**Kańduła S.** − professor Department of Public Finance;
**Przybylska J.** – ph. d., assistant professor Department of Public Finance Poznań University of Economics and Business, Poznań, Poland

# Internal Audit of the National Interoperability Framework as a Tool for Assessing Information Security in the Conditions of Economy 4.0

**The problem of information security in the conditions of the economy 4.0.** In economy 4.0 we are dealing with the widespread use of the so-called general purpose technology: computer, internet and smartphone. They are characterized by ubiquity, i.e. the ability to spread to all sectors of the economy, continuous improvement and dynamism of development, and the ability to intensively stimulate innovation in many areas of the economy and society [1]. They are also the basis on which new inventions and innovations are built up at a rapid pace. Some of them show enormous transformative potential and transform themselves into technologies of wide application over time. According to Śledziewska and Włoch [2], these are the so-called intensifying technologies, which are the foundation of economy 4.0. The authors included artificial intelligence, robotization, Internet of Things, cloud technologies and blockchain. Economy 4.0 and the changes related to it occur simultaneously in all its areas, including public administration [3]. Key technologies of the economy 4.0 are shown in Figure 1.

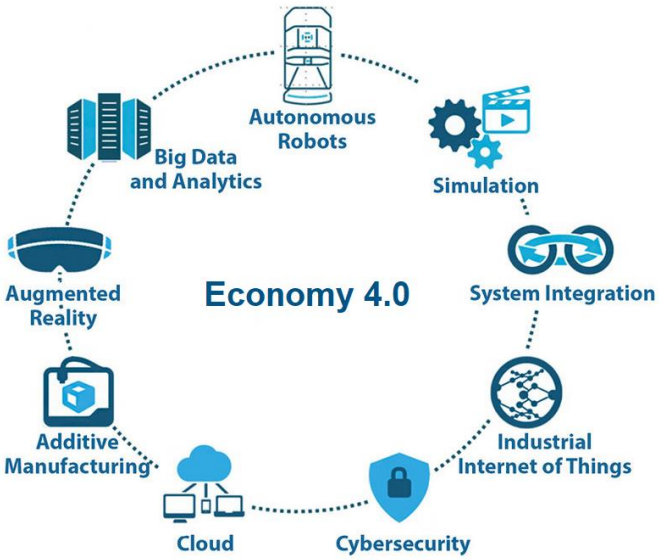


**Fig. 1.** *Key technologies of the economy 4.0*
*Source:* own elaboration based on [4].

These technologies bring new areas of cyberattacks [5]. In the conditions of economy 4.0, it is of special importance to ensure the security of information transferred between individual participants in the social and economic life. This security is an element of the financial security of the state, generally understood as the lack of threats in the sphere of public and private finances. The importance of this issue increases when the information provided concerns the so-called sensitive or confidential data. Therefore, modern states are faced with the task of creating a framework for the functioning of entities, including public entities, in a manner ensuring information security.

**National Interoperability Framework (NIF) – minimum requirements for information security in the conditions of the digital economy.** The National Interoperability Framework (NIF) sets out the minimum requirements for public registers and the exchange of information in electronic form, as well as minimum requirements for the ICT systems in which the information is collected.

The aim of NIF is, inter alia, to determine the methods of data exchange between IT systems used for public tasks, adapting these systems to the needs of disabled people and ensuring the security of these systems. In this article, we will omit the first two aspects and deal only with safety, because it is in this area that it is obligatory to perform an audit at least once a year, referred to in short as NFI audit.

According to the NIF guidelines, each entity performing public tasks is obliged to implement the Information Security Management System (ISMS). The legal regulations specify in detail the requirements that an ISMS should meet. The entity performing public tasks must develop and implement an information security management system that will ensure the confidentiality, availability and integrity of information, taking into account such attributes as authenticity, accountability, non-repudiation and reliability. This system must also be monitored and improved.

The management of a public entity must ensure the conditions for the implementation and enforcement of many activities within the NFI to ensure information security. The first of these activities, of a very general, but at the same time superior, nature is keeping the internal regulations in force in the unit up-to-date. Another issue is keeping the inventory of equipment and software used for information processing up-to-date. The unit should also carry out periodic risk analysis of the loss of integrity, availability or confidentiality of information and taking actions to minimize this risk, according to the results of the analysis. Actions should also be taken to ensure that persons involved in the information processing process have appropriate powers and participate in this process to an extent that is adequate to their tasks and obligations aimed at ensuring information security. Persons involved in the information processing process should be provided with training, covering such issues as: information security threats, the effects of information security breaches, including legal liability and the use of information security measures, including devices and software minimizing the risk of human errors.

The entity performing public tasks should also protect the processed information against theft, unauthorized access, damage or interference. This protection is considered to be provided by: monitoring access to information, activities aimed at detecting unauthorized activities related to information processing, as well as providing measures to prevent unauthorized access at the level of operating systems, network services and applications. The unit should also establish basic rules ensuring safe work in mobile processing and remote work, as well as securing information in a way that prevents its disclosure, modification, deletion or destruction by an unauthorized person. The service contracts signed with third parties should contain provisions guaranteeing an appropriate level of information security.

An appropriate level of security should also be ensured in ICT systems. In particular, you should take care of updating the software, minimize the risk of losing information as a result of a failure, protect against errors, loss, unauthorized modification, use cryptographic mechanisms in a manner adequate to threats or legal requirements, ensure the security of system files. After noticing undisclosed vulnerabilities of ICT systems to the possibility of a security breach, actions should be taken immediately to eliminate these vulnerabilities. In the event of information security breach incidents, the unit is obliged to immediately report these incidents, which is to enable quick corrective actions [6].

**Internal audit of NFI.** Pursuant to the guidelines contained in the provisions of law, the entity performing public tasks is obliged to ensure periodic internal audit in the field of information security at least once a year. It is worth clarifying here that the minister responsible for administration and digitization clarified that internal audit is an audit carried out by a unit for internal needs, not necessarily by people from within the organization (internal audit department). At the same time, the need for independence of the audit unit is emphasized. Therefore, such an audit can be commissioned to companies or external persons. Preferred to perform audit tasks are specialists with ISO 27001 lead auditor certificates, which is related to the fact that the information security system is considered to meet the minimum requirements if it was developed on the basis of the Polish Standard PN-ISO/ IEC 27001. Establishing security, management risk and auditing are carried out on the basis of other standards, in particular: PN-ISO/IEC 17799 – for establishing security, PN-ISO/IEC 27005 – for risk management and PN-ISO/IEC 24762 – for recovery post-disaster information technology as part of business continuity management.

Due to very limited budgets, it is difficult to require public sector entities to implement the ISO 27001 standard, or to train and hire their own representatives maintaining ISMS. The implementation and auditing of the information security system is most often limited to the verification of 14 requirements specified in legal regulations and described in the previous section of this study.

***Sources and literature***


1. Cantner U., Vannuccini S. A new view of general purpose technologies. *Jena Economic Research Papers*, 2012. T. 6. Nr 54. URL: https://www.econstor.eu/bitstream/10419/70135/1/726781037.pdf
2. Śledziewska K., Włoch R. Cyfrowa gospodarka. Jak nowe technologie zmieniają świat. Warszawa: Wydawnictwo Uniwersytetu Warszawskiego, 2020.
3. Oleśków-Szłapka J., Przybylska J. Elektroniczna administracja – niezbędny element innowacyjnej gospodarki. *Zarządzanie – zasoby, ich dobór i sposoby wykorzystania/*red. M. Fersch, K. Grzybowski, A. Stachowiak. Poznań: Wydawnictwo Politechniki Poznańskiej, 2008.
4. Kaliczyńska M. Kluczowe technologie przemysłu 4.0. 2018. URL: https://automatykaonline.pl/Artykuly /Przemysl-4.0/Kluczowe-technologie-Przemyslu-4.0 (accesed: 03.10.2020).
5. Kańduła S., Przybylska J. Cybersecurity in local government: essence, tasks and threats. Conference: "Цифрова трансформація фінансового сектора економіки". 2020. URL: https://www.researchgate.net/ publication/344172548_cybersecurity_in_local_government_essence_tasks_and_threats
6. Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. W sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, t. j. DzU z 2017 poz. 2247.



**Кисличко К.** − студентка

Науковий керівник: к. е. н., доц.
Г. Кошельок
Одеський національний економічний університет, м. Одеса, Україна


## Фінансова безпека підприємства та шляхи її забезпечення

Поняття фінансової безпеки було введено у кінці двадцятого століття і пояснювалося як забезпечення умов збереження комерційної таємниці та інших секретів підприємства. Сучасні нестабільні політичні та економічні умови змусили подивитися набагато ширше на проблему фінансової безпеки підприємств. Стало поширюватися думка, що її зміст показує стан підприємства, що забезпечує здатність протистояти несприятливим зовнішнім впливам. Так, фінансову безпеку визначають як захищеність діяльності фірми від критичних впливів зовнішнього середовища, а також як здатність швидко усунути можливі загрози або пристосуватися до вже сформованих умов, які не впливають негативно на діяльності самого підприємства.

В умовах нестабільної економіки, підприємству в ході свого розвитку необхідно забезпечувати захист своїх фінансових інтересів для того, щоб домогтися збереження свого становища на ринку і отримувати максимально можливий прибуток. Основний принцип збереження фінансової безпеки підприємства – це здійснення контролю і балансування доходів і витрат господарюючого суб'єкта [1, 131].

Головними загрозами фінансової безпеки є:

1) макроекономічні проблеми:

− тривала економічна криза, уповільнений вихід з нього;

− скорочення ресурсів в економічній системі для виходу з фінансової кризи і успішного проведення подальших перетворень;

− погіршення платоспроможності населення;