

Людмила Рибальченко

кандидат економічних наук, доцент

Олександр Косиченко

кандидат технічних наук, доцент

*(Дніпропетровський державний
університет внутрішніх справ)*

АКТУАЛЬНІСТЬ ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Із стрімким розвитком сучасних інформаційних технологій, ідентифікація фізичної особи є необхідною до надання багатьох послуг: надання кредитів, виплата допомоги, оплата комунальних послуг, робота з банківськими установами, оплата товару через інтернет тощо. Оскільки більшість подібних послуг надається через мережу та видалений доступ і без особистої присутності, можна із упевненістю сказати, що вимоги до захисту та безпеки персональних даних мають бути більш жорсткими. Персональні дані – це інформація, здатна ідентифікувати особу. Такими даними є: паспортні дані, відомості про соціальний та сімейний стан, власність на майно, освіта, професія та інше. Останнім часом стало з'являтися багато інших персональних даних: номери банківських карт, логіни та паролі від різних сервісів, дані зі смартфона, що дозволяють відстежити переміщення користувача та інше.

Для боротьби із шахрайством в багатьох країнах на законодавчому рівні розроблялися нові вимоги безпеки до компаній, які працюють з персональними даними. Цей процес носить постійний характер, оскільки інформаційні технології розвиваються і разом з ними з'являються все нові вимоги щодо забезпечення безпеки інформації. З іншого боку, такий розвиток штовхає злочинців на винахід нових методів розкрадання даних. Оскільки Україна підтримує курс європейського розвитку, розглянемо розвиток системи захисту персональної інформації в ЄС. Європейське законодавство вже більше трьох десятиліть удосконалює систему захисту персональних даних. В 1995 році на території Європи була введена директива, що зобов'язує країни, які входять до складу ЄС, забезпечити захист персональних даних громадян. Кожна європейська країна ухвалювала свої закони про захист персональних даних, які найчастіше не збігалися із законами інших країн ЄС. Багато міжнародних компаній, що передають дані через кордон, стали зазнавати великі труднощі, які пов'язані з дотриманням законів різних країн. Саме тому в 2012 році було вирішено створити загальний регламент GDPR (General Data Protection Regulation) по захисту персональних даних на території ЄС, який прийшов на зміну існуючої директиви.

Після декількох років переговорів регламент було затверджено 25

травня 2016 року. У травні 2018 року набуло чинності нове положення про захист даних. У числі нововведень — заборона на збір персональних даних компаніями і державою без дозволу з боку фізичної особи. Виключення допускаються тільки в тому випадку, якщо в країні існують законодавчі акти, які примушують до передачі інформації. Протягом двох років, до 25 травня 2018 року, усі компанії, які зберігають, передають і обробляють особисті дані європейців, зобов'язані були забезпечити безпеку таких даних відповідно до положень GDPR. Варто відзначити, що це також стосується компаній, що перебувають за межами країн ЄС, що працюють із персональними даними громадян європейських країн (наприклад, України).

Важливим для держав Європейського союзу є те, що підтверджувати дозвіл на обробку персональних даних можна не з 13, а лише з 16 років. На компанії з європейськими представництвами накладається ряд обмежень. Їм неможна виконувати обмін даними з іншими підрозділами, якщо не виконуються правила по захисту даних. Також неможна передавати інформацію владі США та іншим країнам. Слід зазначити, що в ЄС новий GDPR регламент привів до масового переходу інформаційних структур європейських підприємств у хмарні сховища. Для багатьох компаній витрати на відповідність вимогам GDPR у якості оброблювача даних є дуже великими, тому більшість європейських підприємств переводять свої інформаційні системи в хмарні сховища.

Захист персональних даних українців знаходиться на критично низькому рівні. Лише у 2011 році в Україні набув чинності Закон України «Про захист персональних даних» [1], згідно з нормами якого фізичні і юридичні особи повинні зареєструвати бази персональних даних у спеціальному реєстрі баз даних, роботу якого контролює Державна служба з питань захисту персональних даних.

Якщо на підприємствах створюються відомості про працівників, клієнтів та осіб, з якими компанія співробітничала або продає авіаквитки, туристичні послуги, проводить опитування, то таке підприємство зобов'язане зареєструвати таку базу даних. У випадку ж невиконання або неналежного виконання фізичними і юридичними особами вимог Закону України «Про захист персональних даних» передбачено покарання і адміністративна відповідальність за порушення законодавства про захист персональних даних» [2]. Кримінальна відповідальність відповідно до даного закону передбачена у випадку незаконного збору, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконної зміни такої інформації.

Усі персональні дані українців, починаючи з номера мобільного телефону і закінчуючи адресою проживання, сьогодні не захищені. Наприклад, усі неодноразово одержували СМС від різних служб таксі, магазинів, у яких ніколи не бували – це означає, що ваші особисті дані було продано. Можна навести багато інших прикладів, коли збирають персональні

дані у науковій сфері та найдивовижніше, що це відбувається у деяких вищих навчальних закладах юридичного профілю. При цьому збирають паспортні дані та податковий код. Це грубе порушення Закону України «Про захист персональних даних».

Характерно те, що спеціальне законодавство, розроблене в Україні для збереження й захисту персональних даних, фактично діє тільки в тому випадку, коли витік інформації походить із якихось державних установ і підприємств. Відповідальність може настати, тільки якщо власник цих даних звернувся в правоохоронні органи. Дуже небезпечна ситуація зараз існує у використанні баз персональних даних системи Мінздраву та інших державних установ України, які легко викрасти, бо вони практично не захищені.

Проконтролювати в Україні, як саме зберігаються та обробляються персональні дані, досить складно і майже не можливо. Система захисту персональних даних в Україні потребує державного моніторингу та реформування на законодавчому рівні. В умовах неухильно зростаючого рівня кіберзлочинності у світі та низького рівня інформаційної культури громадян, а також відсутності розуміння ними всіх можливих кіберзагроз, необхідно на державному рівні забезпечити захист громадян від витоку персональних даних. Вести боротьбу з кіберзлочинністю з використанням персональних даних можна тільки на основі системного підходу на усіх рівнях. Проблемою безпеки персональних даних повинно займатися не тільки відомство омбудсмена, але і структури, пов'язані з безпекою і правоохоронною діяльністю держави.

Проблема в Україні ще збільшується тим, що громадяни добровільно передають свої дані при одержанні різних дисконтних карт та інших випадках не замислюючись про можливі наслідки. Будь-який витік персональних даних здатен доставити серйозні фінансові неприємності. Проблеми безпеки персональних даних мають велике значення для безпеки громадян та держави. І що особливо важливо, необхідний особливий, високий рівень захисту персональних даних усіх, хто має відношення до захисту України від агресії з боку РФ.

1. General Data Protection Regulation (EU GDPR). The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex:02016R0679-20160504>

2. Закон України «Про захист персональних даних» (Відомості Верховної Зароди України (ВВР), 2010, № 34, ст. 481). Нова редакція №2297-VI від 30.01.2018.

3. Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних (Відомості Верховної Зароди України, 2011, N 50, ст. 549).

4. Rybalchenko L., Kosyuchenko O. Features of latency of economic crimes in Ukraine / L Rybalchenko, O. Kosyuchenko // Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. – 2019. – Special Issue № 1 (102). – P. 264-267.

5. Ludmila Rybalchenko, Oleksandr Kosyuchenko, Klinytskyi Illia. Ensuring economic security of enterprises taking into account the peculiarities of information security. Scientific journal «Philosophy, Economics and Law Review». Volume 1 (3), 2022. – p. 71-81.