Формування параметрів оцінювання негативних наслідків витоку персональних даних в автоматизованих системах

УДК 004.056.5

Юрій Дрейс[1], Ірина Лозова[2]

Національний авіаційний університет, [1] dreisyuri@gmail.com, [2]illozovaya@gmail.com

З 25.05.2018 р. вступає в дію GDPR (General data protection regulation / Загальний регламент по захисту даних). Регламент є загальнообов'язковим документом без необхідності імплементації його норм до національного законодавства кожної країни-учасниці. Дія Регламенту буде поширюватися і на компанії, які здійснюють діяльність на території ЄС або в процесі своєї діяльності збирають дані громадян ЄС.

У зв'язку з цим захист персональних даних (ПД) та його вдосконалення є не просто обов'язком держави і предметом державно-правового регулювання, а повинні нерозривно розглядатися в поєднанні зі захистом прав та свобод людини, в тому числі захистом права на повагу до приватного життя. Крім того, створення дієвої системи захисту ПД належить до міжнародних зобов'язань України, пов'язаних із європейською інтеграцією нашої держави.

Метою роботи є розробка моделі оцінювання негативних наслідків витоку ПД під час їх обробки в автоматизованих системах (АС), яка дасть можливість в подальшому створити відповідний метод.

На національному рівні ключовими документами у сфері захисту ПД є Конституція України, Закон України «Про захист персональних даних», документи у сфері захисту ПД прийняті Уповноваженим ВРУ з прав людини. Наразі існує Типовий порядок обробки ПД за яким визначено загальні вимоги до обробки та захисту ПД суб'єктів ПД, що обробляються повністю чи частково із застосуванням АС. Конкретних способів, методів і засобів захисту та достатність їх застосування для досягнення необхідного рівня захищеності ПД оброблюваних в АС законодавством невизначено. Залишаються відкритими питання щодо архітектури ІТС/АС, остаточного вибору заходів захисту, технічних рішень та стандартів, якими необхідно керуватися, що покладаються в межах компетенції на володільців, розпорядників і власників цих систем разом з безпосередньою оцінкою ризиків порушень безпеки даних, тобто захисту ПД.

Для визначення вхідних, вихідних та внутрішніх параметрів забезпечення захисту ПД, які використовуються для оцінки ризиків, проведено дослідження міжнародних стандартів, актуальних законодавчих вимог та існуючих методик на основі яких розроблено модель оцінювання негативних наслідків витоку ПД під час їх обробки в АС, яка має типову структуру і містить набір параметрів представлення негативних наслідків витоку ПД, що обробляються в АС.

Дану модель представимо у вигляді кортежу:

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

де $\mathbf{IDF}_i \subseteq \mathbf{IDF}$ $(i = \overline{1,n})$ – компонент кортежу, що відображає *i*-й ідентифікатор ПД, *n* їх кількість, а для всіх членів **IDF** характерна властивість порядку.

Наприклад, при *n* = 9 кортеж (1) визначимо як:

$$\mathbf{IDF} = < \mathbf{IDF}_1, \mathbf{IDF}_2, ..., \mathbf{IDF}_7, ..., \mathbf{IDF}_9 > = < \mathbf{C, DO, P, A, CR, TH, L, R, MA} >, \quad (2)$$

де $\mathbf{IDF}_1 = \mathbf{C}$ (характеристика (Characteristic) ПД (ідентифікація їх складу та змісту); $\mathbf{IDF}_2 = \mathbf{DO}$ (загальновідомі документи (Documentation), що містять ПД); $\mathbf{IDF}_3 = \mathbf{P}$ (мета (Purpose) обробки ПД); $\mathbf{IDF}_4 = \mathbf{A}$ (аудит (Audit) застосованих механізмів безпеки); $\mathbf{IDF}_5 = \mathbf{CR}$ (множина критеріїв (Criterion) захищеності ПД, які обробляються в АС); $\mathbf{IDF}_6 = \mathbf{TH}$ (ідентифікація загроз (Threats) безпеці ПД при обробці БПД в АС); $\mathbf{IDF}_7 = \mathbf{L}$ (величина нанесених збитків (Losses) від втрати ПД); $\mathbf{IDF}_8 = \mathbf{R}$ (оцінка ризику (Risk) захисту ПД в АС); $\mathbf{IDF}_9 = \mathbf{MA}$ (управління (Management) ризиком та досягнення необхідного рівня захищеності ПД в АС).

Наприклад розглянемо перший компонент кортежу, де **C** – множина ідентифікаторів характеристик ПД (ідентифікація їх складу та змісту) відображається як:

$$\mathbf{C} = \{ \bigcup_{i=1}^{n_1} C_i \} = \{ C_1, C_2, ..., C_{n_1} \}, \quad (2)$$

де $C_i \subseteq \mathbf{C}$ $(i = \overline{1, n_1})$ – *i*-й ідентифікатор характеристик ПД, а n_1 їх кількість.

Наприклад, при $n_1 = 25$ $(i = \overline{1, 25})$ формула (2) набере вигляду:

$$\mathbf{C} = \{ \bigcup_{i=1}^{25} C_i \} = \{ C_1, C_2, ..., C_{24}, C_{25} \},$$

де C_1 = «Імена (ім'я, по батькові, прізвище) особи», C_2 = «Дата і місце народження», …, C_{24} = «Фотографія, інші художні твори, на яких зображено фізичну особу», а C_{25} = «Інші дані (видані на ім'я особи, тощо)».

У роботі розроблено модель оцінювання негативних наслідків витоку ПД в АС, в основу якої увійшли положення міжнародних стандартів та діючі вимоги законодавства України, яка дасть можливість розробити метод оцінювання негативних наслідків витоку ПД під час їх обробки в державних АС для забезпечення необхідного рівня захищеності при допустимих затратах і заданому рівні обмежень.

Науковий керівник – д.т.н., професор, Корченко О.Г.