Yurii DREIS[1], Iryna LOZOVA[2], Andrii BISKUPSKYI[3],
Yevhenii PEDCHENKO[4], Yevheniia IVANCHENKO[5]

Scientific supervisor: Alexander KORCHENKO[6]

GDPR-MODEL OF PARAMETERS FOR ESTIMATING LOSSES FROM LOSS OF PERSONAL DATA

Abstract: A mathematical model of negative impact assessment has been developed that allows to determine losses for an organisation in case of leakage of personal data in accordance with the provisions of the GDPR Regulation and provides guidance on identifying and minimising gaps in information security policy of an organisation.

Keywords: personal data, GDPR-model, consequences of leakage of personal data, personal data protection.

MODEL PARAMETRÓW GDPR DO SZACOWANIA STRAT Z UTRATY DANYCH OSOBOWYCH

Streszczenie: Opracowano model matematyczny oceny negatywnego wpływu utraty danych. Ten model pozwala określić straty dla organizacji w przypadku wycieku danych osobowych zgodnie z przepisami rozporządzenia GDPR i zawiera zalecenia dotyczące identyfikacji i minimalizacji braków w polityce bezpieczeństwa informacyjnego organizacji.

Słowa kluczowe: dane osobowe, model GDPR, skutki wycieku danych osobowych, ochrona danych osobowych

---

[1] PhD Eng (Information security), associate professor of IT-Security Academic Department, National Aviation University, Dreisyuri@gmail.com
[2] Senior lector of IT-Security Academic Department, National Aviation University illozovaya@gmail.com
[3] Assistant Professor of IT-Security Academic Department, National Aviation University andrii.biskupskyi@gmail.com
[4] Master of IT-Security Academic Department, National Aviation University zhenia1398@gmail.com
[5] PhD Eng (Information security), professor of IT-Security Academic Department, National Aviation University evivancenko@gmail.com
[6] Dr Eng (Information security), Professor, Laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Visit-Professor at The University of Bielsko-Biala (Akademia Techniczno-Hu-manistyczna, Bielsko-Biała, Poland), Leading Researcher of the National Academy of SS of Ukraine, icaocentre@nau.edu.ua

1. Introduction

In 2018, a new European Union (EU) law on personal data (PD) protection – GDPR (General Data Protection Regulation) has come into force, which differs from the existing laws by unprecedented penalties for breaches of the rules on protection of PD in EU organisations, including those with Ukrainian capital [1]. Since entering into force of the GDPR many entitites have been subjected to the law effect, in particular: the hospital in Portugal paid €400,000 after clients' PDs were opened; German social media paid €20,000 for keeping passwords in the public domain and etc. Even such "giants" as Google and Facebook were also forced to pay the relevant fines (Facebook paid €1.42 million for breaching the security rules of the pages of the EU members') [2-4].
Therefore, at this stage, it is important for organisations operating in the EU area to comply with the rules of the GDPR, being capable of assessing their own extent of losses in the event of exposure of the PD or being capable of evaluating existing security measures in order to prevent a PD leak.

2. The mathematical model for evaluating the negative consequences of leakage of personal data

Based on the analysis of the GDPR, criteria and proportions of fines have been determined in accordance with the Article 83 (4,5) of this Regulation: 1) up to €10 million or up to 2% of total global annual turnover for the previous financial year in the event of a breach of one of the following Articles 8, 11, 25-39, 41, 42 and 43; 2) up to € 20 million or up to 4% of the total global annual turnover for the previous financial year in the event of breach of one of the following Articles 5, 6, 7, 9, 12-22, 44-49, 58 and Chapter IX of this Regulation [5].
In accordance with the Article 83 (2), the final amount of the fine is determined by taking into account the violation of one, several or all of the components of this Article, such as: a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; b) the intentional or negligent character of the infringement; c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; e) any relevant previous infringements by the controller or processor; f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; g) the categories of personal data affected by the infringement; h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement [6].

The model is designed in the form of a tuple:

$$\mathbf{IDF} =< \mathbf{IDF_1}, \mathbf{IDF_2}, ..., \mathbf{IDF_i}, ..., \mathbf{IDF_n} >, \quad (1)$$

where: $\mathbf{IDF_i} \subseteq \mathbf{IDF}$ $(i = \overline{1,n})$ – a tuple component which reflects the *i*-th identifier of the object, *n* their number, and for all elements **IDF** order property is characteristic.
For example, for $n = 13$ we define the tuple (1) as:

$$\mathbf{IDF} = < \mathbf{IDF_1}, \mathbf{IDF_2}, ..., \mathbf{IDF_7}, ..., \mathbf{IDF_{13}} >=$$

$$< \mathbf{T}, \mathbf{L}, \mathbf{N}, \mathbf{CH}, \mathbf{A}, \mathbf{R}, \mathbf{I}, \mathbf{C}, \mathbf{CA}, \mathbf{M}, \mathbf{ME}, \mathbf{AD}, \mathbf{F}, \mathbf{RE} >,$$

where: $\mathbf{IDF_1} = \mathbf{T}$ (total worldwide annual turnover (T) of an enterprise for the preceding financial year); $\mathbf{IDF_2} = \mathbf{L}$ (level (L) of violation); $\mathbf{IDF_3} = \mathbf{N}$ (the nature (N), gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them); $\mathbf{IDF_4} = \mathbf{CH}$ (intentional or negligent character (CH) of breaches); $\mathbf{IDF_5} = \mathbf{A}$ (any action (A) taken by the controller or operator to reduce the level of harm caused to the data subjects); $\mathbf{IDF_6} = \mathbf{R}$ (the degree of responsibility (R) of the controller or operator, given the technical and organizational tools they apply in accordance with Articles 25 and 32); $\mathbf{IDF_7} = \mathbf{I}$ (any relevant previous infringements (I) by the controller or the operator); $\mathbf{IDF_8} = \mathbf{C}$ (level of cooperation (C) with the supervisory authority to compensate for the infringement and reduce the possible negative consequences of the breach); $\mathbf{IDF_9} = \mathbf{CA}$ (categories (CA) of personal data affected by the breach); $\mathbf{IDF_{10}} = \mathbf{M}$ (the manner (M) in which the supervisory authority became aware of the breach, in particular, or, and if so, to what extent the controller or operator reported the breach); $\mathbf{IDF_{11}} = \mathbf{ME}$ (if the measures (ME) referred to in Article 58 (2) have previously been imposed against the controller or operator concerned on the same issue, – compliance with those measures); $\mathbf{IDF_{12}} = \mathbf{AD}$ (adherence (AD) to approved codes of conduct in accordance with Article 40 or approved codes of conduct in accordance with Article 42); $\mathbf{IDF_{13}} = \mathbf{F}$ (any other percipitating or mitigating factor (F) applicable to the circumstances of the case, such as financial gain or expense that has been avoided, directly or indirectly, from the violation); $\mathbf{IDF_{14}} = \mathbf{RE}$ (recommendations (RE)) [7-8].

The first component of the tuple **T** – total worldwide annual turnover of an enterprise for the preceding financial year.

The second component **L** – level of violation, is defined by the expression:

$$\mathbf{L} = \{\bigcup_{i=1}^{n_1} \mathbf{L_i}\} = \{\mathbf{L_1}, \mathbf{L_2}, ..., \mathbf{L_{n_1}}\}, \quad (2)$$

where: $\mathbf{L_i} \subseteq \mathbf{L}$ $(i = \overline{1,n_1})$ – *i*-th identifier of the object, and n_1 their number.

For example, for $n_1 = 2$ $(i = \overline{1,2})$ formula (2) can be represented as:

$$\mathbf{L} = \{\bigcup_{i=1}^{2} \mathbf{L_i}\} = \{\mathbf{L_1}, \mathbf{L_2}\},$$

where in accordance with Articles 83(4,5): $\mathbf{L_1}$ = «Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher»; $\mathbf{L_2}$ = «Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher».

The third component **N –** the nature, gravity and duration of the violation, taking into account the nature, scope or purpose of the relevant processing, as well as the number of data subjects affected and the level of the harm caused to them:

$$\mathbf{N} = \{\bigcup_{i=1}^{n_2} \mathbf{N_i}\} = \{\mathbf{N_1}, \mathbf{N_2}, ..., \mathbf{N_{n_2}}\}, \quad (3)$$

where $\mathbf{N_i} \subseteq \mathbf{N}$ $(i = \overline{1,n_2})$ the *i*-th subset of the criteria for determining the nature, severity and duration of the violation, and n_2 their number.

For example, for $n_2 = 4$ $(i = \overline{1,4})$ formula (3) can be represented as:

$$\mathbf{N} = \{\bigcup_{i=1}^{4} \mathbf{N_i}\} = \{\mathbf{N_1}, \mathbf{N_2}, \mathbf{N_3}, \mathbf{N_4}\},$$

where: $\mathbf{N_1}$ = « Classification of lost data »; $\mathbf{N_2}$ = «The duration of the violation»; $\mathbf{N_3}$ = « Number of affected personal data subjects »; $\mathbf{N_4}$ = « The level of influence on personal data subjects ».

The fourth component **CH** – intentional or negligent character of breaches, is defined by the expression:

$$\mathbf{CH} = \{\bigcup_{i=1}^{n_3} \mathbf{CH_i}\} = \{\mathbf{CH_1}, \mathbf{CH_2}, ..., \mathbf{CH_{n_3}}\}, \quad (4)$$

where $\mathbf{CH_i} \subseteq \mathbf{CH}$ $(i = \overline{1,n_3})$ the *i*-th subset of the criteria of the infringement character, and n_3 their number.

For example, for $n_3 = 3$ $(i = \overline{1,3})$ formula (4) can be represented as:

$$\mathbf{CH} = \{\bigcup_{i=1}^{3} \mathbf{CH_i}\} = \{\mathbf{CH_1}, \mathbf{CH_2}, \mathbf{CH_3}\},$$

where: $\mathbf{CH_1}$ = «The level of industry support of the organisation's software security in accordance with international standards»; $\mathbf{CH_2}$ = «Availability of notifications to the management by controllers on identified risks»; $\mathbf{CH_3}$ = «Managements's actions on the security recommendations of the supervisory authority».

The fifth component **A** – any action taken by the controller or processor to mitigate the damage suffered by data subjects:

$$\mathbf{A} = \{\bigcup_{i=1}^{n_4} \mathbf{A_i}\} = \{\mathbf{A_1}, \mathbf{A_2}, ..., \mathbf{A_{n_4}}\}, \quad (5)$$

where $\mathbf{A_i} \subseteq \mathbf{A}$ $(i = \overline{1,n_4})$ the *i*-th subset of the actions taken by the controller or processor to mitigate the damage, and n_4 their number.

For example, for $n_4 = 3$ $(i = \overline{1,3})$ formula (5) can be presented as:

$$\mathbf{A} = \{\bigcup_{i=1}^{3} \mathbf{A_i}\} = \{\mathbf{A_1}, \mathbf{A_2}, \mathbf{A_3}\},$$

where: $\mathbf{A_1}$ = «A measure of compensation for the losses suffered by the data subjects»; $\mathbf{A_2}$ = «Availaibility of an effective plan in place to mitigate the effects of losses prior to supervisory authority intervention»; $\mathbf{A_3}$ = «The amount of estimated costs associated with mitigating the consequences of losses».

The sixth component **R –** the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32, is defined by expression:

$$\mathbf{R} = \{\bigcup_{i=1}^{n_5} \mathbf{R_i}\} = \{\mathbf{R_1}, \mathbf{R_2}, ..., \mathbf{R_{n_5}}\}, \quad (6)$$

where $\mathbf{R_i} \subseteq \mathbf{R}$ $(i = \overline{1,n_5})$ the *i*-th subset of the degree of responsibility of the controller or processor, and n_5 their number.

For example, $n_5 = 8$ $(i = \overline{1,8})$ formula (6) can be presented as:

$$\mathbf{R} = \{\bigcup_{i=1}^{8} \mathbf{R_i}\} = \{\mathbf{R_1}, \mathbf{R_2}, \mathbf{R_3}, \mathbf{R_4}, \mathbf{R_5}, \mathbf{R_6}, \mathbf{R_7}, \mathbf{R_8}\},$$

where: $\mathbf{R_1}$ = «Availaibilty of protection of personal data in the organization »; $\mathbf{R_2}$ = «Availability of the use the means of encryption and marking personal data in the organisation»; $\mathbf{R_3}$ = «Utilisation by the organisation of modern standards for encryption of information »; $\mathbf{R_4}$ = «When using encryption, the keys were lost along with the data»; $\mathbf{R_5}$ = «Implementation of approved incident response and recovery plans by the organisation»; $\mathbf{R_6}$ = «Availability of reliable testing procedures in the organisation»; $\mathbf{R_7}$ = «Availability of reliable risk management procedures in the organisation»; $\mathbf{R_8}$ = «Availability of Code of Conduct for employees in the organisation».

The seventh component **I** – any relevant previous infringements by the controller or processor are defined by the expression:

$$\mathbf{I} = \{\bigcup_{i=1}^{n_6} \mathbf{I_i}\} = \{\mathbf{I_1}, \mathbf{I_2}, ..., \mathbf{I_{n_6}}\}, \quad (7)$$

where $\mathbf{I_i} \subseteq \mathbf{I}$ $(i = \overline{1,n_6})$ the *i*-th subset of the any proper infringements by the controller or processor, and n_6 their number.

For example, $n_6 = 1$ $(i = 1)$ formula (7) can be presented as:

$$\mathbf{I} = \{\bigcup_{i=1}^{1} \mathbf{I_i}\} = \{\mathbf{I_1}\},$$

where: $\mathbf{I_1}$ = « The first loss of personal data in the organisation ».

The subset $\mathbf{I_i}$ defined as:

$$\mathbf{I_i} = \{\bigcup_{j=1}^{n_{6i}} \mathbf{I_{ij}}\} = \{\mathbf{I_{i1}}, \mathbf{I_{i2}}, ..., \mathbf{I_{in_{6i}}}\}, \tag{8}$$

where $\mathbf{I_{ij}} \subseteq \mathbf{I_i}$ $(j = \overline{1, n_{6i}})$ – the *j*-th subset of the groups of taken actions to mitigate the losses clustered by a specific topic or grouped by certain characteristics within the bounds of the *i*-th subset, and n_{6i} the number of the groups of the *i*-th subset.

Considering (8) the expression (7) can be presented as:

$$\begin{aligned}\mathbf{I} = \{\bigcup_{i=1}^{n_6} \mathbf{I_i}\} = \{\bigcup_{i=1}^{n_6} \{\bigcup_{j=1}^{n_{6i}} \mathbf{I_{ij}}\}\} = \{\{\mathbf{I_{11}}, \mathbf{I_{12}}, ..., \mathbf{I_{1n_{6i}}}\}, \\ \{\mathbf{I_{21}}, \mathbf{I_{22}}, ..., \mathbf{I_{2n_{6i}}}\}, ..., \{\mathbf{I_{n_6 1}}, \mathbf{I_{n_6 2}}, ..., \mathbf{I_{n_6 n_{6i}}}\}\},\end{aligned} \tag{9}$$

For example, for $n_6 = 1$ $(i = \overline{1})$, $n_{61} = 2$ $(j = \overline{1,2})$, formula (9) can be presented as:

$$\mathbf{I_i} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{n_{6i}} \mathbf{I_{ij}}\}\} = \{\{\mathbf{I_{11}}, \mathbf{I_{12}}\}\}, \tag{10}$$

where: $\mathbf{I_{11}}$ = «Yes»; $\mathbf{I_{12}}$ = «No».

Considering the expression (10), namely the component $\mathbf{I_{12}}$, which consists of the answer "No", we get the following branch of the subset $\mathbf{I_{ij}}$:

$$\mathbf{I_{ij}} = \{\bigcup_{k=1}^{n_{6ij}} \mathbf{I_{ijk}}\} = \{\mathbf{I_{ij1}}, \mathbf{I_{ij2}}, ..., \mathbf{I_{ijn_{6ij}}}\}, \tag{11}$$

where $\mathbf{I_{ijk}} \subseteq \mathbf{I_{ij}}$ $(k = \overline{1, n_{6ij}})$ – the *k*-th subset of the groups of the taken actions to mitigate the losses clustered by a specific topic or grouped by certain characteristics within the bounds of the *ij*-th subset, and n_{6ij} the number of the groups of the *ij*-th subset.

Considering (11) the expression (9) can be presented as:

$$\begin{aligned}\mathbf{I} = \{\bigcup_{i=1}^{n_6} \mathbf{I_i}\} = \{\bigcup_{i=1}^{n_6} \{\bigcup_{j=1}^{n_{6i}} \mathbf{I_{ij}}\}\} = \{\bigcup_{i=1}^{n_6} \{\bigcup_{j=1}^{n_{6i}} \{\bigcup_{k=1}^{n_{6ij}} \mathbf{I_{ijk}}\}\}\} = \{\{\{\mathbf{I_{111}}, \mathbf{I_{112}}, ..., \mathbf{I_{11n_{6ij}}}\}, \\ \{\mathbf{I_{121}}, \mathbf{I_{122}}, ..., \mathbf{I_{12n_{6ij}}}\}, ..., \{\mathbf{I_{1n_{6i}1}}, \mathbf{I_{1n_{6i}2}}, ..., \mathbf{I_{1n_{6i}n_{6ij}}}\}\}, ..., \\ \{\{\mathbf{I_{n_6 11}}, \mathbf{I_{n_6 12}}, ..., \mathbf{I_{n_6 1n_{6ij}}}\}, \{\mathbf{I_{n_6 21}}, \mathbf{I_{n_6 22}}, ..., \mathbf{I_{n_6 2n_{6ij}}}\}, ..., \\ \{\mathbf{I_{n_6 n_{6i}1}}, \mathbf{I_{n_6 n_{6i}2}}, ..., \mathbf{I_{n_6 n_{6i}n_{6ij}}}\}\}\},\end{aligned} \tag{12}$$

For example, for $n_6 = 1$ $(i = \overline{1})$, $n_{61} = 2$ $(i = \overline{1,2})$, and for $n_{61} = 1$ $n_{611} = 0$ $(j = \overline{0})$, and for $n_{61} = 2$ $n_{612} = 3$ $(j = \overline{1,3})$, formula (12) can be presented as:

$$\mathbf{I} = \{\bigcup_{i=1}^{1} \mathbf{I_i}\} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{2} \mathbf{I_{ij}}\}\} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{2} \{\bigcup_{k=1}^{n_{6ij}} \mathbf{I_{ijk}}\}\}\} = \{\{\mathbf{I_{11}}, \{\mathbf{I_{121}}, \mathbf{I_{122}}, \mathbf{I_{123}}\}\}\},$$

where: $\mathbf{I_{121}}$ = «The new infrigement (data loss, deletion, data types) is similar to the previous one »; $\mathbf{I_{122}}$ = «The organisation has taken measures to remedy the problems that were identified in the previous infrigement»; $\mathbf{I_{123}}$ = «Availability of the penalty for new infringement».

The eighth component **C** – the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement, is defined by the expression:

$$\mathbf{C} = \{\bigcup_{i=1}^{n_7} \mathbf{C_i}\} = \{\mathbf{C_1}, \mathbf{C_2}, ..., \mathbf{C_{n_7}}\}, \quad (13)$$

where $\mathbf{C_i} \subseteq \mathbf{C}$ $(i = \overline{1, n_7})$ the *i*-th subset of the degree of cooperation with the supervisory authority, and n_7 their number.

For, $n_7 = 3$ $(i = \overline{1,3})$ formula (13) can be presented as:

$$\mathbf{C} = \{\bigcup_{i=1}^{3} \mathbf{C_i}\} = \{\mathbf{C_1}, \mathbf{C_2}, \mathbf{C_3}\},$$

where: $\mathbf{C_1}$ = «Degree of immediate involvement of management to the investigation of the supervisory authority»; $\mathbf{C_2}$ = «Employees, on their own initiative, gave evidence to the supervisory authority»; $\mathbf{C_3}$ = «The organisation has developed and submitted a Recovery Plan / Obtained a Supervisory Order».

The ninth **CA** – the category of personal data affected by the infringement, is defined by the expression:

$$\mathbf{CA} = \{\bigcup_{i=1}^{n_8} \mathbf{CA_i}\} = \{\mathbf{CA_1}, \mathbf{CA_2}, ..., \mathbf{CA_{n_8}}\}, \quad (14)$$

where $\mathbf{CA_i} \subseteq \mathbf{CA}$ $(i = \overline{1, n_8})$ *i*-th subset of the personal data criteria affected by the infringement, and n_8 their number.

For example, $n_8 = 3$ $(i = \overline{1,3})$ formula (14) can be presented as:

$$\mathbf{CA} = \{\bigcup_{i=1}^{3} \mathbf{CA_i}\} = \{\mathbf{CA_1}, \mathbf{CA_2}, \mathbf{CA_3}\},$$

where: $\mathbf{CA_1}$ = «The lost data on the staff organisation were unencrypted »; $\mathbf{CA_2}$ = «The lost data contained sensitive personal data of the organisation»; $\mathbf{CA_3}$ = « The lost data contained information on the criminal offenses of the organisation».

The tenth component **M** – the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; is defined by the expression:

$$\mathbf{M} = \{\bigcup_{i=1}^{n_9} \mathbf{M_i}\} = \{\mathbf{M_1}, \mathbf{M_2}, ..., \mathbf{M_{n_9}}\}, \quad (15)$$

where $\mathbf{M_i} \subseteq \mathbf{M}$ $(i = \overline{1, n_9})$ the *i*-th subset of the manner in which the infringement became known to the supervisory authority, and n_9 their number.

For example, $n_9 = 1$ $(i = 1)$ formula (15) can be presented as:

$$\mathbf{M} = \{\bigcup_{i=1}^{1} \mathbf{M_i}\} = \{\mathbf{M_1}\},$$

where: $\mathbf{M_1}$ = « The supervisory authority received a notice of infringement from:».

The subset $\mathbf{M_i}$ we define as:

$$\mathbf{M_i} = \{\bigcup_{j=1}^{n_{9i}} \mathbf{M_{ij}}\} = \{\mathbf{M_{i1}}, \mathbf{M_{i2}}, ..., \mathbf{M_{in_{9i}}}\}, \quad (16)$$

where: $\mathbf{M_{ij}} \subseteq \mathbf{M_i}$ $(j = \overline{1, n_{9i}})$ – the *j*-th susbet of the groups of the taken actions to mitigate the losses clustered by a specific topic or grouped by certain characteristics

within the bounds of the *i*-th subset, and n_{9i} the number of the groups of the *i*-th subset.

Considering (16) the expression (15) can be presented as:

$$\mathbf{M} = \{\bigcup_{i=1}^{n_9} \mathbf{M_i}\} = \{\bigcup_{i=1}^{n_9} \{\bigcup_{j=1}^{n_{9i}} \mathbf{M_{ij}}\}\} = \{\{\mathbf{M_{11}}, \mathbf{M_{12}}, ..., \mathbf{M_{1n_{9i}}}\}, \{\mathbf{M_{21}}, \mathbf{M_{22}}, ..., \mathbf{M_{2n_{9i}}}\}, ..., \{\mathbf{M_{n_9 1}}, \mathbf{M_{n_9 2}}, ..., \mathbf{M_{n_9 n_{9i}}}\}\}, \quad (17)$$

For example, for $n_9 = 1$ $(i = 1)$, $n_{91} = 4$ $(j = \overline{1,4})$, formula (17) can be presented as:

$$\mathbf{M} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{n_{9i}} \mathbf{M_{ij}}\}\} = \{\{\mathbf{M_{11}}, \mathbf{M_{12}}, \mathbf{M_{13}}, \mathbf{M_{14}}\}\},$$

where: $\mathbf{M_{11}}$ = «Trespasser»; $\mathbf{M_{12}}$ = «Informant»; $\mathbf{M_{13}}$ = «Media headlines»; $\mathbf{M_{14}}$ = «Other».

The eleventh component **ME** – where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures, is defined by the expression:

$$\mathbf{ME} = \{\bigcup_{i=1}^{n_{10}} \mathbf{ME_i}\} = \{\mathbf{ME_1}, \mathbf{ME_2}, ..., \mathbf{ME_{n_{10}}}\}, \quad (18)$$

where $\mathbf{ME_i} \subseteq \mathbf{ME}$ $(i = \overline{1, n_{10}})$ the *i*-th subset of the measures have previously been ordered against the controller or processor, and n_{10} their number.

For example, $n_{10} = 1$ $(i = 1)$ formula (18) can be presented as:

$$\mathbf{ME} = \{\bigcup_{i=1}^{1} \mathbf{ME_i}\} = \{\mathbf{ME_1}\},$$

where: $\mathbf{ME_1}$ = «Applied corrective measures in accordance with the Article 58 (a-h and j)».

The subset $\mathbf{ME_i}$ we define as:

$$\mathbf{ME_i} = \{\bigcup_{j=1}^{n_{10i}} \mathbf{ME_{ij}}\} = \{\mathbf{ME_{i1}}, \mathbf{ME_{i2}}, ..., \mathbf{ME_{in_{10i}}}\}, \quad (19)$$

where $\mathbf{ME_{ij}} \subseteq \mathbf{ME_i}$ $(j = \overline{1, n_{10i}})$ – the *j*-th subset of the groups of the taken measures to mitigate the losses clustered by a specific topic or grouped by certain characteristics within the bounds of the *i*-th subset, and n_{10i} the number of the groups of the *i*-th subset.

Considering (19) the expression (18) can be presented as:

$$\mathbf{ME} = \{\bigcup_{i=1}^{n_{10}} \mathbf{ME_i}\} = \{\bigcup_{i=1}^{n_{10}} \{\bigcup_{j=1}^{n_{10i}} \mathbf{ME_{ij}}\}\} = \{\{\mathbf{ME_{11}}, \mathbf{ME_{12}}, ..., \mathbf{ME_{1n_{10i}}}\}, \{\mathbf{ME_{21}}, \mathbf{ME_{22}}, ..., \mathbf{ME_{2n_{10i}}}\}, ..., \{\mathbf{ME_{n_{10}1}}, \mathbf{ME_{n_{10}2}}, ..., \mathbf{ME_{n_{10}n_{10i}}}\}\}, \quad (20)$$

For example, for $n_{10} = 1$ $(i = 1)$, $n_{101} = 2$ $(j = \overline{1,2})$, formula (20) can be presented as:

$$\mathbf{ME_i} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{n_{10i}} \mathbf{ME_{ij}}\}\} = \{\{\mathbf{ME_{11}}, \mathbf{ME_{12}}\}\},$$

where: $\mathbf{ME_{11}}$ = «Yes»; $\mathbf{ME_{12}}$ = «No».

The twelfth **AD** – adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; is defined by the expression:

$$\mathbf{AD} = \{\bigcup_{i=1}^{n_{11}} \mathbf{AD_i}\} = \{\mathbf{AD_1}, \mathbf{AD_2}, ..., \mathbf{AD_{n_{11}}}\}, \quad (21)$$

where $\mathbf{AD_i} \subseteq \mathbf{AD}$ $(i = \overline{1, n_{11}})$ *i*-th subset of the approved codes of conduct, and n_{11} their number.

For example, $n_{11} = 2$ $(i = \overline{1,2})$ formula (21) can be presented as:

$$\mathbf{AD} = \{\bigcup_{i=1}^{2} \mathbf{AD_i}\} = \{\mathbf{AD_1}, \mathbf{AD_2}\},$$

where: $\mathbf{AD_1}$ = «Availability of Code of Conduct for employees in the organisation (Article 40)»; $\mathbf{AD_2}$ = «Availability of a State certification mechanism of personal data protection means».

The subset $\mathbf{AD_i}$ we define as:

$$\mathbf{AD_i} = \{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}}\} = \{\mathbf{AD_{i1}}, \mathbf{AD_{i2}}, ..., \mathbf{AD_{in_{11i}}}\}, \quad (22)$$

where $\mathbf{AD_{ij}} \subseteq \mathbf{AD_i}$ $(j = \overline{1, n_{11i}})$ – the *j*-th subset of the groups of the taken measures to mitigate the losses clustered by a specific topic or grouped by certain characteristics within the bounds of the *i*-th subset, and n_{11i} the number of the groups of the *i*-th subset.

Considering (22) the expression (21) can be presented as:

$$\begin{aligned}\mathbf{AD} = \{\bigcup_{i=1}^{n_{11}} \mathbf{AD_i}\} = \{\bigcup_{i=1}^{n_{11}} \{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}}\}\} = \{\{\mathbf{AD_{11}}, \mathbf{AD_{12}}, ..., \mathbf{AD_{1n_{11i}}}\}, \\ \{\mathbf{AD_{21}}, \mathbf{AD_{22}}, ..., \mathbf{AD_{2n_{11i}}}\}, ..., \{\mathbf{AD_{n_{11}1}}, \mathbf{AD_{n_{11}2}}, ..., \mathbf{AD_{n_{11}n_{11i}}}\}\},\end{aligned} \quad (23)$$

For example, for $n_{11} = 2$ $(i = \overline{1,2})$, namely, for $n_{11} = 1$ $n_{111} =$ determining the availability of a Code of Conduct for employees in the organisation, and for $n_{11} = 2$ $n_{112} = 2$ $(j = \overline{1,2})$, formula (23) can be presented as:

$$\mathbf{AD_i} = \{\bigcup_{i=1}^{2} \{\bigcup_{j=1}^{n_{11i}} \mathbf{AD_{ij}}\}\} = \{\{\mathbf{AD_{11}}\}, \{\mathbf{AD_{21}}, \mathbf{AD_{22}}\}\},$$

where: $\mathbf{AD_{11}}$ = «Yes/No »; $\mathbf{AD_{21}}$ = «Yes»; $\mathbf{AD_{22}}$ = «No».

The thirteenth component **F** – any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement, is defined by the expression:

$$\mathbf{F} = \{\bigcup_{i=1}^{n_{12}} \mathbf{F_i}\} = \{\mathbf{F_1}, \mathbf{F_2}, ..., \mathbf{F_{n_{12}}}\}, \quad (24)$$

where $\mathbf{F_i} \subseteq \mathbf{F}$ $(i = \overline{1, n_{12}})$ the *i*-th subset of the infringement factors, and n_{12} their number.

For example, $n_{12} = 2$ $(i = \overline{1,2})$ formula (24) can be presented as:

$$\mathbf{F} = \{\bigcup_{i=1}^{2} \mathbf{F_i}\} = \{\mathbf{F_1}, \mathbf{F_2}\},$$

where: $\mathbf{F_1}$ = «Obtained the financial benefit of personal data leaking»; $\mathbf{F_2}$ = «Obtained the financial loss from personal data leaking».

The subset $\mathbf{F_i}$ we define as:

$$\mathbf{F_i} = \{\bigcup_{j=1}^{n_{12i}} \mathbf{F_{ij}}\} = \{\mathbf{F_{i1}}, \mathbf{F_{i2}}, ..., \mathbf{F_{in_{12i}}}\}, \tag{25}$$

where $\mathbf{F_{ij}} \subseteq \mathbf{F_i}$ ($j = \overline{1, n_{12i}}$) – the *j*-th subset of the groups of the taken measures to mitigate the losses clustered by a specific topic or grouped by certain characteristics within the bounds of the *i*-the subset, and n_{12i} the number of the groups of the *i*-th subset.

Considering (25) the expression (24) can be presented as:

$$\begin{aligned}\mathbf{F} = \{\bigcup_{i=1}^{n_{12}} \mathbf{F_i}\} = \{\bigcup_{i=1}^{n_{12}} \{\bigcup_{j=1}^{n_{12i}} \mathbf{F_{ij}}\}\} = \{\{\mathbf{F_{11}}, \mathbf{F_{12}}, ..., \mathbf{F_{1n_{12i}}}\}, \\ \{\mathbf{F_{21}}, \mathbf{F_{22}}, ..., \mathbf{F_{2n_{12i}}}\}, ..., \{\mathbf{F_{n_{12}1}}, \mathbf{F_{n_{12}2}}, ..., \mathbf{F_{n_{12}n_{12i}}}\}\},\end{aligned} \tag{26}$$

For example, for $n_{12} = 2$ ($i = \overline{1,2}$), $n_{12l} = 3$ ($j = \overline{1,3}$), formula (26) can be presented as:

$$\mathbf{F_i} = \{\bigcup_{i=1}^{2} \{\bigcup_{j=1}^{n_{12i}} \mathbf{F_{ij}}\}\} = \{\{\mathbf{F_{11}}, \mathbf{F_{12}}, \mathbf{F_{13}}\}, \{\mathbf{F_{21}}, \mathbf{F_{22}}, \mathbf{F_{23}}\}\},$$

where: $\mathbf{F_{11}}$ = «Yes»; $\mathbf{F_{12}}$ = «No»; $\mathbf{F_{13}}$ = «Unknown»; $\mathbf{F_{21}}$ = «Yes»; $\mathbf{F_{22}}$ = «No»; $\mathbf{F_{23}}$ = «Unknown».

The fourteenth component **RE** – recommendations. They are specified for all components 3 to 13. In this case, the variable n_{13} is a constant, and being 11 subsets. This component is defined by the expression:

$$\mathbf{RE} = \{\bigcup_{i=1}^{n_{13}} \mathbf{RE_i}\} = \{\mathbf{RE_1}, \mathbf{RE_2}, ..., \mathbf{RE_{n_{13}}}\}, \tag{27}$$

where $\mathbf{RE_i} \subseteq \mathbf{RE}$ ($i = \overline{1, n_{13}}$) the *i*-th subset component of the tuple, and n_{13} their number.

Since n_{13} =11 ($i = \overline{1,11}$), formula (27) can be presented as:

$$\begin{aligned}\mathbf{RE} = \{\bigcup_{i=1}^{11} \mathbf{RE_i}\} = \{\mathbf{RE_1}, \mathbf{RE_2}, \mathbf{RE_3}, \mathbf{RE_4}, \mathbf{RE_5}, \mathbf{RE_6}, \mathbf{RE_7}, \\ \mathbf{RE_8}, \mathbf{RE_9}, \mathbf{RE_{10}}, \mathbf{RE_{11}}\},\end{aligned}$$

where: $\mathbf{RE_1}$ = «Recommendations for the component N»; $\mathbf{RE_2}$ = «Recommendations for the component CH»; … $\mathbf{RE_{11}}$ = «Recommendations for the component F».

The subset $\mathbf{RE_i}$ we define as:

$$\mathbf{RE_i} = \{\bigcup_{j=1}^{n_{13i}} RE_{ij}\} = \{RE_{i1}, RE_{i2}, ..., RE_{in_{13i}}\}, \tag{28}$$

where $RE_{ij} \subseteq \mathbf{RE_i}$ ($j = \overline{1, n_{13i}}$) – the *j*-th of the groups of the taken measures to mitigate the losses clustered by a specific topic or grouped by certain characteristics

within the bounds of the *i*-th susbet, and n_{I3i} the number of the groups of the *i*-th subset.

Considering (27) the expression (28) can be presented as:

$$\begin{aligned}\mathbf{RE} = \{\bigcup_{i=1}^{n_{I3}} \mathbf{RE_i}\} = \{\bigcup_{i=1}^{n_{I3}} \{\bigcup_{j=1}^{n_{I3i}} RE_{ij}\}\} = \{\{RE_{11}, RE_{12}, ..., RE_{1n_{I3i}}\},\\ \{RE_{21}, RE_{22}, ..., RE_{2n_{I3i}}\}, ..., \{RE_{n_{I3}1}, RE_{n_{I3}2}, ..., RE_{n_{I3}n_{I3i}}\}\},\end{aligned} \tag{29}$$

For example, for $n_{I3} = 11$ ($i = \overline{1,11}$), $n_{I31} = 4$ ($j = \overline{1,4}$), $n_{I32} = 3$ ($j = \overline{1,3}$), $n_{I33} = 3$ ($j = \overline{1,3}$), $n_{I34} = 8$ ($j = \overline{1,8}$), $n_{I35} = 4$ ($j = \overline{1,4}$), $n_{I36} = 3$ ($j = \overline{1,3}$), $n_{I37} = 3$ ($j = \overline{1,3}$), $n_{I38} = 3$ ($j = \overline{1,3}$), $n_{I39} = 2$ ($j = \overline{1,2}$), $n_{I310} = 3$ ($j = \overline{1,3}$), $n_{I311} = 4$ ($j = \overline{1,4}$) and considering all the above listed examples formula (29) can be represented as:

$$\begin{aligned}\mathbf{RE} = \{\bigcup_{i=1}^{11} \mathbf{RE_i}\} = \{\bigcup_{i=1}^{11} \{\bigcup_{j=1}^{n_{I3i}} RE_{ij}\}\} = \{\{RE_{11}, RE_{12}, RE_{13}, RE_{14}\},\\ \{RE_{21}, RE_{22}, RE_{23}\}, \{RE_{31}, RE_{32}, RE_{33}\},\\ \{RE_{41}, RE_{42}, RE_{43}, RE_{44}, RE_{45}, RE_{46}, RE_{47}, RE_{48}\},\\ \{RE_{51}, RE_{52}, RE_{53}, RE_{54}\}, \{RE_{61}, RE_{62}, RE_{63}\},\\ \{RE_{71}, RE_{72}, RE_{73}\}, \{RE_{81}, RE_{82}, RE_{83}\}, \{RE_{91}, RE_{92}\},\\ \{RE_{101}, RE_{102}, RE_{103}\}, \{RE_{111}, RE_{112}, RE_{113}, RE_{114}\}\},\end{aligned} \tag{30}$$

where: RE_{11} = «Perform periodic inventory of data in the organisation»; RE_{12} = «Perform periodic analysis of deficiencies in the organisation's PD protection»; … RE_{113} = «Conduct internal audits to identify the controller / processor who created the conditions for the leakage of the subjects' PD and to investigate all possible gaps in ISMS»; RE_{114} = «Analyze the lost PD of the subjects and find out how the organisation has received the loss».

CONCLUSIONS

As a result of the study, a mathematical model for assessing the effects of personal data leakage in accordance with the provisions of the GDPR was developed B результаті, that allows the possibility to estimate the losses by any entity, institution or organisation in the event of infringement of one of the provisions of the GDPR. The model is based on the choice of the level of violation, to determine the maximum penalty ratio and the expert's responses, taking into account the components of Article 83 (2) of the GDPR, to determine the exact fine to the organisation and provide guidance on identifying and minimising deficiencies in the information security policy of the organisation.

REFERENCES

1. ДРЕЙС Ю., ЛОЗОВА І., ПЕДЧЕНКО Є.: Оцінювання негативних наслідків від витоку персональних даних. ITSec-2019: матеріали IX міжнар. наук.-техніч. конф., м. Київ, 22-27 березня 2019 року. Київ, 2019. С. 41-42.

2. Google fined €50 million for GDPR violation in France / Jon Porter // Policy : [website]. New York : Vox Media Inc, 2019. *URL: https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil*
3. Facebook could face up to $1.6 billion in fines over data breach as regulatirs eye formal probe / Arjun Kharpal // Tech : [website]. New Jersey : CNBC, 2018. *URL: https://www.cnbc.com/2018/10/02/facebook-data-breach-social-network-could-face-eu-fine.html*
4. Portuguese hospital receives and contests 400,000 € fine for GDPR infringement / Anna Oberschelp de Meneses, Kristof Van Quathem // Data Privacy : [website]. Washington : Convington & Burling, 2018. *URL: https://www.insideprivacy.com/data-privacy/portuguese-hospital-receives-and-contests-400000-e-fine-for-gdpr-infringement/*
5. Germany: first data protection authority issues GDPR fine / Privacy Matters : [website]. London: DLA Piper, 2018. *URL: https://blogs.dlapiper.com/privacymatters/germany-first-data-protection-authority-issues-gdpr-fine/*
6. First GDPR fine issued by Austrian data protection regulator / Gernot Fritz // Digital : [website]. London : Freshfields Bruckhaus Deringer, 2018. *URL: https://digital.freshfields.com/post/102f39w/first-gdpr-fine-issued-by-austrian-data-protection-regulator*
7. GDPR data protection impact assessments. Schaumburg : ISACA, 2017. 22 p. *URL: https://isaca-gwdc.org/wp-content/uploads/2018/01/GDPR_res_eng_0917.pdf*
8. General Data Protection Regulation. URL: *https://gdpr-info.eu/*