

## Розробка моделі системи оцінки негативних наслідків втрати персональних даних

УДК 004.056.5:005.8

Ірина Лозова<sup>1</sup>, Олександр Корченко<sup>2</sup><sup>1</sup>ДУ «Київський авіаційний інститут», *iryna.lozova@npp.kai.edu.ua*<sup>2</sup>Державний університет інформаційно-комунікаційних технологій, *o.korchenko@duikt.edu.ua*

Актуальність розробки моделі оцінки наслідків втрати персональних даних (ПД) відповідно до GDPR зумовлена вимогами ЄС щодо захисту ПД. Регламент зобов'язує організації оцінювати ризики для прав осіб у разі витоку, а стандартизована система допомагає своєчасно ухвалювати рішення щодо інформування та мінімізувати ризики штрафів, репутаційних і правових втрат.

Метою роботи є розробка моделі системи, що забезпечить організаціям дотримання вимог безпеки ПД, зниження ймовірності порушення конфіденційності та зменшення негативних наслідків втрати ПД.

Сучасні системи оцінки наслідків втрати ПД у контексті GDPR мають низку недоліків. Серед них – низький рівень автоматизації, складність інтеграції в бізнес-процеси, неврахування особливостей конкретних організацій, відсутність ефективного моніторингу та прозорої звітності, а також складність впровадження для малого та середнього бізнесу через високу вартість і складність алгоритмів.

На основі короткої GDPR-моделі параметрів ПД [1] та методу визначення негативних наслідків порушення конфіденційності ПД [2] сформовано структурну модель системи для оцінювання наслідків втрати ПД (див. рис. 1), до складу якої входять: блок формування та зберігання даних (БФЗД); блок ідентифікації та визначення рівня порушення (БВРП); блок формування експертної інформації (БФЕІ); блок обробки експертних даних (БООД).

БФЗД призначений для підготовки даних (суджень експертів) і складається з: бази даних (БД) групи питань (БДГП) – питання для аналізу ризиків; БД результатів опитувань (БДРО) – зібрані відповіді експертів; БД рекомендацій (БДР) – зберігає пропозиції щодо мінімізації ризиків.

БВРП складається з: модуля визначення загального глобального річного обігу (ЗГРО) – компонента  $T^{\Phi}$  формується шляхом визначення експертом річного обігу в €; модуля визначення показника рівня порушення (ПРП) –  $P_{PT}^{\Phi}$  обчислюється на основі множини визначених рівнів порушень, відносно яких формується коефіцієнт максимально можливого збитку.

БФЕІ – складається з модулів оцінювання та вибору певних характеристик порушення (специфіка порушення (СП), характер порушення (ХП), зниження шкоди (ЗШ), ступінь відповідальності (СВ), рецидив порушення (РП), рівень співпраці (РС), категорії даних (КД), спосіб виявлення (СПВ), відповідність заходам (ВЗ), дотримання кодексів (ДК), визначаючий чинник (ВЧ)), що засновується на конкретних оцінках діяльності підприємства, які в результаті сформулюють значення показників  $P_i^{\Phi}$  ( $i = \overline{1, 11}$ ), що в подальшому буде використано для обчислення сумарного збитку  $\phi$ -го підприємства.

