УДК 004.056

АНАЛІЗ ОСНОВНИХ РИЗИКІВ ПРИ ВПРОВАДЖЕННІ GDPR

Товкун Ю.І.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(066) 129-66-30, email: yuliia.tovkun@nure.ua

The modern vision of personal data protection involves an ongoing assessment of the risks that may arise for both the campaign and for other entities that are in one way or another associated with the company in the processing of personal data.

Risk assessments are essential to effective cybersecurity, helping organizations address issues that, if left unaddressed, can lead to chaos.

Organizations may mistakenly believe that the only risks they face come from cybercriminals trying to infiltrate their systems.

However, the GDPR makes it clear that data is also vulnerable to accidental or unlawful destruction, loss or disclosure.

Актуальність теми пов’язана з важливістю впровадження вимог GDPR в українських компаніях, що виходять на європейський ринок. Не дивлячись на те, що GDPR є внутрішнім актом Європейського Союзу (ЄС), у певних випадках він має екстериторіальну дію. Так, на значну частину українських компаній поширюється обов’язок GDPR compliance, що обумовлює наступне: якщо компанія виявить ризики, які мають високий рівень небезпеки у контексті обробки персональних даних (ПД), то ігнорування процедури мінімізації таких ризиків може призвести до застосування до компанії штрафних санкцій. GDPR охоплює набагато більше, ніж просто дотримання вимог регламенту. Він також може впливати на інші ризики, з якими компанії стикаються на регулярній основі [1].

У роботі розглянуто деякі з ризиків відповідності GDPR, яким слід приділити пріоритетну увагу в контексті впровадження GDPR.

1. Комплаєнс-ризики.

Розмір штрафів відповідно до GDPR є одним із головних приводів для занепокоєння більшості компаній. Штрафи накладаються за порушення відповідності – до 20 мільйонів євро або сума, що становить 4% від річного глобального обороту компанії, про яку йдеться [2].

2. Юридичні ризики.

Той факт, що GDPR поширюється на всі компанії, які опрацьовують дані громадян ЄС, викликає занепокоєння у компаній, які не розташовані в ЄС. Це також порушує питання про потенційні конфлікти з місцевим

законодавством, а також про так звані сірі зони для GDPR – правила боротьби з відмиванням грошей та подібних до них.

3. Ризики кібербезпеки.

В ідеалі всі компанії повинні спочатку мати відповідний рівень безпеки даних. На жаль, це не так, і компаніям слід приділяти пильну увагу своїм заходам щодо забезпечення безпеки та конфіденційності даних, оновлюючи та розширюючи їх за потреби.

4. Репутаційні ризики.

Ще одна частина ризиків, пов'язаних з дотриманням GDPR, стосується кількох нових прав, доступних кожному громадянинові ЄС. До них відносяться право дізнатися, які дані про громадян зберігає фірма, право стерти ці дані, тощо [2].

5. Ризики, пов'язані з новими продуктами.

Вимога проведення оцінки впливу на захист даних (DPIA) та інших оцінок змушує деякі компанії сильно змінити свої поточні графіки та операційні механізми, щоб реалізувати принцип безпеки "за умовчанням", пов'язаний з GDPR, для всіх оброблюваних даних [1].

Під час кожної оцінки ризиків необхідно враховувати кілька важливих моментів [3]. Першим з багатьох кроків є розуміння як типу, так і характеру ПД, які компанія обробляє на регулярній основі. Після визначення того, які особисті дані є у компанії і як вони обробляються, вирішуються питання щодо захисту інформації та мінімізації ризиків.

Крім того, дотримання GDPR також вимагає, щоб було підтверджено відповідальність перед різними органами захисту даних як у формі документального підтвердження зусиль із забезпечення безпеки, так і у формі демонстрацій [1].

Отже, компанія завжди повинна бути готова до ідентифікації нових ризиків та бути спроможною вирішувати питання щодо їх мінімізації. Саме така готовність, у поєднанні з іншими заходами, що реалізуються, допоможе компанії мати статус GDPR compliance на постійній основі.

Список використаних джерел:

1. GDPR [Електронний ресурс] – Режим доступу до ресурсу: https://gdpr-info.eu/.

2. Risk assessment and GDPR [Електронний ресурс] – Режим доступу до ресурсу: https://www.cpprotect.com/blog/gdpr-compliance-risks/# GDPR_compliance_risks.

3. Добринін І.С., Мальцева Н.О. Вдосконалення методики факторного аналізу інформаційних ризиків //Системи обробки інформації. – 2017. – №3. – С. 146-150.