УДК 004.056.5

Дрейс Ю.О. канд. техн. наук., доцент, старш. наук. співробітник,
Національна академія Служби безпеки України
Лозова І.Л., старш. викладач кафедри,
Національний авіаційний університет

РОЗРОБКА GDPR-МОДЕЛІ ПАРАМЕТРІВ ОЦІНЮВАННЯ НАСЛІДКІВ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ

В 2016 році вступив у дію новий закон Європейського союзу (ЄС) про захист персональних даних (ПД) – GDPR (General data protection regulation), який відрізняється безпрецедентними штрафними санкціями за порушення норм захисту ПД в організаціях ЄС, у тому числі й з українським капіталом. Після введення GDPR під його дію вже потрапило багато суб'єктів господарювання, зокрема: госпіталь в Португалії сплатив 400 тис. €, після того як були відкриті ПД клієнтів; соціальні медіа Германії сплатили 20 тис. € за збереження паролів у відкритому вигляді тощо. Навіть, такий «гігант» як Facebook сплатив 1,42 млн. € за порушення правил безпеки сторінок осіб членів ЄС.

Отже, на даному етапі для таких організацій, які здійснюють діяльність в просторі ЄС, *актуальним* є питання відповідності нормам положень регламенту GDPR, можливості оцінити власні масштаби збитку (наслідків) у разі розголошення ПД чи існуючі заходи забезпечення безпеки щодо можливого попередження їх витоку.

Метою роботи є розробка GDPR-моделі оцінювання негативних наслідків (збитків) суб'єктам господарювання від витоку ПД за європейським законодавством.

На основі проведеного аналізу регламенту GDPR визначено критерії та пропорції штрафів відповідно до статті 83(4,5) даного регламенту:

1) *сумою до 10 млн. € або до 2%* від загального глобального річного обігу за попередній фінансовий рік у випадку порушення однієї із статей: 8, 11, 25-39, 41, 42 та 43;

2) *сумою до 20 млн. € або до 4%* від загального глобального річного обігу за попередній фінансовий рік у випадку порушення однієї із статей: 5, 6, 7, 9, 12-22, 44-49, 58 та глави IX даного регламенту.

Відповідно до статті 83 (2), кінцева сума штрафу визначається, враховуючи порушення однієї, декількох або всіх компонент (параметрів) даної статті GDPR. Тому, GDPR-модель розроблено у вигляді кортежу цих параметрів [1]:

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

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

де $\mathbf{IDF_1 = T}$ -загальний глобальний річний обіг (turnover) підприємства за попередній фінансовий рік; $\mathbf{IDF_2 = L}$ -рівень (level) порушення; $\mathbf{IDF_3 = N}$ -специфіка (nature), ступінь тяжкості і тривалість порушення, а також кількість суб'єктів даних, які зазнали впливу, і рівень заподіяної їм шкоди; $\mathbf{IDF_4 = CH}$ -навмисний або недбалий характер (character) порушення; $\mathbf{IDF_5 = A}$ - дії (action), вжиті контролером або оператором для зниження рівня шкоди, заподіяної суб'єктами даних; $\mathbf{IDF_6 = R}$ -ступінь відповідальності (responsibility) контролера або оператора; $\mathbf{IDF_7 = I}$ -попередні порушення (infringements) з боку контролера або оператора; $\mathbf{IDF_8 = C}$ -рівень співпраці (cooperation) з наглядовим органом для відшкодування порушення і скорочення можливих негативних наслідків; $\mathbf{IDF_9 = CA}$ -категорії (categories) персональних даних на які вплинуло порушення; $\mathbf{IDF_{10} = M}$ -спосіб (manner) у який наглядовому органу стало відомо про порушення або якою мірою, контролер або оператор повідомив про порушення; $\mathbf{IDF_{11} = ME}$ -заходи (measures) вжиті щодо порушення, – відповідність цим заходам; $\mathbf{IDF_{12} = AD}$ -дотримання (adherence) кодексів поведінки відповідно до статті 40 або 42; $\mathbf{IDF_{13} = F}$ - обтяжуючий чи пом'якшуючий фактор (factor) такий як отримана фінансова вигода, застосований до обставин справи або витрати, яких вдалося уникнути прямо чи опосередковано від порушення; $\mathbf{IDF_{14} = RE}$ - рекомендації (recommendations)).

В результаті розроблено математичну модель оцінки наслідків від витоку персональних даних відповідно до GDPR, що дає можливість оцінити збитки суб'єкту господарювання у разі порушення одного з положень регламенту. GDPR-модель побудовано за принципом вибору рівня порушення з коефіцієнтом максимального штрафу та відповідей експерта відповідно до компонентів (параметрів) статті 83(2) регламенту, що реалізує подальше визначення величини нанесених збитків (шкоди) і надає необхідні рекомендацій щодо виявлення та мінімізації недоліків у політиці інформаційної безпеки організації.

Література:

General Data Protection Regulation, GDPR; Regulation (EU) 2016/679 (укр.), URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf