995; Tapscott, 2016), E. Shcherbakova, M. Shkreb (Rashkovan, 2016).

In the light of deep digitalization, innovation and automation of production, Ukrainian economists are also actively involved in systematic research on cybersecurity, cyber-attacks, cyber threats, which take place directly at the stage of digital economy and are gaining momentum. Among them are the names of V. Groysman, V. Heitz, A. Hrytsenko, G. Karcheva (Karcheva, 2017), V. Kavetsky, Yu. Kohut (Kogyt, 2019), S. Kubiv, E. Stepanyuk (Stepanyuk, 2018), R. Lernatovych, T. Yefimenko. However, at the same time, there are a number of problems with the practice of quality implementation of cybersecurity at the micro and macro levels and the development of measures to avoid cyber threats; increasing the level of financial inclusion and the development of tools in terms of financial literacy of economic entities, the future development of finance in the digital world, remain insufficiently disclosed.

The aim of the article is to study of the basic principles of practical implementation of cybersecurity of economic entities and financial inclusion at different levels of economic aggregation in the context of digitalization and martial law. Development of practical guidelines in terms of improving business efficiency as a result of quality implementation of financial inclusion and in terms of procedural management of cyber incidents.

Introduce global aspects of cybersecurity in the current context of global challenges and

provide a good example of DigitalLab licensing by businesses to enhance cybersecurity in its operations. Finding out the features of intelligent security in the context of digitalization of business. Substantiation of the main tasks of enterprises in terms of cybersecurity.

Results and discussion

Today, cybersecurity is an extremely important issue, and the figures clearly confirm this. Yes, every 40 seconds there is a new cyber-attack. According to Cybersecurity Ventures, global losses from cybercrime in 2021 reached 6 trillion dollars, which is more than 5% of world GDP. Important aspects of cybersecurity in today's world are presented in Table 1.

Table 1. Key aspects of cybersecurity in the current context of global challenges

Aspect	Problems of practical use	Ways of protection
1	*2*	*3*
Strong and strong passwords	Using strong passwords that include lowercase and uppercase letters, characters, and numbers is correct and secure. But this is just the beginning, because even a unique and complex combination of characters is not able to protect against attackers	Two-factor authentication should be used to increase data protection
Password protected Wi-Fi networks	Any Wi-Fi network can be hacked, even with a simple password setup or external physical intervention. Typically, these passwords are created to limit the number of users on the Wi-Fi network, but attackers have access to this network and have access to all sensitive data transmitted	You should use virtual private networks (VPNs) to mask your real traffic so that it is not detected and intercepted by fraudsters
Detect system / password hacking or information leakage	It can take months or even years to realize that cybersecurity has been compromised and your computer is infected with malware	You need to regularly update your passwords and antivirus software
External cyber threats	External threats are the most serious problem for any organization, so information and cybersecurity specialists are responsible for building and constantly monitoring comprehensive security systems around the company's perimeter, servers, systems, information transmission channels and more. However, internal threats can also be dangerous and important. Simple negligence, ignorance of the basics of cybersecurity, or malicious actions can lead to sad consequences	Internal factors are the cause of almost 60% of all cyber-attacks in business, so basic knowledge in the field of cybersecurity is required not only at work, but also to protect personal information. Ongoing training on employee cybersecurity is an important solution to this problem
Sophisticated mechanisms for hacking IT systems	According to a study by Positive Technologies in 57% of cases, the main means of cyber-attacks on companies is social engineering – access to confidential information, passwords, banking data and other secure systems based on human psychology. If we talk about attacks aimed at individuals, the share of social engineering reaches 90%	To protect: do not send personal information by phone or e-mail; not to pay attention to the alleged "urgency" of the issue; clarify and verify information about who is applying, regardless of regalia; interrupt and not continue communication if there is an understanding that someone is

		urging urgent and unclear actions
Cyberattacks are complex and massive	Large companies and organizations have always been and will be the target of cybercriminals. However, criminals are interested in those who are less protected and those who are easiest to attack. According to statistics, most cases of cyber-attacks are aimed at an unprepared user who is unfamiliar with the basic rules of cybersecurity	To protect your organization from large-scale attacks and block access to its systems, you should: recognize phishing emails, ban unknown links, install software from unverified sources, download unknown files and voluntarily transfer personal data to the Internet, and more
Additional protection for smartphone	Even the most modern smartphone is not protected from cyber threats. Mobile devices have long been one of the goals of cybercriminals, because they are always interested in two goals: money or personal information	Be sure to follow the basic rules of cybersecurity when using a smartphone
Cybersecurity	Cybersecurity is an ongoing process, not an outcome	New ways of cyber-attacks appear every day, so companies should constantly conduct internal audits, analyze the existing situation in the organization and raise the level of cybersecurity education of employees

Source: Metinvest Digital, 2021.

According to Ukrainian experts, Ukraine has two scenarios for Ukraine's future economic development, which are presented in Table 2.

Table 2. Scenarios for the future economic development of Ukraine

Indexes	Baseline scenario (80%)	Optimistic scenario (20%)
1	*2*	*3*
GDP	$ 280 billion	$ 1 trillion
Employment	9 million people	14,7 million people
Productivity	↑ in 5 times	↑ in 11 times

Source: summarized by the authors.

There are two scenarios, but one way to implement them. Today, the result of the Hi-tech sector is only 4% of GDP, and according to the optimistic scenario, in 2030 the Hi-tech sector will account for 60% of GDP, while traditional sectors (finance, transport, trade, manufacturing, agriculture, etc.) will be 40% GDP.

Any new technology goes through a period of misunderstanding, then hype, recession, and only then returns to normal growth. Blockchain or bitcoin has really been "laid out" and proved a lot to humanity. For example, that an alternative reality where people create technology is possible. And it exists outside the format of corporations and state regulators, without control and public capital, and can even improve itself *(Special Edition, 2018).*

Shaping the Field of Financial Inclusion for 25 Years and the content of The Consultative Group's work to Assist the Poor (CGAP) are presented in Figure 1 and in Table 3.

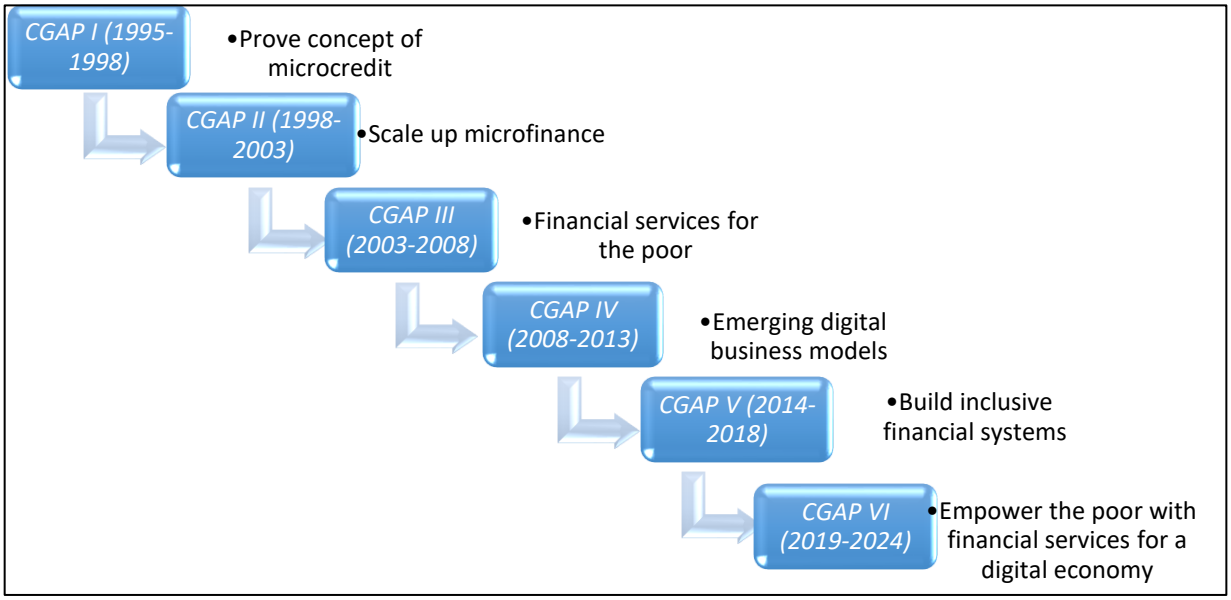

Figure 1. Shaping the Field of Financial Inclusion for 25 Years

(summarized by authors)

Table 3. The Consultative Group to Assist the Poor (CGAP)

Mission	**Microfinance: what we learned**
To make financial services meet the needs of poor people. By advancing responsible and inclusive financial systems, we help move people out of poverty, protect their gains and advance global development goals.	Poor people want to save and borrow and are credit-worthy. Concentration of successful markets in South Asia, Latin America, Eastern Europe and Central Asia and East Asia. MFLs can prosper where there is: Supportive regulatory environment; Population density; Adequate economic growth
Where it all began: Microfinance	**Mobile Money**
Roots in Bangladesh and Latin America in the 1970s Today: - 774 financial services providers - more than 115 million borrowers - gross loan portfolio of $ 96,6 billion - 99 million depositors, saving $ 64 billion - $ 16 billion under management in specialized MIVs	Mobile payments take off *M-Pesa launched in Kenya in 2007*… and spread widely across Africa and beyond. Today: - 272 deployments in90 countries - 866m registered users - $ 1,3 billion in payment processed per day - Payments a universal financial service. Data trails foundational to other services - Technology + Distribution - Changes in regulation required to enable mobile money, and to protect consumers - Future is in platforms.

Source: summarized by the authors.

E-commerce and social media, which provide impetus for mobile-based financial services, is clearly demonstrated by the example of China in Figure 2, and the case for enabling market infrastructure on the example of India is given in Figure 3.

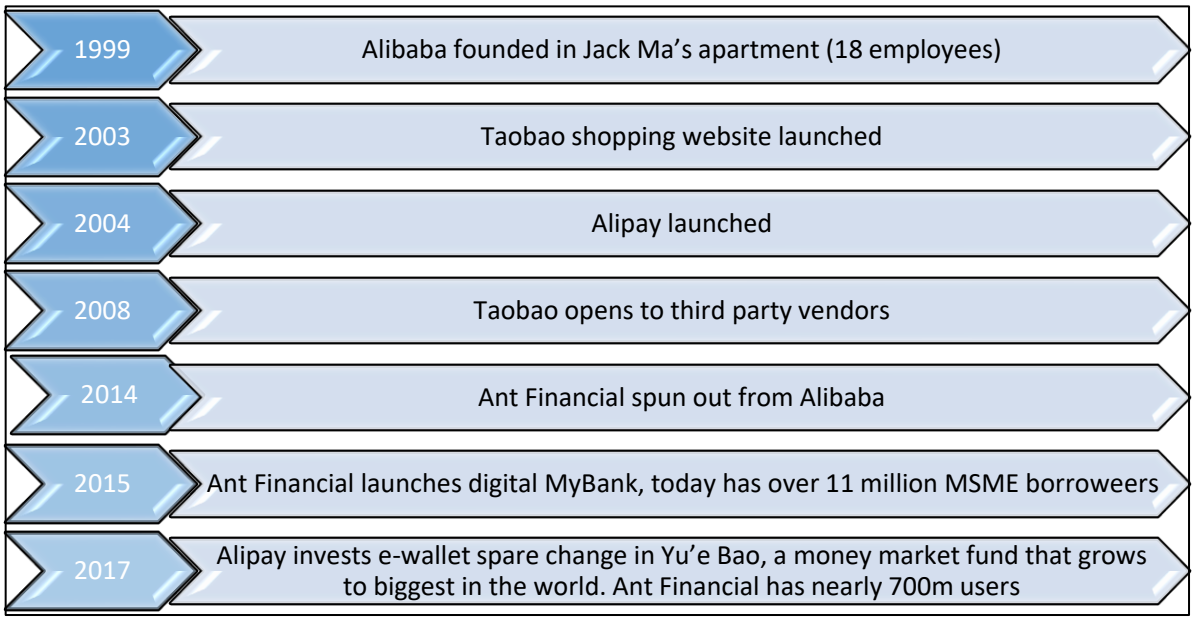

Figure 2. E-commerce and social media provide impetus for mobile-based financial services
(summarized by authors)

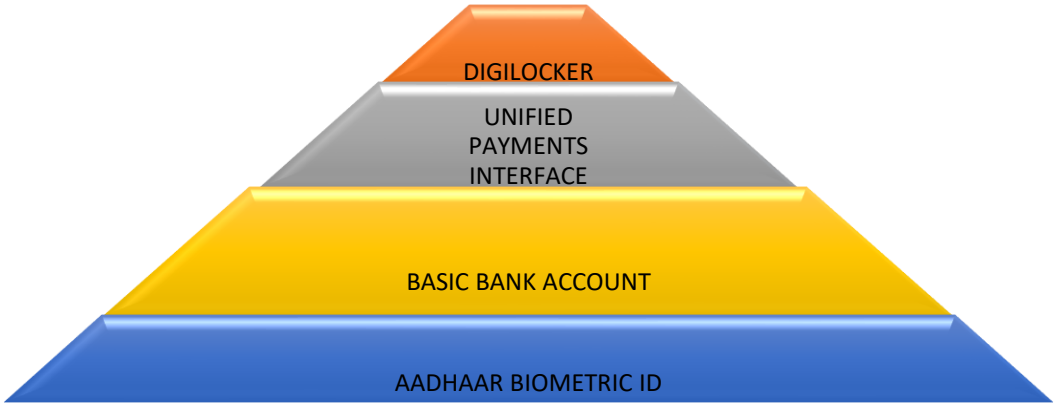

Figure 3. India stack – power of integrated market infrastructure and digital tools for citizens
(summarized by authors)

In July 2020, National Bank of Ukraine approved the Strategy for the Development of Fintech in Ukraine until 2025 – a detailed plan for the initialization in Ukraine of fintech ecosystems with affordable digital services and innovative financial services. The strategy envisages the development of the financial sector in five main areas:

- Development of financial markets;
- Strengthening financial stability;
- Introduction of innovations in the financial sector;
- Promoting macroeconomic development and economic growth;
- Expanding financial inclusion.

To a large extent, the implementation of the strategy also depends on the implementation of related digital projects. In particular, the implementation of the PSD2 European Directive, the introduction of remote identification and verification, the ability to make instant payments from account to account around the clock, strengthening the regulatory perimeter in cybersecurity and all other innovative projects of the central bank. Today, the Ukrainian market of financial technologies is the most developed in the field of payment services and microcredit.

The COVID-19 pandemic has significantly affected the growth of fintech, due to the need for social distancing and self-isolation. The total volume of digital payments in the world amounted to $ 4.1 trillion in 2019. In 2023, $ 6.7 trillion in such payments is projected. Chatbots will save banks $ 7.3 billion by 2023. Total assets under the management of digital capital management companies specializing in retail are projected to reach $ 600 billion by 2022.

As for Ukraine, according to the NBU, the total number of transactions (non-cash and cash) using payment cards issued by Ukrainian banks in the first quarter of 2020 amounted to 1.4 billion worth ₴ 920.5 billion.

Compared to the same period in 2019, the number of these transactions increased by 24.5% and the amount – by 15.6%. In terms of quantity and amount, non-cash transactions predominated in the first quarter of 2020. Thus, the number of non-cash transactions amounted to 1.2 billion (85.4% of all transactions), and the amount – ₴ 503 billion or 54.6% of the sum of all card transactions (last year, in the first quarter, the figure was 49.7%). The result of achieving the goals of the strategy should be the creation of favorable conditions for the development of all niches in this market.

Cash is a backup payment instrument in case of technical failures of traditional payment systems. Digital currencies, as an additional payment instrument, can increase the operational reliability of the payment infrastructure. The use of digital currencies is likely to make payments faster and cheaper due to the lower cost of digital currency turnover and reducing the monopolization of the payment services market. This is especially true for cross-border transfers in foreign currencies, which are quite complex and expensive.

Improving financial inclusion, i.e. public access to financial services, can be another positive consequence of the introduction of digital currencies. This requires increasing public access to digital technologies and other structural reforms that take into account the specifics of individual countries. Will society give up paper money?

Society is unlikely to give up paper money in the near future. We are likely to see a gradual decline in the use of cash, especially in developed countries, but it will continue to play a significant role for many years to come. We see examples of countries that have begun to encourage the use of cash after a significant reduction in its share in the payment turnover. This is primarily due to the function of cash as a backup payment instrument in case of technical failures of traditional payment systems.

It is easier to deliver digital currency to remote areas and in cases of natural disasters, compared to cash. In addition, the cost of securing paper money is likely to be higher than that of digital currencies.

The introduction of digital currencies will provide direct access to business and individuals to money issued by central banks, which can increase confidence in the currency in the event of a significant reduction in the use of cash. In addition, cash is a backup payment instrument in case of technical failures of traditional payment systems. Digital currencies, as an additional payment instrument, can increase the operational reliability of the payment infrastructure.

The use of digital currencies is likely to make payments faster and cheaper due to the lower cost of digital currency turnover and reducing the monopolization of the payment services market. This is especially true for cross-border transfers in foreign currencies, which are quite complex and expensive.

Improving financial inclusion, i.e. public access to financial services, can be another positive consequence of the introduction of digital currencies. This requires increasing public access to digital technologies and other structural reforms that take into account the specifics of individual countries.

Society is unlikely to give up paper money in the near future. We are likely to see a gradual

decline in the use of cash, especially in developed countries, but it will continue to play a significant role for many years to come. We see examples of countries that have begun to encourage the use of cash after a significant reduction in its share in the payment turnover. This is primarily due to the function of cash as a backup payment instrument in case of technical failures of traditional payment systems. It is easier to deliver digital currency to remote areas and in cases of natural disasters, compared to cash. In addition, the cost of securing paper money is likely to be higher than that of digital currencies.

One of the trends in the development of cybersecurity in Ukraine is the creation of the concept and implementation of Smart Information Systems. The main results achieved should be the ability to monitor, controllable, intelligent control of the decision-making system of digital asset management, which provides high reliability and high economic performance. Global distributed monitoring, protection and control systems, which are based on the technology of vector measurements with high accuracy of synchronization of spatially spaced devices, are becoming more and more widely used.

The most complete general functional and technological ideology of this concept is reflected in the definition of Smart Information Systems as the concept of "fully integrated, self-regulating and self-healing digital asset management decision-making system". The intelligent digital asset management system involves the integration of digital asset databases with new electronic communications and a holistic multi-loop decision-making system. Since such a system provides for independent decision-making by the system, an important component is the creation of an intrusion detection system as part of a holistic system (Desyatko, 2020).

Changing world presented today:

- Use of data growing exponentially, same for the collected PII;
- Adversarial machine learning and AI;
- Evolving ransomware;
- Use of cloud platforms;
- Mass collection of marketing data;
- Collection of data from children.

The marketplace is full of fragmented point solutions: infrastructure security, threat solutions, compliance tools, identity solutions, end-point security, IOT security, security management, datacenter security, information solutions. We are convinced that in the context of digitalization of the economy there is an urgent need for integration Integrate security into your platform, services, and productivity tools (Figure 4).

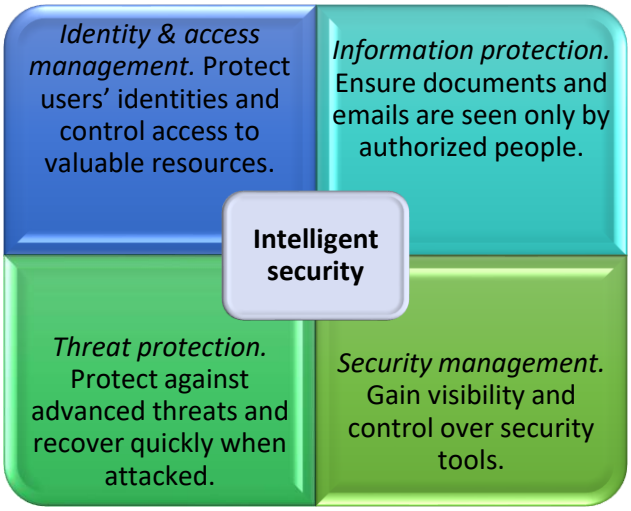

Figure 4. Intelligent security in the context of digitalization of business
(development by authors)

To get started with intelligent security:

- Begin with a customized Value Discovery Workshop;
- Calculate the expected ROI of digital transformation with our Value Calculator;

Chat with an account specialist to design your strategic approach.

The information security policy of the enterprise should consist of the following sections:

- The purpose of the document, the main tasks of information security of the business entity;
- Scope of the Company's Information Security Policy;
- Role and responsibility for information

security;

- The purpose of ensuring information security at the enterprise;
- Principles (rules, requirements) of information security of the enterprise;
- List of interrelated documents, including legislative and other normative legal acts of Ukraine, international, national standards on information security and protection against cyber threats;
- Revision of the Information Security Policy of the enterprise (which department, service, officials review the Policy, who is responsible for the changes in the Policy, who is responsible for the support of the Policy);
- History of changes in the document (Kogyt, 2019).

Creating a high-quality, reliable, with a high degree of protection of cloud infrastructure from cyberattacks, we will try to summarize below.

State regulation of cyberspace protection processes in Ukraine is an integral part of ensuring information security of the state. At the beginning of 2020, the main legal framework for the implementation of state policy to ensure the protection of cyberspace and cybersecurity was formed at the level of the legal system of Ukraine.

However, the administrative and legal regulation of state protection of cybersecurity is characterized by certain gaps. In particular, it is the slow reform of regulatory frameworks for cybersecurity, lack of regulation of aspects of administrative interaction between the subjects of the national cybersecurity system, lack of clear regulation of major risks and threats to the national cyberspace of Ukraine (Desyatko, 2020).

The Cyber Security Strategy of Ukraine is a long-term planning document that identifies threats to Ukraine's cybersecurity, priorities and directions of Ukraine's cybersecurity in order to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and state (Law of Ukraine, 2018). The purpose of the Cyber Security Strategy of Ukraine is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state (Decree of the President of Ukraine, 2016). We present some of the main threats to the national security of Ukraine and the security and defense sector in Table 4.

Table 4. Entities involved in cyber defense and implementation of the Cyber Security Strategy of Ukraine

Steps aimed at implementing the Cyber Security Strategy of Ukraine	creation of a national cybersecurity system; increasing the effectiveness of combating threats in the military sphere; cyber protection of state electronic information resources, as well as information infrastructure; protection of the interests of the citizen, society and the state in cyberspace.
Main threats to national security	non-compliance of infrastructure and modern requirements; Insufficient efficiency and level of coordination of the security and defense sector of Ukraine.
Security and defense actors	Ministry of Defense of Ukraine (repulse of military aggression in cyberspace); State Service for Special Communications and Information Protection of Ukraine (formation and implementation of state policy); Security Service of Ukraine (prevention and detection of crimes); National Police of Ukraine (ensuring the protection of civil rights and freedoms); National Bank of Ukraine (formation of cybersecurity requirements in the banking sector); intelligence agencies (implementation of intelligence in cyberspace).

Source: compiled by authors based on sources (Law of Ukraine, 2018; Decree of the President of Ukraine, 2016).

We are deeply convinced that industry standards for cybersecurity should be developed and approved at the state level. It is important to create conditions for effective cooperation between the state and other economic entities in order to establish reliable data collection on cybersecurity incidents at the level of large and medium-sized enterprises. Today, both individuals and businesses are not always able to say with certainty that they are dealing with information leakage or other cybersecurity violations.

A practical example of DigitalLab licensing by businesses to enhance cybersecurity is presented in Table 5.

Table 5. Licensing DigitalLab by businesses to enhance its cybersecurity *(compiled by authors)*

Name	Storage	Possibilities of expansion
1	*2*	*3*
DigitalLab-Light package	Server data processing module. Server license for up to 5 simultaneous connections of APM engineer and APM laboratory assistant clients. APM Engineer – 1 pc. APM laboratory assistant – 1 pc.	APM engineer. APM laboratory assistant. APM viewer.
DigitalLab-Express package	Server data processing module. Server license for up to 10 simultaneous connections of APM engineer and APM laboratory assistant clients. APM Engineer – 2 pc. APM laboratory assistant – 3 pc.	Server module for data collection from equipment. Server package of functional extensions for laboratory management. Server package of functional extensions for quality control of research results. Server package of functional extensions for statistical control. Server module integration with adjacent AC class ERP / MES / MDM. Server package of functional extensions for managing the certification of marketable products. APM engineer. APM laboratory assistant. APM viewer. Web browsing APM.
DigitalLab-Standart package	Server data processing module. Server package of functional extensions for laboratory management. Server license for up to 20 simultaneous connections of APM engineer and APM laboratory assistant clients. APM Engineer – 4 pc. APM laboratory assistant – 6 pc.	Server module for data collection from equipment. Server package of functional extensions for quality control of research results. Server package of functional extensions for statistical control. Server module integration with adjacent AC class ERP / MES / MDM. Server package of functional extensions for managing the certification of marketable products. APM engineer. APM laboratory assistant. APM viewer. Web browsing APM.
DigitelLab-PRO package		All components can be included, with any number of customers.

It is necessary to pay attention to the increase in the receipt of phishing emails in the information space of society, containing malicious software, the government team

responding to computer emergencies of Ukraine CERT-UA basic rules of cyberhygiene:

- Be especially careful when opening e-mail attachments from unknown people. When working with mail, you need to check attachment extensions and not open files even with secure extensions;
- Do not follow unknown links or download files that have potentially dangerous extensions (such as .exe, .bin, .ini, .dll, .com, .sys, .bat, .js, etc.) and even secure ones (such as: .docx, .zip, .pdf), because vulnerabilities, macros and other threats can be used;
- Carry out outreach work with subordinates who have access to the Internet and work with mail agents;
- Use licensed / legalized operating systems, other software products, update them in a timely and systematic manner;
- Use anti-virus software with heuristic analysis technology;
- Perform regular data backup, save backups on external media (SSD, HDD, etc.) and configure the "system restore" function;
- Deny access to the Internet to programs that could potentially be used by attackers, if it does not affect the stability of their work *(Desyatko, 2020; Decree of the President of Ukraine, 2016; Law of Ukraine, 2020).*

Technologies that will increase business efficiency are the following:

1. Optimization of business processes: control of production and people (modules and sensors), detection of counterfeit products using blockchain, simplification of communication via VR and AR.
2. Cost management (cloud services, Internet of Things): accounting, logistics, quality, personnel (robotics and automation).
3. New solutions with big data: individual approach to the client, personal sales and advertising, cognitive learning systems, neobanking, p2p systems, solutions at the crossroads of industries and professions.

Developmental Process for the National Financial Inclusion Strategy Lessons and Learned – NFIS Implementation are presented in Figure 5 and Figure 6.

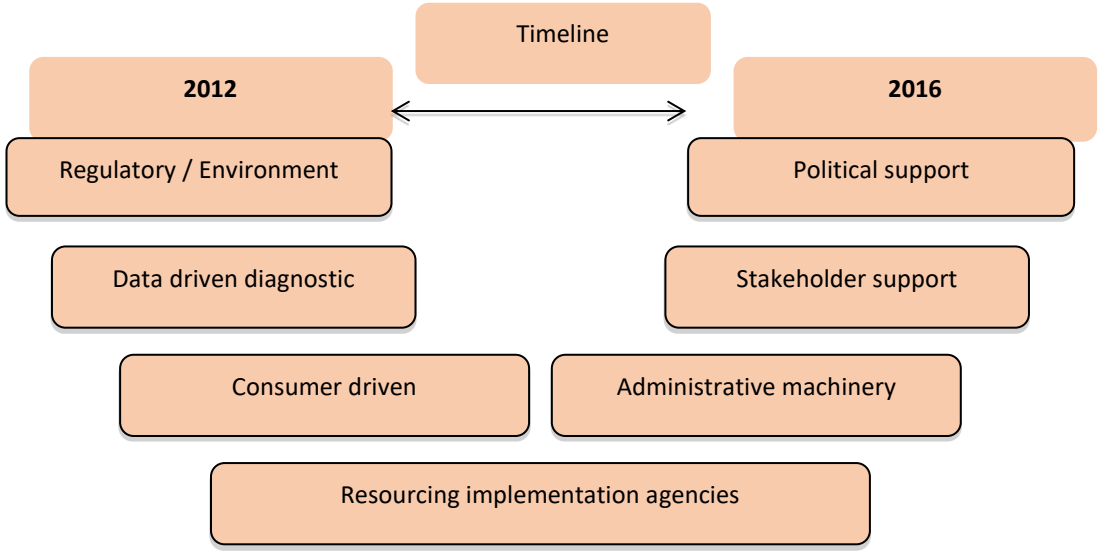

Figure 5. Developmental Process for the National Financial Inclusion Strategy
(compiled by authors)

Financial well-being calls for an integrated and multi-dimensional approach. So, financial well-being depends on:

- Ensuring a deep and liquid markets (financial inclusion);
- Formal, functioning, and regulated institutions (financial consumer protection);
- Consumers aware of the needs, the costs, and risks (financial literacy).

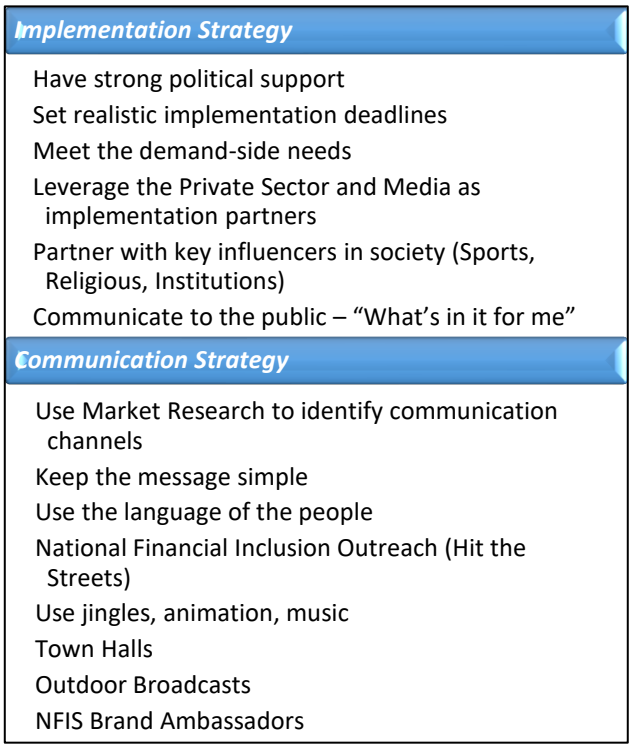

Figure 6. Lessons Learned – NFIS Implementation
(compiled by authors)

OECD's key focus and mandate has been to look at how financial education can improve the financial literney of consumers / investors and in turn lead them to better financial well-being. OECD/INFE definition of financial literacy: combination of awareness, knowledge, skill, attitude and behavior necessary to make sound financial decisions and achieve individual financial well-being. OECD's work covers all three elements:

1. Financial Literacy and Education – G2o/OECD INFE report on digitalization, consumer protection and financial literacy (2017);

2. Financial Consumer Protection – G2o/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age (2018);

3. Financial Inclusion – G2o High-Level Principles for Digital Financial Inclusion (YouTube, 2015).

Enabling Financial and Digital Inclusion відбувається шляхом реалізації наступного ланцюга типу: "Financial identity – Secure electronic account – Ability to save, borrow, insure – Access to global economy".

The OECD is working with countries on National Strategies and their implementation is shown in Figure 7.

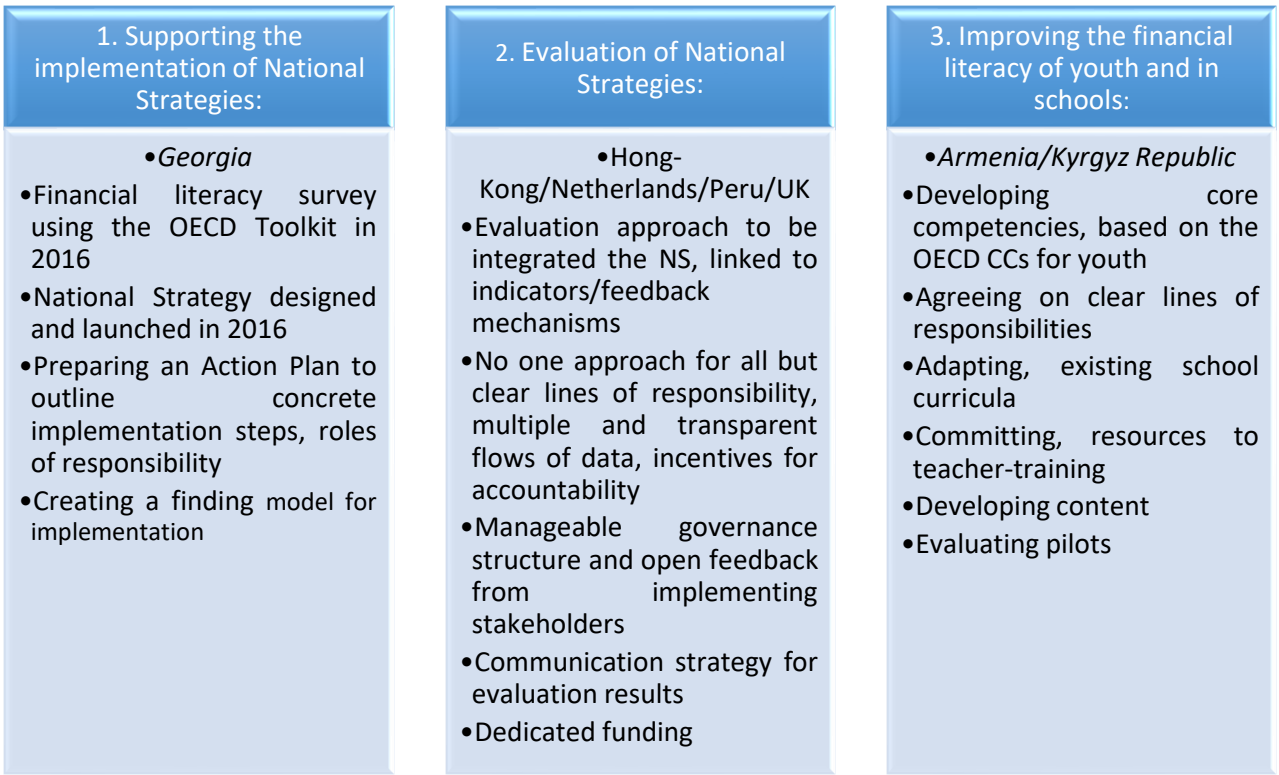

Figure 7. OECD is working with countries on National Strategies and their implementation
(compiled by authors)

How to build financial literacy shown in Figure 8.

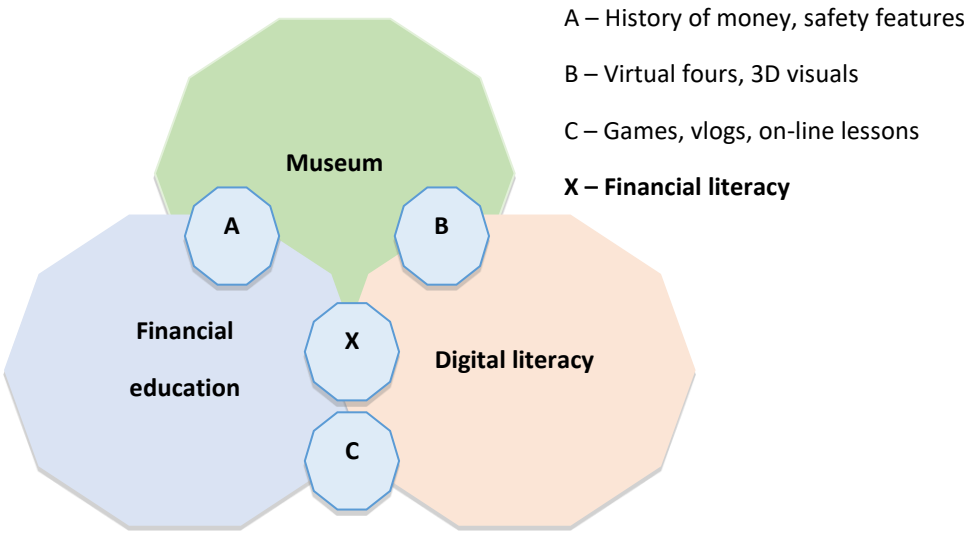

Figure 8. Scheme of building financial literacy
(compiled by authors)

In general, the future of finance in the digital world, which involves the emergence of new qualities of financial literacy, is possible through the following vectors of development, namely:

1. The finance factory. Transactions will be touchless as automation and new technologies reach deeper into finance operations. In the years ahead innovations will continue apace, creating opportunities to radically simplify processes. There will be a premium on talent that understands technology and business. These professionals are already in short supply.

2. The role of Finance. With operations automated, Finance will double down on business insights and service. Success is not assured due to high expectations from customers. The skills required by finance professionals will change, likely dramatically, as new combinations of technology and human workforces permeate the workplace.

3. Finance cycles. Finance goes real time. Periodic reporting will no longer drive operations and decisions – if it ever did. The old distinction between operational and analytical data begins to disappear. You're not forecasting once a month or quarterly. It's all happening in real time.

4. Self-service. Self-service will become the norm. Finance will be uneasy about this. Activities ranging from budget queries to report production and more will be automated. As that future unfolds, data in spreadsheets will be replaced by visually rich information that is intuitively accessible and easy to use. With growing expectations for responsiveness and quality from Finance, getting self-service right is paramount.

5. Operating model. New service-delivery models will emerge as robots and algorithms join a more diverse finance workforce; think about the integration of freelancers, gig workers, and crowds. Automation provides a new lever for managing costs, one that gives finance organizations the opportunity to reevaluate how they're organized, where work gets done, and what kinds of processes no longer require human intervention.

6. ERP. Finance applications and micro-services will challenge traditional ERP. New players enter the ERP space with specialized applications and micro-services that sit on top of – and integrate with – ERP platforms. You'll be able to drastically reduce the complexity and cost of technology, without sacrificing functionality.

7. Data. The proliferation of APIs will drive data standardization, but it won't be enough. Many companies will still struggle to clean up

their data messes. Few companies are doing the hard work needed to align and integrate data. Those hoping for a silver bullet to solve their data problems will be disappointed.

Big data management is a function of the top management of the organization, so its role should change *(Special Edition, 2018)*:

First, develop leadership within the company. Businesses are successful not just because they have more data. Market leaders are those who have teams of leaders with their own vision, ability to set clear goals and determine what to consider a success for this particular business.

Second, it is a talent management skill. Statistics obtained with the help of big data are important, but in themselves, without interpretation by talented people who know how to work with it, it will not give exciting expected results.

Third, working with big data should be part of the organization's culture. If top management asks not "what do we think about it?", but "what do we know?", - the number of decisions made by intuition will be reduced. This means that the data will not be "adjusted" to the decisions made, but vice versa. Absolutely crystal-clear sobriety, skepticism and independence in formulating arguments to confirm or refute hypotheses, three lines of defense and assessment of the impact of potential errors – these are the skills and approaches to learn from an auditor to work effectively with big data and get on the road revolution in trust management. Decisions made on the basis of big data are always more accurate and progressive.

8. Workforce and workplace. Employees will be doing new things in new ways, some of which will make CFOs uncomfortable. Finance talent models are evolving quickly, with a premium placed on data scientists, business analysts, and storytellers. Important qualities include a strong customer service orientation, flexibility, and good collaboration skills – in addition to the technical capabilities needed for specific jobs.

Conclusions

In conclusion, we note that the leading fight against cybercrime is:

- Investigations, forensics, and analytics;
- Machine learning, AI, and data visualization;
- Public and private partnership;
- Creative legal standings.

Main tasks to prevent cyber threats in martial law, in our opinion, should be: protection of personal data (intensive exchange and use of large data flows reduces the degree of confidentiality of information used, which creates digital threats); security of commercial information systems; security of information systems of state structures; protection of the working environment, technologies and tools.

The problem of effective cybersecurity at the micro and macro levels needs to be addressed comprehensively and requires coordinated action at the national, regional and international levels to prevent, prepare, respond to and recover from incidents by government, the private sector and civil society. Given the current socio-political and informational challenges of defining political, scientific, technical, organizational and educational areas, the construction of an effective cyber defense system in the framework of integrated cyber threat management will contribute to the formation of an effective mechanism for countering threats in cyberspace, anticipating the dynamic changes taking place in cyberspace, developing and implementing effective means and tools for a possible response to aggression in cyberspace, which can be used as a means of deterring military conflict and cyber conflict (Desyatko, 2020).

Methods and means of protection still remain passwords to files; PGP encryption; server encryption. Digital way of life, the introduction of new information programs and digital technologies, the problems of big data analysis, the changing technological age, the emergence of blockchain technology, the Internet of Things are forcing companies to treat their own human resources and knowledge assets differently.

References

Business and Art Ambassadors of Ukraine (2018). Special Edition Kyiv International Economic Forum "Destinations", no. 8.

Cybersecurity: myths and reality (2021). Metinvest Digital, from 30 November 2021. URL: https://metinvest.digital/page/k-berbezpeka-m-fi-ta-realn-st?fbclid=IwAR1MKGMXbhAyDs8vqZ0Qezf9W7v-k2-cgwol6LuJ2uKiRJo2vZhOZjEoX10 (assessed 4 May 2022).

Desyatko, A.M. (2020). Cyberhygiene. Cybersecurity. State security. Kyiv: KNTEU.

Didenko, S. (2019). Financial inclusion: how society affects economic growth. UA.NEWS, from 13 June 2019. URL: https://ua.news/ua/finansova-inklyuziya-yak-suspilstvo-vplyvaye-na-ekonomichne-zrostannya/ (assessed 5 May 2022).

Dudynets, L.A., Vernii, O.Ye. (2018). Financial inclusiveness and its determinants. Economics and management of the national economy, vol. 2 (130). 8–13.

Karcheva, H.T., Lernatovych, R.Ya., Kavetskyi, V.Ya. (2017). The use of blockchain technology as a factor in improving the efficiency of the financial sector. Banking, no. 2. 110–119.

Kogyt, Yu.I. (2019). Cybersecurity of digital economy for business owners. Kyiv: SIDCON Consulting Company LLC.

Kraus, N., Andrusiak, N., Savchenko, A., Iavich, M. (2019). Practices of Using Blockchain Technology in ICT under the Digitalization of the World Economy. Proceedings of the International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019) co-located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019) Lviv, Ukraine, November 29. URL: http://sunsite.informatik.rwth-aachen.de/ftp/pub/publications/CEUR-WS/Vol-2588.zip (assessed 10 May 2022).

Kraus, N., Kraus, K. (2018). Digitalization in the minds of the institutional transformation of the economy: basic warehouses and tools for digital technologies. Intellect of XXI century, no. 1. 211–214.

Kraus, N., Zerniuk, O., Chaikina, A. (2020). Construction enterprises innovating activities on the basis of Industry 4.0 and "Deep" digital transformations. Proceedings of the 2nd International Conference on Building Innovations (ICBI 2019). Lecture Notes in Civil Engineering, Switzerland, Cham: Springer, vol. 73, Chapter 54. 49–55. URL: https://doi.org/10.1007/978-3-030-42939-3_61 (assessed 8 May 2022).

On National Security of Ukraine: Law of Ukraine from 21 Lune 2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (assessed 7 May 2022).

On the basic principles of cybersecurity in Ukraine: Law of Ukraine from 24 Octovber 2020, 912-IX, Document 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (assessed 8 May 2022).

On the decision of the National Security and Defense Council of Ukraine (2016): Decree of the President of Ukraine from 27 January 2016 "About the Cyber Security Strategy of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11 (assessed 5 May 2022).

Pohosyan, A.M. (2017). Innovative payment instruments in digital economy. Scientific notes of young researchers, no. 3. 63–67.

Rashkovan, V., Shkreb, M. (2016). How to beat financial illiteracy. DELO.UA, from 29 July 2016. URL: https://delo.ua/econonomyandpoliticsinukraine/kak-pobedit-finansovuju-bezgramotnost-320669/ (assessed 7 May 2022).

Stepanyuk, Ye. (2018). From slogans to action. Why financial inclusion. LIGA.FINANCE. URL: https://finance.liga.net/ekonomika/opinion/ot-lozungov-k-delu-zachem-nujna-finansovaya-inklyuziya (assessed 9 May 2022).

Svon, M. (2017). Blockchain: schematic of new

economy. M.: Olymp business.
Tapscott, D. (1995). Digital economy. Promise and peril in the age of networked intelligence. McGraw-Hill, New York.
Tapscott, D., Tapscott, A. (2016). The blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin Books.
World Bank Group: Financial Inclusion – A Foothold on the Ladder toward Prosperity? (2015). YouTube. URL: https://www.youtube.com/watch?v=4jH7A0LORGQ (assessed 9 May 2022).
Yefimushkin, V.A., Ledovskikh, E.N., Shcherbakov, E.N. (2017). Infocommunication technological space of the digital economy. T-Comm: Telecommunications and transport, vol. 11, no. 5. 15–20.