УДК 004.77

**GENERAL DATA PROTECTION REGULATION ТА ЙОГО ВПЛИВ НА КІБЕРБЕЗПЕКУ**

автор: Голуб’ятніков А.С., науковий керівник: к.п.н. Блозва А.І.

Останнім часом в світі нерідко спостерігаються випадки зламів приватних компаній з метою викрадення персональних даних фізичних осіб. Заголовки новин містять безліч повідомлень про зломи комерційних структур, витік даних, електронне шахрайство, порушення функціонування державних структур або критично важливих об’єктів інфраструктури, крадіжку інтелектуальної власності, витоки інформації, пов’язаної з національною безпекою, тощо. Кіберзлочинність з роками набирає обертів.

Зовнішніми загрозами для бізнесу є: шкідливе програмне забезпечення, DDoS-атаки, фішингові атаки, проникнення у мережу, втрата пристроїв зі збереженими паролями та інші. Внутрішніми найпопулярнішими загрозами є вразливе програмне забезпечення та витоки через співробітників або з їх вини. Збільшення обсягів клієнтських даних, що оброблюються, і зростаюча роль інтелектуальної власності в успіху продукту призводять до виникнення нових форм розкрадання інформації. На рис.1 наведено статистику (зібрана компанією ElevenPath), щодо витрат в світі на забезпечення безпеки бізнесу, статистику щодо втрачених даних та інше. Проблема кібербезпеки полягає у тому, що бізнес рідко використовує надійні антивірусні засоби чи спеціалізовані рішення щодо захисту від атак, вживає дії для захисту інформації та фінансових транзакцій [1].



Рис. 1. Статистика по кібербезпеці від компанії ElevenPath

​

В травні 2018 року в ЄС впровадили General Data Protection Regulation (GDPR) – загальний регламент про захист даних, який передбачає значні штрафні санкції за порушення його правил, які можуть сягати 4% від річного обігу підприємства або 20 млн євро (залежно від того, що є більшим), отримання прямої згоди від користувачів на обробку їхніх персональних даних. Вводиться можливість відкликання згоди на обробку даних. Суб’єкти данихмають право бути повідомленими про будь-які витоки даних протягом 72 годин з моменту виявлення такого витоку; право доступу до своїх даних – суб’єкт даних може отримати інформацію щодо того, чи обробляються його дані, які саме дані обробляються та з якою метою, у будь-якого оператора, право бути забутим, тобто право на повне видалення своїх даних з системи оператора, припинення використання даних та повідомлення іншим третім особам, які з ним пов’язані, про припинення використання даних; право отримувати всі свої дані, які є в оператора у структурованому вигляді, який широко використовується та у форматі для зчитування машинами з правом їх подальшої передачі будь-якому іншому оператору, право заперечення обробки своїх персональних даних [2].

GDPR в Україні повинні впроваджувати компанії, які, мають постійне представництво в ЄС, не мають постійного представництва, але обробляють персональні дані людей (суб'єктів персональних даних), які знаходяться в одній з країн ЄС і можуть мати громадянство іншої держави, співпрацюють з організаціями, які вже впровадили GDPR і для збереження свого статусу зобов'язані вибирати підрядника за тим же принципом.

Регламент стосується абсолютно всіх підприємств, які так чи інакше обробляють дані осіб, які перебувають в Європейському Союзі. Тобто якщо компанії поставляють свої товари або послуги фізичним особам на території ЄС, то вони зобов’язані дотримуватися європейський регламент щодо захисту персональних даних. А такими можуть бути ті компанії, які ведуть онлайн-продажу, туроператори, транспортні компанії. Вони хоч і знаходяться в Україні, але обробляють дані резидентів ЄС. Також під дію GDPR підпадають компанії, які проводять різні маркетингові дослідження, що охоплюють споживачів з Європи.

Компанії відчують відповідальність за збір, обробку та зберігання даних. Велика кількість даних вже не буде дорівнювати «хорошому результату», а буде, швидше за все, мати на увазі незнання і невміння ефективно використовувати її у своїй роботі. Розробка продукту або сервісу буде починатися з продумування та оцінки впливу й ризиків для даних вже до релізу, а не після. Кожен співробітник, який має доступ до персональної інформації буде обізнаний про правила і тому буде вже усвідомлено піклуватися про збереження персональних даних, тим самим дотримуючись базових правил щодо їх захисту.

З норм регламенту випливає, що розміщення персональних даних на хмарних сховищах вважається їх передачею третім особам. Варто остерігатися сховищ з низьким рівнем захисту, а також обмежити розміщення на них персональних даних. При цьому, якщо передача даних за допомогою хмарного сховища відбувається за межі ЄС без належної захищеності (псевдонімізації, шифрування, засекречування або у будь-який інший спосіб), такі дії є порушенням норм законодавства ЄС.

Згідно регламенту, кожен, хто надає свої персональні дані, має право на інформацію про їх обробку, право на доступ до даних, право на виправлення даних, на видалення даних, право на обмеження обробки, право переносу даних, право на їх заперечення, права щодо автоматизованого прийняття рішень, включаючи складання профілю та право знати про витоки даних[3].

Однією з основних змін, які привносить GDPR, є надання клієнтам права знати, коли їх дані були зламані. Організаціям доведеться якнайшвидше повідомляти відповідні органи, щоб гарантувати, що клієнти зможуть вжити відповідних заходів для запобігання зловживанню їхніми даними

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Legalitgroup.com [Електронний ресурс]: «Кібербезпека бізнесу це не лише технічні заходи». – Режим доступу: <https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/>

2. Yur-gazeta.com [Електронний ресурс]: «Кібербезпека у 2018 році: новий виклик для бізнесу, необхідність чи побажання?». – Режим доступу: <http://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/kiberbezpeka-u-2018-roci-noviy-viklik-dlya-biznesu-neobhidnist-chi-pobazhannya.html>

3. Zdnet.com [Електронний ресурс]: «What is GDPR? Everything you need to know about the new general data protection regulations». – Режим доступу: <https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/>