

Теоретико-множинне представлення параметру «Рівень порушення» для кортежної GDPR-моделі

УДК 004.056.5

Ірина Лозова¹, Євгеній Педченко²,
Анастасія Балайда³Національний авіаційний університет, ¹illozovaya@gmail.com,
²ydedchenko@intrasystems.ua, ³anasteisha.b.a@gmail.com

Для організацій, які здійснюють діяльність у просторі ЄС актуальним є питання відповідності нормам положень Регламенту GDPR, можливості оцінити власні масштаби збитку у разі його порушення та існуючі заходи забезпечення безпеки, щодо попередження витоку персональних даних.

Отже, постає задача розробки моделі, що дозволяє відповідно до положень Регламенту GDPR визначити множини вхідних та вихідних параметрів для формалізації процесу оцінювання збитків від втрати персональних даних.

Метою даної роботи є представлення параметру «Рівень порушення» з використанням теоретико-множинних підходів для побудови кортежної GDPR-моделі, що дозволить формалізувати процес оцінювання збитків від втрати персональних даних.

Один з параметрів кортежної GDPR-моделі є L – «Рівень порушення», що визначаємо виразом:

$$L = \left\{ \bigcup_{i=1}^{n_l} L_i \right\} = \{L_1, L_2, \dots, L_{n_l}\}, \quad (1)$$

де: L – множина усіх можливих рівнів порушень, $L_i \subseteq L$ ($i = \overline{1, n_l}$) – i -та підмножина рівнів порушення, а n_l кількість таких підмножин.

Наприклад, при $n_l = 2$ ($i = \overline{1, 2}$) формулу (1) можна представити як:

$$L = \left\{ \bigcup_{i=1}^2 L_i \right\} = \{L_1, L_2\} = \{\text{"Ст.83, п.4"}, \text{"Ст.83, п.5"}\},$$

де відповідно до Регламенту GDPR: $L_1 = \{\text{"Ст.83, п.4"}\}$ та $L_2 = \{\text{"Ст.83, п.5"}\}$, що відповідно трактується як: «На порушення таких положень, згідно з параграфом 2, поширюється застосування адміністративних штрафів сумою до 10 000 000 євро або, у випадку підприємства, до 2% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою» та «На порушення таких положень, згідно з параграфом 2, поширюється застосування адміністративних штрафів сумою до 20 000 000 євро або, у випадку підприємства, до 4% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою».

Далі, підмножину L_i визначимо як:

$$L_i = \left\{ \bigcup_{j=1}^{n_{ij}} L_{ij} \right\} = \{L_{i1}, L_{i2}, \dots, L_{in_i}\}, \quad (2)$$

де $L_{ij} \subseteq L_i$ ($i = \overline{1,2}$, $j = \overline{1, n_{i1}}$) – j -а підмножина груп рівнів порушення споріднених за певною темою чи близьких за певними характеристиками у межах i -ї підмножини, а n_{i1} кількість груп i -ї підмножини.

Відповідно до статті 83 (п.4, п.5) та, з урахуванням (2) вираз (1) можна представити у такому вигляді:

$$L = \left\{ \bigcup_{i=1}^{n_1} L_i \right\} = \left\{ \bigcup_{i=1}^{n_1} \left\{ \bigcup_{j=1}^{n_{i1}} L_{ij} \right\} \right\} = \{ \{L_{11}, L_{12}, \dots, L_{1n_{11}}\}, \{L_{21}, L_{22}, \dots, L_{2n_{21}}\}, \dots, \{L_{n_1,1}, L_{n_1,2}, \dots, L_{n_1, n_{n_1,1}}\} \}, \quad (3)$$

Тоді, наприклад, при $n_1 = 2$ ($i = \overline{1,2}$), $n_{11} = 3$ ($j = \overline{1,3}$), $n_{12} = 5$ ($j = \overline{1,5}$), формула (3) матиме вигляд:

$$L = \left\{ \bigcup_{i=1}^2 \left\{ \bigcup_{j=1}^{n_{i1}} L_{ij} \right\} \right\} = \{ \{L_{11}, L_{12}, L_{13}\}, \{L_{21}, L_{22}, L_{23}, L_{24}, L_{25}\} \} = \{ \{ "Cm.83, n.4, nn.a", "Cm.83, n.4, nn.b", "Cm.83, n.4, nn.c" \},$$

$\{ "Cm.83, n.5, nn.a", "Cm.83, n.5, nn.b", "Cm.83, n.5, nn.c", "Cm.83, n.5, nn.d", "Cm.83, n.5, nn.e" \} \}$

де: $L_{11} = \{ "Cm.83, n.4, nn.a" \}$, $L_{12} = \{ "Cm.83, n.4, nn.b" \}$, $L_{13} = \{ "Cm.83, n.4, nn.c" \}$, $L_{21} = \{ "Cm.83, n.5, nn.a" \}$, $L_{22} = \{ "Cm.83, n.4, nn.b" \}$, $L_{23} = \{ "Cm.83, n.4, nn.c" \}$, $L_{24} = \{ "Cm.83, n.4, nn.d" \}$ та $L_{25} = \{ "Cm.83, n.4, nn.e" \}$, що трактується як: «Обов'язки контролера і оператора відповідно до статей 8, 11, 25–39, і 42, і 43», «Обов'язки органу з сертифікації відповідно до статей 42 і 43», «Обов'язки органу з моніторингу відповідно до статті 41 (п.4)», «Основні принципи опрацювання, в тому числі умови надання згоди, відповідно до статей 5, 6, 7 і 9», «Права суб'єктів даних відповідно до статей 12–22», «Акти передавання персональних даних до одержувача в третій країні чи до міжнародної організації відповідно до статей 44–49», «Будь-які обов'язки відповідно до закону держави-члена, ухваленого згідно з главою IX» та «Невідповідність постанові або тимчасовому чи остаточному обмеженню на опрацювання чи призупинення потоків даних наглядового органу відповідно до статті 58 (п.2) або ненадання доступу як порушення статті 58 (п.1)».

Ієрархічну структуру параметра L можна представити у вигляді схеми на рис.

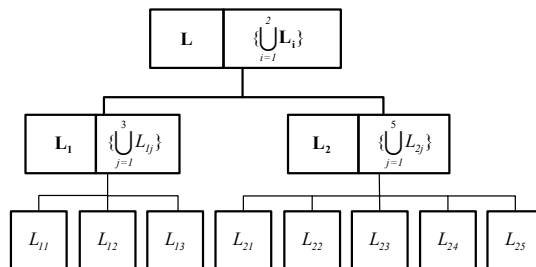


Рис. Ієрархічна структура параметра L

Отже, розроблено ієрархічну структуру та теоретико-множинне представлення параметра «Рівень порушення», що дозволить побудувати кортежну GDPR-модель, яка формалізує процес оцінювання збитків від втрати персональних даних.

Для фіналізації процесу створення GDPR-моделі в подальшому необхідно здійснити аналогічне представлення інших параметрів, що є складовими зазначеної моделі.