Measurements infrastructure Vol. 4 (2022) MI_019_120122 https://doi.org/10.33955/v4(2022)-019

Information security system structural modelling concept of digital process-oriented enterprise

Tupkalo Vitalii [1], Cherepkov Serhii [2]

[1] Kyiv Institute of Intellectual Property and Law of National University Odesa Law Academy, Ukraine
[2] SE «Ukrmetrteststandart», Ukraine

E-mail: tvn.prof@gmail.com

Abstract

The authors vision of the information security system structural model of digital process-oriented enterprise is based on analysis of existing «information security» and its components, «cyber security» and «network security» concepts. Model is based on complex causal-consequential chains character of two processual authors models: «enterprise business value creation chain» and «process management pyramid». The enterprise business value creation chain is determined as a logical sequence of digitalized technological business processes (TBP) of business value creation chain: customer/consumer engagement, production organization, goods production/services provision, goods/services sales. Herewith, «enterprise created business value» concept means the complex of two target production results: produced goods/services in terms of value for customer and sales revenue received on the seller bank account is value for the enterprise. Office automation systems (OAS) in all levels of the enterprise process management pyramid are used as an instrument for information collecting and processing and primary accounting data submitting from each technological business process in the value creation chain and analytical management data from managers personal business processes. This system is a corporate enterprise portal having an Internet connection. Herewith, «enterprise process management pyramid» concept is considered a digital organizational management structural model for the process-oriented enterprise. The structure model is a hierarchical system of managed by known PDCA (plan – do – check – act) management cycle internal and interrelated functions of each manager and lower (adjacent) level directly subordinate managers whose aim is managerial decisions production for directly subordinate executors. Concerning digitalized process-oriented enterprise management model, a vision of possible internal accidents and enterprise automated management system database hackers distortions model is created. Authors proposed «informational security of digital enterprise» concept variant is based on these two models components analysis.

Published
20.11.22

Keywords: informational security, informational security of enterprise, digital enterprise, digitalized enterprise management model.

1. Introduction

Problem statement. Digital economy as «Industry 4.0» concept [1] becomes a new driver for the economy and society development. Methodology for modern enterprises digitalization creation becomes urgent, taking into account this modern necessity. The methodology is determining the basis for digital economy practical implementation in all extensive expressions (regional and worldwide) [2, 3]. This causes the new problem of digital enterprise informational security in turn.

Measurements infrastructure Vol. 4 (2022) MI_019_120122 https://doi.org/10.33955/v4(2022)-019

2. Main body

Latest sources and publications research. Many publications exist in the general problem context of informational security ensuring in various organizational structures. Authors of publications propose definitions of «informational security» term and its «cyber security» and «network security» components [4-11]. Practically, these concepts are considered separately from each other and do not provide a systematic (comprehensive) idea of ways to solve the informational security ensuring problem of digitalized organizational structures within the interrelation chain of concepts. Though, a complex analysis of those sources considers that authors should agree with the authors of [4] concerning the mentioned chain (Fig.1).

Herewith, the model concepts interpretation in Fig.1 may be the following:

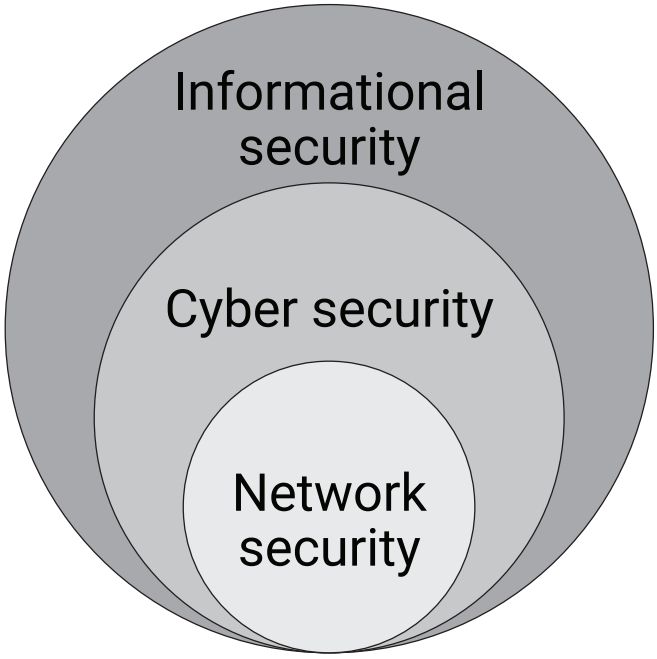

Fig. 1. *Interrelation chain of «informational security», «cyber security», and «network security» concepts* [4]

1. *Informational security* is information protection from unauthorized access, use, disclosure, distortion, alteration, research, recording, or destruction. This comprehensive concept can be applied regardless of the possible data form used.

2. *Cyber security* is human vital interests, society, state, and separate organizations (enterprises) protection when using the informational digital communicative environment (cyberspace), existing and potential threats to these interests prevention and neutralization in cyberspace.

3. *Network security* is a component of «cyber security» concept characterizing activity or process of global and local telecommunication networks protection from unauthorized access from third parties (hackers) aiming to infringe data storage and effective functioning of the whole network.

It should be mentioned that the modern tendency of enterprise transition to the process-oriented management system should be considered within the problem context relevance for informational security ensuring for various organizational structures [12-14]. Publications analysis demonstrates the absence of accent on enterprise informational security ensuring (*research subject*) necessity in terms of process-oriented digitalized informational management model (*research object*). Thus, *the research object* is out of attention.

Unsolved part of the general problem. Considering the above, comprehensive research on the information security structural model of digital process-oriented enterprise development is necessary.

The research goal. Authors conceptual vision of informational security system structural modelling of digital enterprise in terms of its process-oriented digitalized informational management model development is based on a critical analysis of existing «information security» and its components: «cyber security» and «network security» concepts.

Research results. According to the set goal, formed in a professional environment interrelation chain of «informational security», «cyber security», and «network security» concepts should be considered first (Fig. 1) [4].

The following definition of «enterprise process-oriented digitalized informational management model» (*research object*) concept is proposed.

Measurements infrastructure Vol. 4 (2022) MI_019_120122 https://doi.org/10.33955/v4(2022)-019

Definition 1. Digital enterprise is the organization using informational technologies (IT) for all activity spheres according to the technological business process (TBP) system (chain) model of enterprise value creation: consumer attraction, production organization, goods production/providing services goods/services sales. The office automation systems (OAS) in all levels of the enterprise process management pyramid are used as a tool for collecting, processing, and presenting primary accounting data from the technological processes (TP) of each TBP and analytical managerial data from personal case processes (CP) by managers. All OASs are consolidated into a corporate enterprise portal having an Internet connection. Herewith, «enterprise created business value» concept means the complex of two target production results: produced goods/services in terms of value for customer and sales revenue received on the seller bank account is value for enterprise [13].

According to this definition, digital management structured by management levels of process-oriented model of the enterprise (digital process management pyramid) is presented in Fig. 2. Three-level, P. Drucker management model, is the basis for authors model development [15].

According to Fig. 2 model, the corporate OAS network as an automated cyber security system (ACSS) of enterprise development component can be confirmed as a separate four-level OASs network complex. Those level networks may be developed according to the ACSS management level as follows:

- general managers OASs – general director, supervisory board members, etc.;
- deputy directors for economic activity types, which are centers of strategic responsibility OASs (commercial director, production director, financial director, organizational development director);

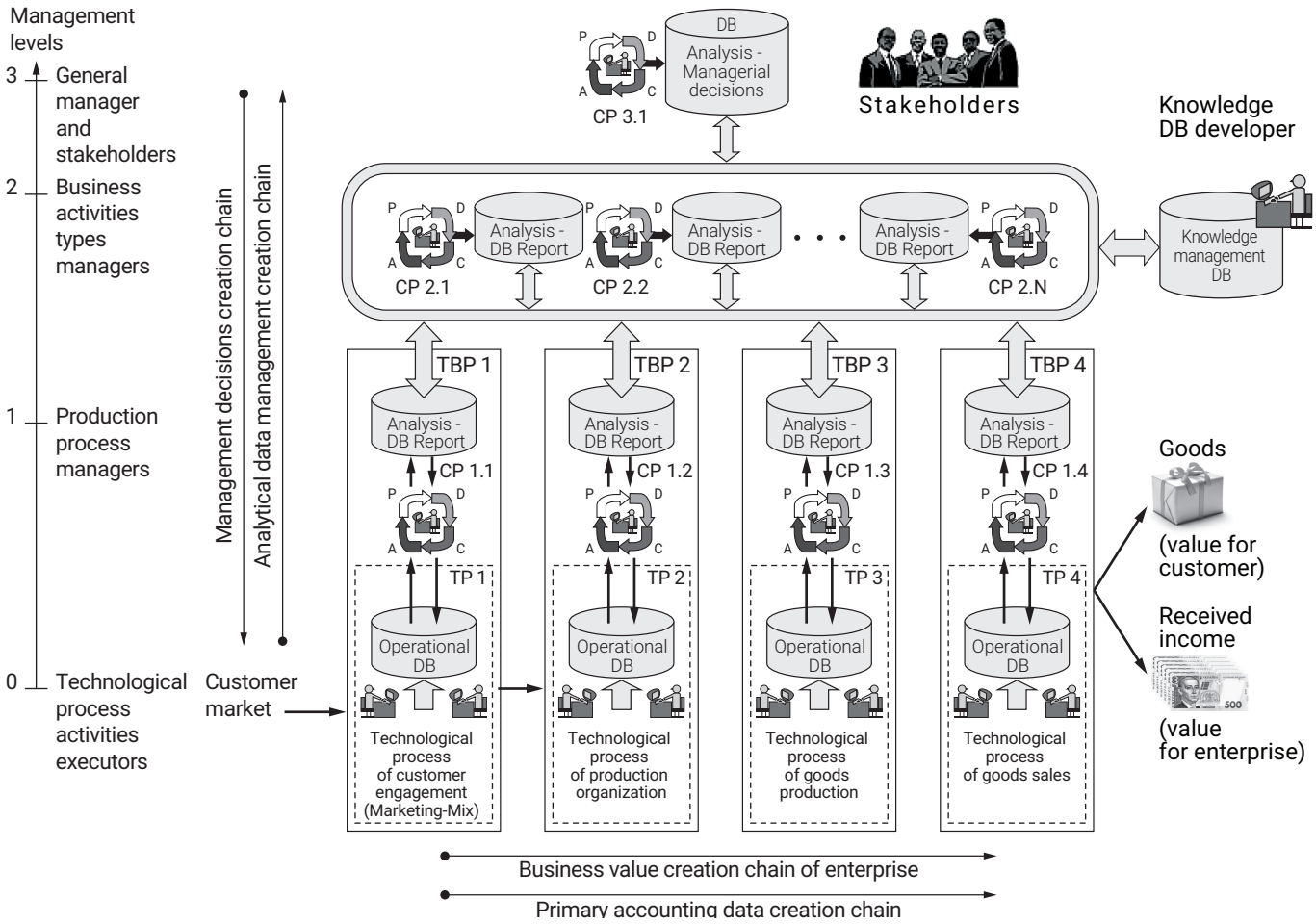

Fig. 2. *Digitalized process-oriented management model of the enterprise (authors model)*

Measurements infrastructure Vol. 4 (2022) MI_019_120122 https://doi.org/10.33955/v4(2022)-019

- middle and lower level managers OASs (heads of separate departments, separate service departments, etc.);
- technological process of value creation chain work executors, who directly create primary data.

Herewith, «digital process management pyramid» concept is considered a digital organizational management structure model for the process-oriented enterprise. Structure model is a hierarchical system of managed by known PDCA (plan – do – check – act) management cycle internal and interrelated functions of each manager and lower (adjacent) level directly subordinate managers whose aim is managerial decisions production for directly subordinate executors [13].

Information created in the enterprise value creation system (chain) business process is certainly valuable in the Definition 1 context. Thus, obtaining information by intruders on competitors behalf brings them certain income. Consequently, the primary purpose of intruders is to obtain information on the structure, state, and activities of confidential interest object (on products (goods/services), business projects, recipes, technologies, etc.). Moreover, the useful purpose may be particular information, circulating in the confidential interest object, distortion. Such action can cause disinformation of enterprise management concerning accounting data and solving particular business tasks results. Finally, this influences efficiency assessment evaluation of particular activity spheres from management as a whole.

More necessary information distortion goal is informational arrays storages destruction in documental digital form (database) and program products for information collecting and processing and primary accounting data submitting for making managerial decisions by enterprise managers. In this case malicious intervention is provided in the enterprise automated management system (EAMS). In this regard, structured for all technological and management business processes model of effective informational security system creation in organizational, software, and technical terms becomes more critical.

Taking into account the above, complex market analysis in the informational security sphere risks of the enterprise informational flows throughout the business process system of management pyramid is necessary first. Possible internal and hacker database distortion incidents on the enterprise model creation are necessary further for the balanced, structured informational security model of enterprise development. Such structural model concept is presented in Fig. 3.

In Fig. 3. model context, a range of probable threats sources to business environment informational security of modern enterprise may be as follows:

- established regulations for collecting, processing, and transfer of information violations;
- intended informational systems personnel actions;
- unintended informational systems personnel mistakes;
- errors in informational systems design (EAMS).

Analyzing the causal-consequential link between Fig. 2 and 3 models, it should be mentioned that the essence and novelty of Fig. 2 model is the principle of risk allocation realization. This principle concerns the entire corporate database and knowledge database placement on separate servers having different IP addresses.

Based on this, the following definition is proposed.

Definition 2. Informational security system of the digital enterprise is complex of organizational and technical character measures on entire corporate database and knowledge database allocation on different level servers of the level primary database, analytical and managerial database and knowledge database of enterprise. According to created process management pyramid of the enterprise, the aim is to ensure storage reliability for the protection of commercial and managerial information and its key elements from probable external (cyber-attacks) and internal threats of theft and distortion, informational arrays storages

Measurements infrastructure Vol. 4 (2022) MI_019_120122 https://doi.org/10.33955/v4(2022)-019

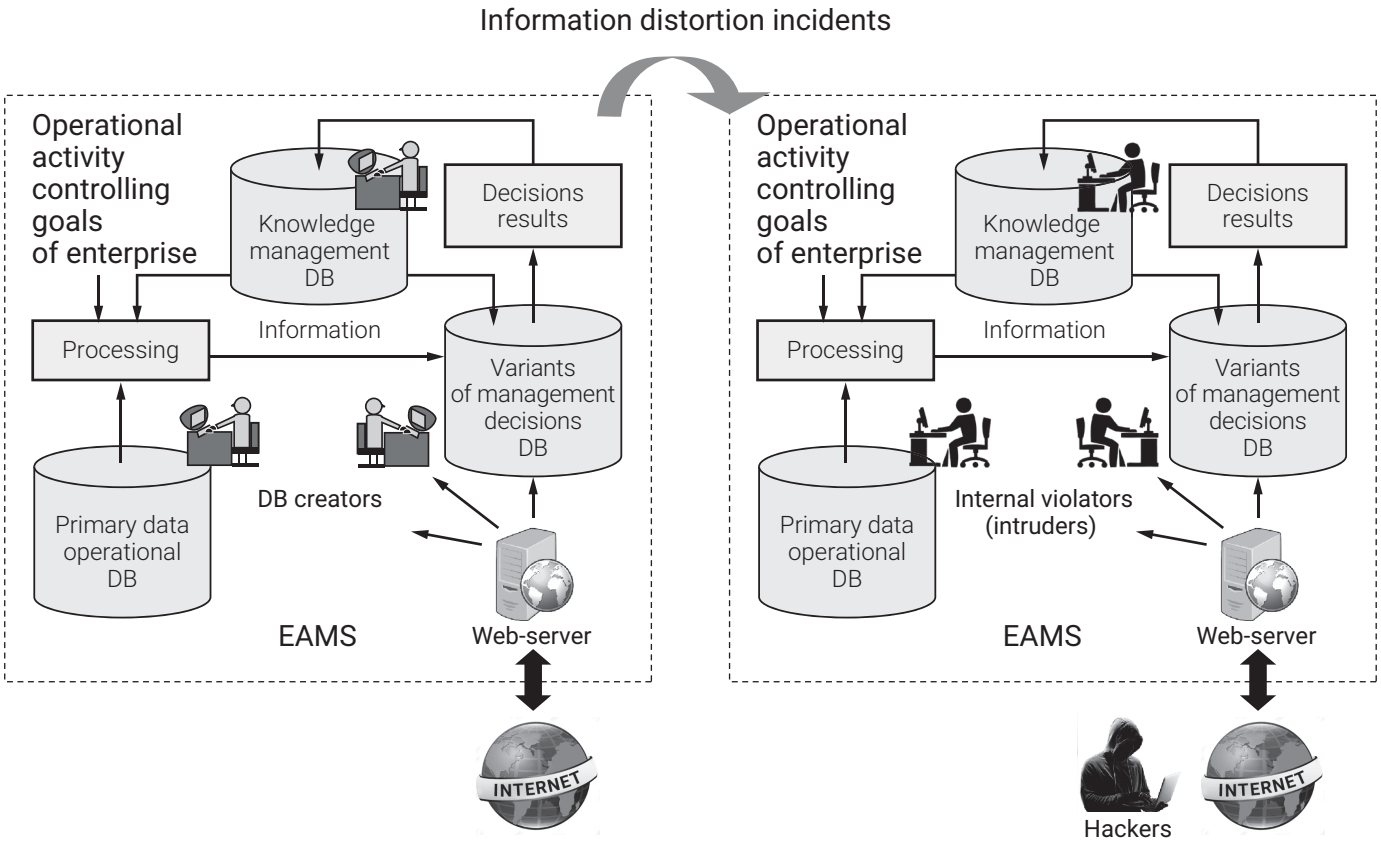

Fig. 3. *Structural model of possible internal and hackers database distortion incidents on the enterprise (authors model)*

destruction in documental digital form (database) and program products for information collecting and processing and primary accounting data submitting for making managerial decisions by enterprise managers.

3. Conclusions

Contrary to the known widespread ACSS development model based on one server OASs network by entire corporate database and knowledge database placement on one common server having one IP address novelty of the proposed model is the principle of risk allocation realization. That is, common enterprise local OASs network development is provided as complex of different level networks according to OASs classification by management level. Herewith, each level network has its separate server with the corresponding IP address. Thereby, the conceptual structural approach to the informational security system of digital process-oriented enterprise modelling considered in the article enables providing its complete evaluation at each corporate OAS network level of management process pyramid (diagnostics capability for internal incidents and hackers database distortion increases). Taking into account the possibility of informational security threat source for modern enterprise business environment as a result of its EAMS design, errors occur. The precondition for further research can be considered as such errors elimination by use of system complex synthesis technology for the business process of the modern digital enterprise (process management pyramid) based on bictivity representation requirements (transformation) of business goals hierarchical system of the enterprise into the hierarchical structure of its managerial responsibility centers [13].

Measurements infrastructure Vol. 4 (2022) MI_019_120122 https://doi.org/10.33955/v4(2022)-019

References

1. Antonov V. H., Samosudov M. V. *Problems and prospects of digital management development* [Проблемы и перспективы развития цифрового менеджмента]. (Accessed 1 January 2022). [In Russian] https://e-management.guu.ru/jour/article/view/16
2. Shushunova T. N., Vakulenko V. F., Frolova A. V. *Modern trends and prospects of management development in digital transformation conditions* [Современные тренды и перспективы развития менеджмента в условиях цифровой трансформации]. (Accessed 2 January 2022). [In Russian] https://cyberleninka.ru/article/n/sovremennye-trendy-i-perspektivy-razvitiya-menedzhmenta-v-usloviyah-tsifrovoy-transformatsii/viewer
3. Baranov O. A. 2018 *Internet of things (IoT): use goal and legal problems* [Інтернет речей (IoT): мета застосування та правові проблеми]. Information and legacy. **№ 2 (25),** pp. 31-44. (Accessed 2 January 2022). [In Ukrainian] http://ippi.org.ua/sites/default/files/5_9.pdf
4. Kozlova O. Yu., Kononovych V. H., Kononovych I. V., Romaniukov L. M., Tymoshenko M. H. 2017 *Dynamic qualities of cyber security ensuring process using cyber security audit example* [Динамічні властивості процесів забезпечення кібербезпеки на прикладі аудиту кібербезпеки]. Informatics and mathematical methods in modelling: an international journal of B category. OPNU. **V. 7, № 3,** pp. 205-212. [In Ukrainian]
5. Sorokivska O. A., Hevko V. L. 2010 *Informational security of the enterprise: modern threats and prospects* [Інформаційна безпека підприємства: нові загрози та перспективи]. Khmelnytskyi National University Bulletin. Economy Science Series. **V. 2, № 2,** pp. 32-35. [In Ukrainian]
6. Melnykov V. P., Kleimenov S. A., Petrakov A. M. 2008 *Informational security and information protection* [Информационная безопасность и защита информации]. M. Academy. **№ 3,** p. 336. [In Russian]
7. Davydiuk T. V., Borymska K. P. 2013 *Positioning of accounting and analytical support for the economic security of the enterprise in the specialists education plans in the «Accounting and Audit» education sphere* [Позиціонування обліково-аналітичного забезпечення економічної безпеки підприємства в навчальних планах фахівців напряму підготовки «Облік і аудит»]. Economy: time realities. Scientific journal. **№ 3 (8),** pp. 83-90. [In Ukrainian]
8. Tsal-Tsalko Yu. S, Moroz Yu. Yu. 2017 *Accounting policy of the enterprise and its cyber security. Accounting, analysis, and control in the modern management of economic potential and enterprise market value concepts: a collection of scientific works* [Облікова політика підприємства та її кібербезпека. Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства: збірник наукових праць]. PP «Ruta». **V. IV, I,** pp. 8-11. [In Ukrainian]
9. *What is network security?* [Що таке безпека мережі]? (Accessed 2 January 2022). [In Ukrainian] https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bezopasnost-seti/
10. Herasimov V. V., Khisayeva H. F., Haripov I. M. 2019 *The intrusion detection system is the most important element of the information security system of the enterprise's corporate network* [Система обнаружения вторжений как важнейший элемент системы информационной безопасности корпоративной сети предприятия]. Scientists Association «Siberian Academic Book», pp. 303-307. [In Russian]
11. *Network security* [Сетевая безопасность]. [In Russian] https://itglobal.com/ru-ru/company/glossary/setevaya-bezopasnost-bezopasnost-seti/
12. Shvydanenko H. O., Prykhodko L. M. 2012 *Business process optimization* [Оптимізація бізнес-процесів]. Educational aid. KNEU. p. 487. [In Ukrainian]
13. Tupkalo V. M. 2016 *Business engineering of modern process-oriented enterprises: a monograph* [Бізнес-інжиніринг сучасних процесно-орієнтованих підприємств: монографія]. DUT, p. 281. [In Ukrainian]
14. Maltsev S. V. *Process management approach: theory and practical use* [Процессный подход к управлению: теория и практика применения]. (Accessed 2 January 2022). [In Russian] http://www.svmal.ru/info_2.html
15. Drucker P. F. 2004 *Encyclopedia of management* [Энциклопедия менеджмента]. Transl. from Engl. – M. Williams. p. 432. [In Russian]