МАТЕМАТИЧНЕ І КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

MATHEMATICAL AND COMPUTER MODELING

DOI: 10.20998/2079-0023.2024.01.05
UDC 004.94

A. M. KOPP, Doctor of Philosophy (PhD), Docent, National Technical University "Kharkiv Polytechnic Institute", Head of Software Engineering and Management Intelligent Technologies Department, Kharkiv, Ukraine, e mail: andrii.kopp@khpi.edu.ua, ORCID: https://orcid.org/0000-0002-3189-5623
D. L. ORLOVSKYI, Candidate of Technical Sciences (PhD), Docent, National Technical University "Kharkiv Polytechnic Institute", Professor at the Department of Software Engineering and Management Intelligent Technologies, Kharkiv, Ukraine, e mail: dmytro.orlovskyi@khpi.edu.ua, ORCID: https://orcid.org/0000-0002-8261-2988
O. S. KIZILOV, National Technical University "Kharkiv Polytechnic Institute", Assistant at the Department of Software Engineering and Management Intelligent Technologies, Kharkiv, Ukraine, e mail: olexiy.kizilov@khpi.edu.ua, ORCID: https://orcid.org/0009-0000-1151-3619
O. S. HALATOVA, National Technical University "Kharkiv Polytechnic Institute", Assistant at the Department of Software Engineering and Management Intelligent Technologies, Kharkiv, Ukraine, e mail: olha.halatova@khpi.edu.ua, ORCID: https://orcid.org/0009-0009-5091-1666

RESEARCH ON ERROR PROBABILITY ASSESSMENT IN USER PERSONAL DATA PROCESSING IN GDPR-COMPLIANT BUSINESS PROCESS MODELS

The only right strategy for businesses and government organizations in Ukraine and other countries that may face aggression is to recognize themselves as a potential target for cyberattacks by the aggressor (both by its government agencies and related cybercriminal groups) and take appropriate measures in accordance with the European Union's General Data Protection Regulation (GDPR). The main purpose of the GDPR is to regulate the rights to personal data protection and to protect EU citizens from data leaks and breaches of confidentiality, which is especially important in today's digital world, where the processing and exchange of personal data are integral parts of almost every business process. Therefore, the GDPR encourages organizations to transform their day-to-day business processes that are involved in managing, storing, and sharing customers' personal data during execution. Thus, business process models created in accordance with the GDPR regulations must be of high quality, just like any other business process models, and the probability of errors in them must be minimal. This is especially important with regard to the observance of human rights to personal data protection, since low-quality models can become sources of errors, which, in turn, can lead to a breach of confidentiality and data leakage of business process participants. This paper analyzes recent research and publications, proposes a method for analyzing business process models that ensure compliance with the GDPR regulations, and tests its performance based on the analysis of BPMN models of business processes for obtaining consent to data processing and withdrawal of consent to user data processing. As a result, the probability of errors in the considered business process models was obtained, which suggests the possibility of confidentiality violations and data leaks of the participants of the considered business processes associated with these errors, and appropriate recommendations were made.

Keywords: business process GDPR compliance, personal data leakage prevention, BPMN business process model analysis, business process model error probability analysis, personal data protection in business processes.

Introduction. According to the authors of the material [1], offline conflicts quickly spill over into the online world. Therefore, in addition to state actors, cyberattacks are also carried out by anonymous criminal groups that can take sides. In this situation, aggressors often rely on chaos, supporting or turning a blind eye to the activities of cybercriminals in their own countries. Even if ransomware and blackmail attacks were intended to affect only special targets, such as certain government organizations, experience shows that business representatives, including international ones, are also victims of malware attacks.

For example, during the large-scale hacker attacks on Ukraine in 2017, 7 banks and about 40 Ukrainian and international companies suffered from cybercriminals' actions [2], including DTEK, Nova Poshta, FedEx, Rozetka, WOG, and others. According to an analytical report by Microsoft [3], since the beginning of the full-scale war, on February 24, 2022, 237 cyberattacks have been carried out on Ukrainian government agencies and enterprises.

Thus, according to the proposal set out in [1], the only correct strategy for enterprises and government organizations in Ukraine and other countries that may face aggression is to recognize themselves as a potential target for cyberattacks by the aggressor (both by its government agencies and related cybercriminal groups) and take appropriate measures in accordance with the General Data

Protection Regulation of the European Union (GDPR) [4]. According to this regulation, institutions are obliged to introduce appropriate technical and organizational measures to prevent data leaks and potential violations of customer privacy [1]. Also, according to [1], in many cases, cybercriminals use the same methods during war as in peacetime. For example, attackers will look for vulnerabilities in an organization's system, including known vulnerabilities (the so-called "exploits") in "everyday" software that have not been patched by its developers [1]. In addition, in order to increase the number of malware victims, attackers may also target infrastructure providers [1].

The GDPR plays an important role in the European Union (EU) legislation on privacy and human rights, which is, in particular, defined in Article 8(1) of the Charter of Fundamental Rights of the European Union [5].The main purpose of the GDPR is to regulate the rights to personal data protection and to protect EU citizens from data leaks and violations of their confidentiality, which is especially important in today's digital world, where the processing and exchange of personal data are integral components of almost every business process [6]. Thus, the GDPR encourages organizations to transform their daily business processes involved in managing, storing, and exchanging customers' personal data during execution [6]. In 2022, after the outbreak of a full-scale war, Ukraine became an EU candidate state, so it is obvious that European integration will be a priority for Ukraine now and during the post-war recovery, and Ukrainian enterprises and institutions already need to build business processes in accordance with the GDPR regulations in order to ensure the privacy of their users and prevent leakage of their personal data.

Related work. The general overview of the recent papers related to EA frameworks indexed in the Google Scholar platform shows the stable interest in EA frameworks, especially defense-oriented ones, over the last five years (see fig. 1).

First, the authors of [6], mentioned above, analyzed the main restrictions of the GDPR on privacy and personal data and proposed a set of business process design templates to take into account and integrate these restrictions into business process models in the BPMN (Business Process Model and Notation) notation [6].

The authors of another work [7] also note that organizations need to implement mechanisms to ensure the security of personal data in business processes in order to avoid liability in the event of an attack by intruders that may lead to data leakage and in accordance with the law, in particular, the GDPR [7]. Therefore, the study [7] proposes to implement compliance with the GDPR regulations by performing security processes based on cloud services, which will allow organizations that do not have the necessary security competencies to use cloud service providers as trusted third parties during GDPR compliance checks or after a data breach [7]. For this purpose, the authors of [7] developed appropriate BPMN models of business processes for their further implementation in the cloud environment [7].

Work [8] also addresses the issues of verification of business processes represented using the BPMN notation in order to detect violations of privacy rules and prevent potential violations of the GDPR [8].

In one of the most recent studies in this area [9], the authors note the need to check the compliance of business process scenarios with the GDPR regulations at the stage of their modeling [9]. Thus, the authors of [9] propose an approach to bringing BPMN models of business processes in line with the GDPR requirements for consent requests and withdrawal of consent to data processing [9].

State-of-the-art. Although the publications under review consider design templates for BPMN business process models [6] and BPMN scenarios for consent requests and withdrawal of consent to data processing [9], as well as approaches to the implementation of business processes in the cloud environment [7] and verification of BPMN models in terms of their compliance with the GDPR [8], insufficient attention is paid to the quality of all proposed BPMN business process models.

Business process modeling is the main tool of the process approach to organizational management. Business process models are used to depict (in the form of graphical diagrams), analyze, and further improve business processes [10]. Most often, business process models are used in the design and analysis of information systems, being a mechanism for communication between business and technical parties [11].

Thus, business process models created in accordance with the GDPR must be of high quality, just like any other business process models, and the probability of errors in them must be minimal. This is especially important in terms of observing human rights to personal data protection, as low-quality models can become sources of errors, which, in turn, can lead to a breach of confidentiality and data leakage of business process participants.

Problem statement. The object of research is the procedure for analyzing business process models that ensure compliance with the GDPR regulations. The subject of the study is a method of analyzing business process models that ensure compliance with the GDPR regulations.

The purpose of the study is to prevent privacy violations and data leaks of business process participants by analyzing the relevant models that ensure compliance with the GDPR regulations. Thus, in order to achieve the goal, the following tasks need to be solved:

- to develop a method for analyzing business process models for the probability of errors, including those related to personal data;
- to test the efficiency of the developed method by analyzing business process models that ensure compliance with the GDPR;
- to determine the probabilities of confidentiality violations and data leaks of business process participants, and to formulate appropriate recommendations.

Materials. A business process model presented using the BPMN notation can be formally represented using an oriented graph:

$$G = (N, A), \tag{1}$$

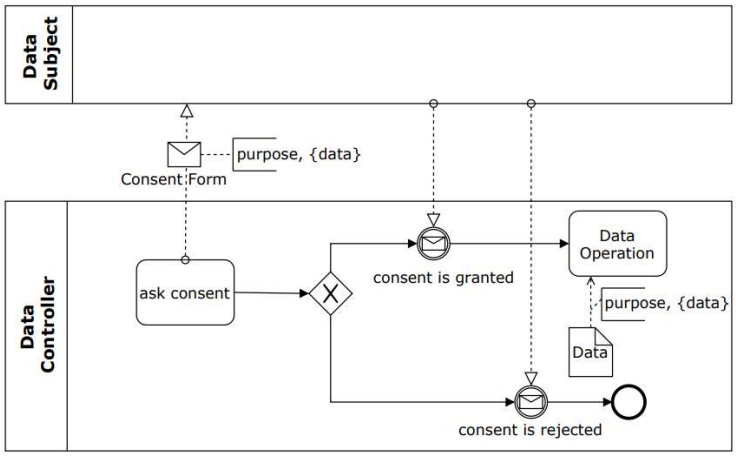

Fig. 1. BPMN model for obtaining consent to data processing [9]

where:

- N is the set of nodes – various elements of the business process model: actions (tasks and sub-processes), events (start, intermediate, end), and logical gateways;
- A is the set of arcs – flows in the business process execution sequence (sequence flows).

According to the results of a study on the probability of errors in the structure of a business process model [12], the following metrics can be determined based on the basic graph structural metrics (1) of the business process model – the number of nodes $|N|$ and the number of arcs $|A|$:

$$\Delta(G)=\frac{|A|}{|N|\cdot(|N|-1)},\ CNC(G)=\frac{|A|}{|N|}, \qquad (2)$$

where:

- $\Delta(G)$ is the density metric of a business process model;
- $CNC(G)$ is the connectivity metric (Coefficient of Network Connectivity, CNC) of a business process model.

The specified density and connectivity metrics (2) have the following thresholds, the excess of which will indicate the corresponding probability of the presence of structural errors in the business process model [12]:

$$P(\Delta(G))=\begin{cases}0.16, & \Delta(G)\le 0.033,\\ 0, & \text{else},\end{cases}$$
$$P(CNC(G))=\begin{cases}0.08, & CNC(G)\le 1.021,\\ 0, & \text{else},\end{cases} \qquad (3)$$

where:

- $P(\Delta(G))$ is the probability of structural errors in the model (16%) if the metric $\Delta(G)$ exceeds the established threshold value (0.033);
- $P(CNC(G))$ is the probability of structural errors in the model (8%) if the $CNC(G)$ metric exceeds the established threshold value (1.021).

Thus, by determining the probabilities (3), it will be possible to determine the probability of errors in the BPMN business process model as a whole:

$$P(\Delta(G),CNC(G))=1-[1-P(\Delta(G))]\cdot[1-P(CNC(G))]. \qquad (4)$$

According to (4), it is proposed to calculate the inverse probabilities of (3), i.e., the non-detection of errors in the business process model, and then, according to the rule of the product of independent events, to determine the probability of non-detection of errors by at least one of the metrics (2) and, finally, to determine the inverse probability of detecting errors by at least one of the metrics (2).

It is proposed to verify the effectiveness of the proposed method by analyzing the models of business processes for obtaining consent and withdrawing consent to data processing that ensure compliance with the GDPR regulations, as defined in the study [9].

Accordingly, the BPMN model of the business process for obtaining consent (OC) to data processing is demonstrated in fig. 1.

Another business process of withdrawing consent (WC) to data processing is demonstrated using a BPMN model in fig. 2.

Table 1 shows the results of calculating the main structural characteristics (1), as well as the density and connectivity metrics (2) of the models of business processes for obtaining consent (fig. 1) and withdrawing consent to data processing (fig. 2), obtained using the proposed method.

Table 1 – Results of business process model metrics calculation

Model	$\|N\|$	$\|A\|$	$\Delta(G)$	$CNC(G)$
OC	6	5	0.17	0.83
WC	2	1	0.5	0.5

It should be noted that the calculations did not take into account the scenario nested in the "handle revocation" action (fig. 2).

Table 2 shows the probabilities of errors in business process models, determined on the basis of compliance of the calculated values of the model metrics (table 1) with their thresholds [12].

Based on the results shown in table 2, it can be determined that the data of the business process models for obtaining consent (fig. 1) and withdrawing consent to data processing (fig. 2) both contain errors with a probability of 16%. Therefore, it can be assumed that the probability of confidentiality violations and/or data leaks of participants

in these business processes due to errors in BPMN models is also close to 16%.

Table 2 – Compliance of the calculated metrics with their thresholds

Model	$P(\Delta(G))$	$P(CNC(G))$	$P(\Delta(G),CNC(G))$
OC	0.16	0	0.16
WC	0.16	0	0.16

The obtained probability values (table 2) indicate the need to correct errors in the analyzed business process models. These errors were identified and listed below.

For the OC business process model:

- there is no start event – it is not clear when the business process starts;
- it is not clear what leads to the execution of the "ask consent" action, which starts the business process;
- the execution of the "Data Operation" action does not lead to the completion of the process or the next action – it is not clear how the business process should be completed or continued;
- there is no end event for the scenario when consent has been obtained – it is not clear when the business process ends in this case.

For the WC business process model:

- there is no start event – it is not clear when the business process starts;
- it is not clear what leads to the execution of the "Data Operations" action, which starts the business process;
- execution of the "handle revocation" action does not lead to the completion of the process or the next action – it is not clear how the business process should be completed or continued.

Thus, we have demonstrated the errors identified in business process models that ensure compliance with the GDPR. If these models are used to adapt the organization's business processes to the GDPR requirements, the identified errors (table 3) should be eliminated to reduce the probability of negative consequences for data.

Thus, it is recommended that all business process models be checked for possible errors in them in order to ensure the confidentiality of business process participants and prevent leakage of their personal data.

Conclusion. This paper analyzes recent research and publications, proposes a method for analyzing business process models that ensure compliance with the GDPR regulations, and tests its performance based on the analysis of BPMN models of business processes for obtaining consent to data processing and withdrawal of consent to user data processing. As a result, the probability of errors in the considered business process models was obtained, which suggests the possibility of confidentiality violations and data leaks of the participants of the considered business processes related to these errors, and appropriate recommendations were made. It is planned to develop a web application that will help Ukrainian enterprises and institutions check BPMN models for possible errors in them in order to prevent data leaks and other negative consequences.

References

1. *Client Alert: The Effects of War on Cyber Security & GDPR*. URL: https://www.corderycompliance.com/war-effects-on-cybersecurity/ (access date: 25.04.2024).
2. *Unknown Virus Attacks Dozens Of Ukrainian Companies*. URL: https://hromadske.ua/en/posts/unknown-virus-attacks-ukraines-state-banks-and-enterprizes (access date: 25.04.2024).
3. *An overview of Russia's cyberattack activity in Ukraine*. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (access date: 25.04.2024).
4. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. URL: https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (access date: 25.04.2024).
5. *How to access your personal data under the GDPR*. URL: https://www.citizensinformation.ie/en/government_in_ireland/data_protection/rights_under_general_data_protection_regulation.html (access date: 25.04.2024).
6. Agostinelli S. et al. *Achieving GDPR compliance of BPMN process models*. URL: https://doi.org/10.1007/978-3-030-21297-1_2 (access date: 25.04.2024).
7. Bryce C. *Security Governance as a Service on the Cloud*. URL: https://doi.org/10.1186/s13677-019-0148-5 (access date: 25.04.2024).
8. Palmirani M., Governatori G. *Modelling Legal Knowledge for GDPR Compliance Checking*. URL: https://doi.org/10.3233/978-1-61499-935-5-101 (access date: 25.04.2024).

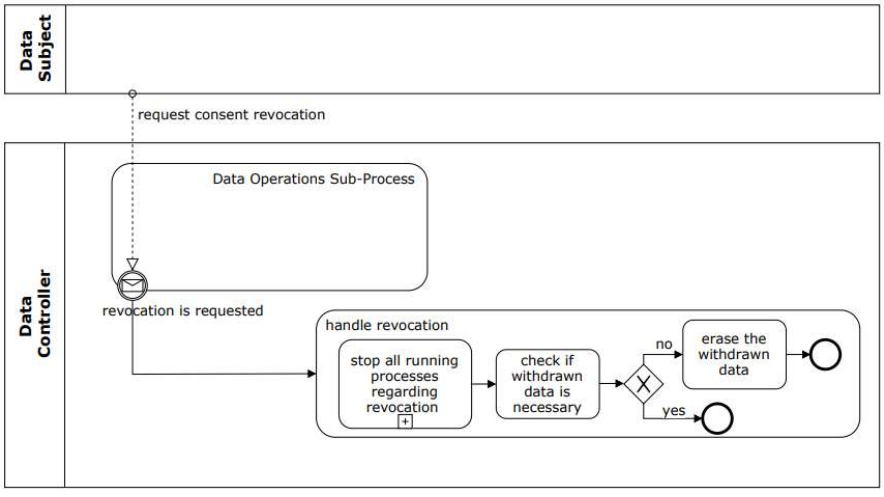

Fig. 2. BPMN model for withdrawing consent to data processing [9]

9. Besik S. I., Freytag J. C. *Managing Consent in Workflows under GDPR*. URL: https://ceur-ws.org/Vol-2575/paper4.pdf (access date: 25.04.2024).
10. Van der Aalst W. M. *Business process management: a comprehensive survey*. URL: https://doi.org/10.1155/2013/507984 (access date: 25.04.2024).
11. Kahloun F., Ghannouchi S. A. *A Classification Algorithm for Assessing the Quality Criteria for Business Process Models*. URL: https://doi.org/10.1007/978-3-319-76351-4_8 (access date: 25.04.2024).
12. Mendling J., Sánchez-González L., García F., La Rosa M. *Thresholds for error probability measures of business process models*. URL: https://doi.org/10.1016/j.jss.2012.01.017 (access date: 25.04.2024).

References (transliterated)

1. *Client Alert: The Effects of War on Cyber Security & GDPR*. Available at: https://www.corderycompliance.com/war-effects-on-cybersecurity/ (accessed 25.04.2024).
2. *Unknown Virus Attacks Dozens Of Ukrainian Companies*. Available at: https://hromadske.ua/en/posts/unknown-virus-attacks-ukraines-state-banks-and-enterprizes (accessed 25.04.2024).
3. *An overview of Russia's cyberattack activity in Ukraine*. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (accessed 25.04.2024).
4. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Available at: https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (accessed 25.04.2024).
5. *How to access your personal data under the GDPR*. Available at: https://www.citizensinformation.ie/en/government_in_ireland/data_protection/rights_under_general_data_protection_regulation.html (accessed 25.04.2024).
6. Agostinelli S. et al. *Achieving GDPR compliance of BPMN process models*. Available at: https://doi.org/10.1007/978-3-030-21297-1_2 (accessed 25.04.2024).
7. Bryce C. *Security Governance as a Service on the Cloud*. Available at: https://doi.org/10.1186/s13677-019-0148-5 (accessed 25.04.2024).
8. Palmirani M., Governatori G. *Modelling Legal Knowledge for GDPR Compliance Checking*. Available at: https://doi.org/10.3233/978-1-61499-935-5-101 (accessed 25.04.2024).
9. Besik S. I., Freytag J. C. *Managing Consent in Workflows under GDPR*. Available at: https://ceur-ws.org/Vol-2575/paper4.pdf (accessed 25.04.2024).
10. Van der Aalst W. M. *Business process management: a comprehensive survey*. Available at: https://doi.org/10.1155/2013/507984 (accessed 25.04.2024).
11. Kahloun F., Ghannouchi S. A. *A Classification Algorithm for Assessing the Quality Criteria for Business Process Models*. Available at: https://doi.org/10.1007/978-3-319-76351-4_8 (accessed 25.04.2024).
12. Mendling J., Sánchez-González L., García F., La Rosa M. *Thresholds for error probability measures of business process models*. Available at: https://doi.org/10.1016/j.jss.2012.01.017 (accessed 25.04.2024).

Received 05.04.2024

УДК 004.94

А. М. КОПП, доктор філософії (PhD), доцент, Національний технічний університет «Харківський політехнічний інститут», завідувач кафедри програмної інженерії та інтелектуальних технологій управління, м. Харків, Україна, e-mail: andrii.kopp@khpi.edu.ua, ORCID: https://orcid.org/0000-0002-3189-5623
Д. Л. ОРЛОВСЬКИЙ, кандидат технічних наук (PhD), доцент, Національний технічний університет «Харківський політехнічний інститут», професор кафедри програмної інженерії та інтелектуальних технологій управління, м. Харків, Україна, e-mail: dmytro.orlovskyi@khpi.edu.ua, ORCID: https://orcid.org/0000-0002-8261-2988
О. С. КІЗІЛОВ, Національний технічний університет «Харківський політехнічний інститут», асистент кафедри програмної інженерії та інтелектуальних технологій управління, м. Харків, Україна, e-mail: olexiy.kizilov@khpi.edu.ua, ORCID: https://orcid.org/0009-0000-1151-3619
О. С. ГАЛАТОВА, Національний технічний університет «Харківський політехнічний інститут», асистент кафедри програмної інженерії та інтелектуальних технологій управління, м. Харків, Україна, e-mail: olha.halatova@khpi.edu.ua, ORCID: https://orcid.org/0009-0009-5091-1666

ДОСЛІДЖЕННЯ ЩОДО ОЦІНКИ ЙМОВІРНОСТІ ПОМИЛОК ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ МОДЕЛЕЙ БІЗНЕС-ПРОЦЕСІВ НА ОСНОВІ GDPR

Єдиною вірною стратегією для підприємств та державних організацій України та інших країн, що можуть зіткнутися з агресією, є усвідомлювати себе потенційною мішенню для кібератак агресора (як з боку його державних структур, так і з боку пов'язаних кіберзлочинних груп), та вживати відповідних заходів відповідно до Загального регламенту про захист даних Європейського Союзу (General Data Protection Regulation, GDPR). Основною метою GDPR є регулювання прав на захист персональних даних та реалізація захисту громадян ЄС від витоків даних та порушень їх конфіденційності, що особливо актуально в цифровому світі сьогодення, де обробка та обмін персональними даними є невід'ємними складовими майже кожного бізнес-процесу. Таким чином, GDPR спонукає організації до перетворення своїх повсякденних бізнес-процесів, які залучені до управління персональними даними клієнтів, їх зберігання та обміну під час виконання. Таким чином, моделі бізнес-процесів, що створюються у відповідності до регламенту GDPR, мають бути високої якості так само, як і будь-які інші моделі бізнес-процесів, а ймовірність наявності у них помилок має бути мінімальною. Це особливо важливо щодо дотримання прав людини на захист персональних даних, оскільки моделі низької якості можуть стати джерелами помилок, які, у свою чергу, можуть призвести до порушення конфіденційності та витоку даних учасників бізнес-процесів. У роботі здійснено аналіз останніх досліджень і публікацій, запропоновано метод аналізу моделей бізнес-процесів, що забезпечують відповідність регламенту GDPR, перевірено його працездатність на основі аналізу BPMN-моделей бізнес-процесів отримання згоди на обробку даних та відкликання згоди на обробку даних користувачів. У результаті було отримано ймовірність виникнення помилок у розглянутих моделях бізнес-процесів, що дозволяє припустити про можливість виникнення пов'язаних з цими помилками порушень конфіденційності та витоків даних учасників розглянутих бізнес-процесів, сформовано відповідні рекомендації.

Ключові слова: відповідність бізнес-процесів GDPR, запобігання витоку персональних даних, аналіз BPMN-моделей бізнес-процесів, аналіз ймовірності помилок у моделях бізнес-процесів, захист персональних даних у бізнес-процесах.

Повні імена авторів / Author's full names

Автор 1 / Author 1: Копп Андрій Михайлович / Kopp Andrii Mykhailovych
Автор 2 / Author 2: Орловський Дмитро Леонідович / Orlovskyi Dmytro Leonidovych
Автор 3 / Author 3: Кізілов Олексій Сергійович / Kizilov Oleksii Serhiiovych
Автор 4 / Author 4: Галатова Ольга Сергіївна / Halatova Olha Serhiivna