УДК 347.426.6 : 343.45

ЧЕХОВСЬКА Марія Миколаївна

МЕТОДИЧНІ ПІДХОДИ ДО ОЦІНЮВАННЯ ЗБИТКІВ, ЗУМОВЛЕНИХ РОЗГОЛОШЕННЯМ ПЕРСОНАЛЬНИХ ДАНИХ

Постановка проблеми. Активний розвиток у нашій країні засад інформаційного суспільства створив умови для інформатизації багатьох сфер життєдіяльності. Одним із аспектів інформатизації є створення підприємствами, організаціями та установами усіх форм власності, органами державної влади або місцевого самоврядування, фізичними особами-підприємцями баз персональних даних, а також здійснення оброблення вказаних відомостей.

Захист персональних даних, зважаючи на законодавчо визначену необхідність підтримання статусу захищеності життєво важливих інтересів людини і громадянина, є складовою забезпечення національної безпеки України. Підкреслимо, що серед основних реальних та потенційних загроз національній безпеці, зокрема в інформаційній сфері, є саме "розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю" [1]. Інакше кажучи, оскільки конституційні права і свободи людини й громадянина є об'єктом національної безпеки, то до зазначеної сфери автоматично належать і персональні дані українських громадян.

Необхідно зазначити, що персональні дані відповідно до Закону України "Про захист персональних даних" за режимом доступу є інформацією з обмеженим доступом, оскільки це відомості або сукупність відомостей про фізичну особу [2]. Особливий статус цих даних також регламентується відповідними статтями Цивільного кодексу України, зокрема ст. 286 "Право на таємницю про стан здоров'я", ст. 299 "Право на недоторканність ділової репутації", ст. 301 "Право на особисте життя та його таємницю", ст. 302 "Право на інформацію" в частині недопущення використання та поширення інформації про особисте життя фізичної особи без її згоди [3].

Оскільки є імовірність витоку та розголошення персональних даних, прогнозована можливість завдання збитків суб'єкту, володільцю чи розпоряднику персональних даних.

Аналіз останніх досліджень і публікацій. Проблемам захисту персональних даних, зокрема впорядкуванню відповідної законодавчої бази, розробленню технікотехнологічних заходів, останніми роками приділяється все більше уваги. Так, зазначений напрям наукових досліджень висвітлювався у працях О.Ю.Баранова, В.М.Брижка, А.І.Марущака, О.І.Мервінського та ін. Водночас питання відшкодування заподіяних витоком персональних даних збитків або моральної шкоди вітчизняними науковцями не розглядалися.

Зважаючи на це, **метою статті** є визначення концептуальних положень методики оцінювання збитків, заподіяних суб'єктам відносин, пов'язаних із персональними даними, через витік інформації.

Виклад основного матеріалу. Відповідно до Закону України "Про захист персональних даних" до суб'єктів відносин, пов'язаних із персональними даними, належать суб'єкт персональних даних, тобто фізична особа, стосовно якої здійснюється оброблення її персональних даних; володілець та розпорядник персональних даних, а саме підприємства, установи й організації усіх форм власності, органи державної влади, місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані; треті особи [2].

У ст. 8 "Права суб'єкта персональних даних" Закону України "Про захист персональних даних" зазначається, що суб'єкт персональних даних може застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних. Крім того, порушення законодавства про захист персональних даних тягне за собою відповідальність, установлену законом (ст. 28 "Відповідальність за порушення законодавства про захист персональних даних" Закону України "Про захист персональних даних"). З огляду на зазначене, а також відповідно до ст. 177 "Види об'єктів цивільних прав" Цивільного кодексу України, в якій вказано, що інформація є об'єктом цивільних прав, особа, якій завдано збитків у результаті порушення її цивільного права, має право на їх відшкодування (ст. 22 "Відшкодування збитків та інші способи відшкодування майнової шкоди" Цивільного кодексу України) [2]. Крім того, за умов порушення особистого немайнового права фізичної особи, внаслідок чого їй завдано майнової та (або) моральної шкоди, ця шкода підлягає відшкодуванню (ст. 280 "Право фізичної особи, особисте немайнове право якої порушено, на відшкодування шкоди" Цивільного кодексу України).

Таким чином, безпосередньо витік, а також розголошення персональних даних можуть завдати шкоду чи збитки першим двом зазначеним категоріям суб'єктів персональних даних, тобто фізичній особі, державному або приватному підприємству чи установі, органу державної влади чи місцевого самоврядування. Також може йтися про відшкодування як моральної шкоди, так і прямих чи непрямих збитків.

У цьому випадку можна говорити про економічний та юридичний зміст категорії "збиток". Так, відомий український економіст С.В.Мочерний пропонує два підходи до визначення сутності збитків, відповідно до яких збитки трактуються як непередбачені витрати, втрата майна і грошей, недоотримана вигода або як шкода, заподіяна діяльністю чи діями одного суб'єкта господарювання іншим, довкіллю, людям [4, с. 258].

За п. 2 ст. 22 "Відшкодування збитків та інші способи відшкодування майнової шкоди" Цивільного кодексу України збитками є або втрати, яких особа зазнала у зв'язку зі знищенням або пошкодженням речі, а також витрати, які особа зробила або мусить зробити для відновлення свого порушеного права (реальні збитки); або доходи, які особа могла б реально одержати за звичайних обставин, якби її право не було порушене (упущена вигода) [2].

Збитки переважно відшкодовуються у повному обсязі, якщо договором або законом не передбачено відшкодування в меншому або більшому розмірі.

Водночас, відповідно до ст. 23 "Відшкодування моральної шкоди" Цивільного кодексу України особа має право на відшкодування моральної шкоди, завданої внаслідок порушення її прав. Моральна шкода зокрема полягає в душевних стражданнях, яких фізична особа зазнала у зв'язку з протиправною поведінкою щодо неї самої, членів її сім'ї чи близьких родичів; приниженні честі та гідності фізичної особи, а також ділової репутації фізичної або юридичної особи.

Моральна шкода, як правило, відшкодовується грішми. Розмір грошового відшкодування моральної шкоди визначається судом залежно від характеру правопорушення, глибини фізичних та душевних страждань [3]. Підкреслимо, що моральна шкода відшкодовується незалежно від майнової шкоди, яка підлягає відшкодуванню, та не пов'язана з розміром цього відшкодування.

На увагу також заслуговує те, що відповідно до Кодексу України про адміністративні правопорушення такий вид адміні-

стративного стягнення, як штраф, тобто грошове стягнення, накладається на громадян і посадових осіб за адміністративні правопорушення [5]. Економічний зміст зазначеної категорії є практично ідентичним із юридичним, тобто штрафом визнається матеріальна відповідальність фізичних і юридичних осіб за порушення правил або договірних зобов'язань у формі примусових стягнень [6, с. 557].

У випадку витоку та протиправного поширення персональних даних штрафи можуть накладатися за статтями 164-3 "Недобросовісна конкуренція", 188-39 "Порушення законодавства у сфері захисту персональних даних", 212-5 "Порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави", 212-6 "Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем" Кодексу України про адміністративні правопорушення.

Натомість згідно з Кримінальним кодексом України штрафом є вид покарання, який полягає у грошовому стягненні, що накладається судом у випадках і розмірі, встановлених в Особливій частині Кримінального кодексу [7]. Підкреслимо, що штраф можна віднести до непередбачених витрат, інакше кажучи, збитків.

У нашому випадку штрафом можуть каратися правопорушення, що передбачені такими статтями Кримінального кодексу України: ст. 132 "Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби", ст. 145 "Незаконне розголошення лікарської таємниці", ст. 361 "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку", ст. 361-1 "Несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації", ст. 363 "Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється". Як правило, розмір штрафу визначається судом залежно від тяжкості вчиненого злочину та з урахуванням майнового стану винного у межах від 30 неоподатковуваних мінімумів доходів громадян до 50 тисяч неоподатковуваних
мінімумів доходів громадян.

Таким чином, за наявності доказової бази найбільш зрозумілим і законодавчо врегульованим є визначення розміру штрафу через витік інформації, що містить персональні дані. Більше того, цей штраф є складовою збитків володільця та розпорядника персональних даних, тобто підприємств, установ і організацій усіх форм власності, органів державної влади, органів місцевого самоврядування, фізичних осіб-підприємців, які обробляють персональні дані, а також третіх осіб.

Фізичній особі, стосовно якої здійснюється обробка її персональних даних, витік та розголошення останніх може заподіяти здебільшого моральну шкоду та збиток, пов'язаний із зашкодженням репутації. Наголосимо, що за кордоном уже набув поширення Довідник з оцінювання впливу на приватне життя (Privacy Impact Assessment Handbook) [8]. Однак у цьому виданні дається характеристика процесу оцінювання ризиків, пов'язаних із впливом на приватне життя фізичної особи внаслідок використання її персональних даних [9]. Тобто безпосередньо фінансова складова витоку та розголошення персональних даних, а саме способи її вирахування, у довіднику відсутні. Передбачається, що кожне підприємство або установа з огляду на ступінь ризику може складати власну калькуляцію витрат на ліквідацію наслідків несанкціонованого витоку інформації та компенсацію потерпілим.

Окремої уваги заслуговує процес визначення збитку, заподіяного володільцям та розпорядникам персональних даних.

Так, фундацією Ponemon Institute щорічно проводиться дослідження "Annual Study : The Cost of data breach", результатом якого є визначення середньої вартості витоку одного приватного запису у різних секторах економіки [10].

Узагальнюючи висновки експертів, можна зазначити, що складовими вартості витоку інформації є:

– витрати на оповіщення постраждалих у письмовій формі;

– організація для постраждалих консультативної "лінії допомоги";

– сплата послуг консультантів з безпеки;

– сплата послуг юристів у випадку судових розглядів;

– витрати на проведення піар-компанії, спрямованої на відновлення іміджу;

– штрафи регулюючим органам;

– виплати постраждалим, зокрема за судовими рішеннями.

Вагомий відсоток становлять витрати, що пов'язані із збитком для репутації підприємства та, відповідно, подальшим відтоком клієнтури. Інакше кажучи, йдеться про упущену вигоду або прибуток, який недоотримала компанія внаслідок заподіяння збитку її іміджу, отже, втрати клієнтури.

Наголосимо, що середні витрати на усунення наслідків одного зафіксованого факту, пов'язаного з витоком даних, у 2011 році становили приблизно 5,5 млн дол. США [11]. Більше того, з плином часу вартість витоку інформації лише збільшується. Так, зважаючи на характер витоку даних, у 2011 році у порівнянні з попереднім роком вартість одного інциденту збільшилася на 22–37 дол. США [12].

Варто підкреслити, що системне вивчення фінансових наслідків витоку персональних даних здійснюється лише у Сполучених Штатах Америки. Останнім часом до моніторингу ситуації з витоком конфіденційної інформації долучились російські компанії. За результатами дослідження, проведеного аналітичним центром компанії Zecurion, у 2011 році було зареєстровано 819 інцидентів, а загальна сума збитків сягає понад 20 млрд дол. США, з яких більше 1 млрд припадає на російські компанії [13].

Для України проблематика витоку персональних даних та, як наслідок, оцінки й відшкодування збитків, заподіяних суб'єктам персональних даних, на сьогодні не набула першочергового значення. Це пояснюється не лише початковим етапом у формуванні вітчизняного сегменту баз персональних даних, а й відсутністю механізму інформування суб'єктів персональних даних про витік або неавторизоване їх використання. У той же час, зважаючи на швидкість інтеграційних процесів як суспільного, так і технологічного характеру, зазначені негативні аспекти інформатизації сучасного суспільства невдовзі стануть його атрибутом.

Висновки. Відомості щодо розмірів та наслідків фінансових виплат через витік персональних даних мають значення не лише для компенсації завданої шкоди. Оперування цими матеріалами дасть змогу оцінити збитки у випадку можливих витоку персональних даних або неавторизованого їх використання, а також реалізувати комплекс заходів із недопущення таких ситуацій у майбутньому.

Загалом можна констатувати, що визначення розміру збитків є індивідуальним для кожного випадку, оскільки залежить від цілого спектра вихідних даних, зокрема кількості осіб, яким завдано шкоду, їх бажання або небажання отримати матеріальну компенсацію, безпосередньо характеру втраченої інформації.

Для мінімізації ризиків, пов'язаних із витоком персональних даних, їх володільцю або розпоряднику варто зменшити кількість облікових даних, час зберігання такої інформації, ввести більш жорсткі заходи із забезпечення безпеки організаційного та технічного характеру, визначити орієнтований рівень наслідків утрати конфіденційності персональних даних.

Список використаних джерел

1. Закон України від 19 червня 2003 року № 964-IV "Про основи національної безпеки України" [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/964-15.

2. Закон України від 1 червня 2010 року № 2297-VI "Про захист персональних даних" [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2297-17.

3. Цивільний кодекс України : чинне законодавство із змінами та допов. на 7 вересня 2012 року : (Відповідає офіц. текстові). – К. : Алерта, 2012. – 344 с.

4. Економічний енциклопедичний словник : у 2 т. / [С.В.Мочерний, Я.С.Ларіна, О.А.Устенко, С.І.Юрій] ; за ред. С.В.Мочерного. – Львів : Світ, 2005. – Т. 1. – 616 с.

5. Кодекс України про адміністративні правопорушення : чинне законодавство із змінами і допов. на 1 вересня 2012 року : (Відповідає офіц. текстові). – К. : Алерта, 2012. – 260 с.

6. Економічний енциклопедичний словник : у 2 т. / [С.В.Мочерний, Я.С.Ларіна, О.А.Устенко, С.І.Юрій] ; за ред. С.В.Мочерного. – Львів : Світ, 2005. – Т. 2. – 568 с.

7. Кримінальний кодекс України : чинне законодавство із змінами і допов. на 21 вересня 2012 року : (Відповідає офіц. текстові). – К. : Алерта, 2012. – 182 с.

8. Privacy Impact Assessment Handbook. Version 2.0 [Електронний ресурс]. – Режим доступу : http://www.ico.org.uk /upload/documents/pia_ handbook_html_ v2/index.html.

9. Оценка рисков и защита персональных данных [Электронный ресурс]. – Режим доступа : http://anvolkov.blogspot.com/2010/06/blog-post_04.html.

10. Сколько стоит утечка банковской информации? [Электронный ресурс]. – Режим доступа : http://swissbankinginfo.blogspot.com/2012/05/blog-post_4268.html.

11. InfoWatch Traffic Monitor Enterprise. Контроль и классификация информационных потоков [Електронний ресурс]. – Режим доступу : http://www.infowatch.ru/sites/default/files/infowatch_traffic_monitor_enterprise_datasheet_russian.pdf.

12. Утечки данных [Электронный ресурс]. – Режим доступа : http://www.tadviser.ru/index.php.

13. Убытки российских компаний от утечек данных в 2011 г. превысили $ 1 млрд [Электронный ресурс]. – Режим доступа : http://ria.ru/economy/20120809/720111574.html.

Аннотация: В статье рассматриваются основные составляющие убытков, нанесенных субъекту, владельцу или распорядителю персональных данных вследствие утечки информации либо неавторизованного ее использования.

Ключевые слова: персональные данные, утечка информации, убытки.

Abstract: The article examines basic constituents of the losses, inflicted to the subject, proprietor or manager of the personal information, because of information leakage or its unauthorized use.

Key words: personal data, information leakage, losses.