Оцінювання негативних наслідків від витоку персональних даних

УДК 004.056.5

Юрій Дрейс, Ірина Лозова[1], Євгеній Педченко[2]

Національний авіаційний університет
[1]illozovaya@gmail.com, [2]zhenia1398@gmail.com

В 2018 році вступив у дію новий закон Європейського союзу (ЄС) про захист персональних даних (ПД) – GDPR (Загальний регламент про захист даних), який відрізняється від існуючих 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, 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 такі «гіганти», як Google та Facebook також змушені були сплатити відповідні штрафи (Facebook сплатив 1,42 млн. € за порушення правил безпеки сторінок осіб членів ЄС).

Отже, можна зробити висновок, що на даному етапі для організацій, які здійснюють діяльність в просторі ЄС актуальним є питання відповідності нормам положень регламенту GDPR, можливості оцінити власні масштаби збитку у разі розголошення ПД та існуючі заходи забезпечення безпеки, щодо попередження витоку ПД.

Метою роботи є розробка програмної моделі оцінки негативних наслідків від витоку ПД організації відповідно до положень регламенту GDPR.

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 даної статті, як-от: a) специфіка, ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і рівень шкоди, заподіяної їм; b) навмисний або недбалий характер порушення; c) будь-які дії, вжиті контролером або оператором для зниження рівня шкоди, заподіяної суб'єктами даних; d) ступінь відповідальності контролера, зважаючи на технічні та організаційні інструменти, які вони застосовують відповідно до статей 25 і 32; e) будь-які належні попередні порушення з боку контролера або оператора; f) рівень співпраці з наглядовим органом для відшкодування порушення і скорочення можливих негативних наслідків порушення; g) категорії ПД, на які вплинуло порушення; h) спосіб, у який наглядовому органу стало відомо про порушення, зокрема, або, і якщо так, то якою мірою, контролер або оператор повідомив про порушення; i) якщо заходи, вказані в статті 58(2), було раніше призначено проти відповідного контролера або оператора щодо того самого питання, – відповідність цим заходам; j) дотримання затверджених кодексів поведінки до

статті 40 або затверджених кодексів поведінки відповідно до статті 42; k) будь-який інший обтяжуваний або пом'якшувальний фактор, застосовний до обставин справи, як-от отримана фінансова вигода або витрати, яких вдалося уникнути, прямо чи опосередковано, від порушення.

Для визначення порушення однієї з компонент, надається перелік питань з варіантами відповідей. Наприклад, для статті 83 (2a) передбачено наступні 4 питання та варіанти відповідей на них: 1) Який був найвищий рівень класифікації втрачених даних? (публічна, комерційна, конфіденційна, цілком таємна, заборонена); 2) Яка була протяжність порушення? (менше тижня, тиждень – місяць, місяць – 6 місяців, 6 місяців – рік, більше року); 3) Як багато суб'єктів ПД постраждало? (менше 1000, 1001 – 50000, 50001 – 100000, 100001 – 1000000, більше 1000000); 4) Якому впливу підлягали суб'єкти ПД? (незначному, низькому, середньому, високому, катастрофічному).

Варіанти відповідей оцінюються за бальною шкалою в градації від 0 до 5. В залежності від набраних балів формується коефіцієнт, за яким оцінюється рівень збитку для організації.

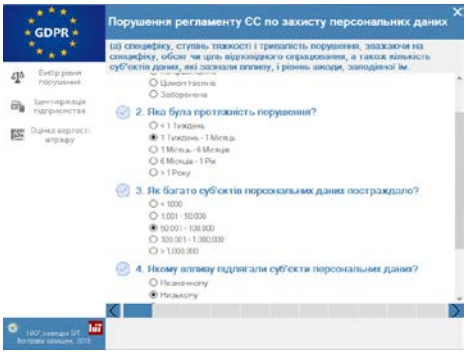

Рис. 1. Приклад вибору відповідей на питання статті 83(2a)

Наприклад, якщо загальний річний обіг організації за попередній фінансовий рік становив 1 млн. € і відбулося порушення статті 83(5), то максимальний штраф буде складати 40 тис. €. Далі, при визначенні кінцевої суми штрафу, з урахуванням відповідей експерта відповідно до компонент статті 83(2) організація отримає, наприклад, 45 балів (із 160 можливих), то кінцева сума штрафу буде складати відповідно 11 250 €.

В результаті роботи розроблено програмну модель, що надає можливість оцінити збитки будь-якому підприємству, установі чи організації у разі порушення одного з положень регламенту GDPR. Програмну модель побудовано на основі вибору рівня порушення, для визначення коефіцієнту максимального штрафу та відповідей експерта, з урахуванням компонент статті 83(2) регламенту GDPR, для визначення точного штрафу організації та надання рекомендацій, щодо виявлення та мінімізації недоліків у політиці інформаційної безпеки організації.