УДК 1:340.1:316.324.8

БРИЖКО В.М., *доктор філософії (Ph.D.) з юридичних наук, старший науковий співробітник*

ПРАВОВИЙ ЗАХИСТ ТА БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ: СОЦІАЛЬНИЙ І КОМЕРЦІЙНИЙ АСПЕКТИ

Анотація. *Про основні підходи у принципах і механізмах нового порядку захисту та безпеки персональних даних в європейських правових стандартах та запровадження у національне законодавство універсального критерію захисту даних людини.*

Ключові слова: *інформаційне право, персональні дані, захист та безпека даних, правові стандарти.*

Summary. *About basic approaches in principles and mechanisms of a new order of protection and safety of the personal data in the European legal standards and introduction to the national legislation of universal criterion for the person’s data protection.*

Keywords: *information right, personal data, data protection and safety, legal standards.*

Аннотация. *Об основных подходах в принципах и механизмах нового порядка защиты персональных данных в европейских правовых стандартах и внедрении в национальное законодательство универсального критерия защиты данных человека.*

Ключевые слова: *информационное право, персональные данные, защита и безопасность данных, правовые стандарты.*

Постановка проблеми. Економічна та соціальна інтеграція у функціонуванні внутрішніх та транскордонних ринків, запровадження інформаційних технологій і мереж призвело до збільшення потоків обміну персональними даними між окремими фізичними особами, комерційними та державними структурами, об’єднаннями Європейського Союзу (далі – Союз). Одночасно з тим, що технології прискорюють розвиток економіки, забезпечують надання різних послуг та сприяють підвищенню добробуту, вони активно впливають на істотні зміни у сучасному соціальному житті. Це, перш за все, стосується існуючої проблеми вільного обігу персональних даних в межах Союзу, а також їх передачі у треті країни та міжнародні організації, за умов забезпечення при цьому високого рівня їх захисту та безпеки на законодавчій основі.

Вперше у світі головні міжнародно-правові принципи захисту персональних даних були закріплені Конвенцією Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28 січня 1981 р. № 108[1] [1, с. 66-72], основною метою якої було створення умов гармонізації національних законодавств в контексті *соціальних аспектів*. Згідно з Конвенцію РЄ № 108 збирання, накопичення, зберігання і поширення персональних даних може здійснюватися лише з дозволу особи, відомості про яку опрацьовуються, шляхом обробки електронних даних. Вказаний акт заклав фундамент узгодженості національних систем захисту персональних даних в країнах світу.

[1] Конвенція Ради Європи від 28 січня 1981 року № 108 та Додатковий протокол до неї від 8 листопада 2001 року / [пер. з англ. В. Брижко, О. Баранов від 2001 р.] : офіційно засвідчено МЗС України від 01.07.02 р. № 72/15-077-1412, ратифіковано Законом України від 06.07.10 р. № 2438-VI .

Через 24 роки, коли Інтернет тільки починав свій розвиток, Європейський Парламент і Рада прийняли Директиву 95/46/ЄС [1, с. 273-293], яка стала ключовим етапом у історії розвитку інформаційно-комунікаційного захисту та безпеки людини. Її головною метою вже було створення умов для гармонізації національних законодавств в контексті *економічних аспектів*.

З часом, у процесах глобалізації та міжнародного трансферту даних, стали проглядатися проблеми, які дедалі визначали появу нових загроз у сфері захисту персональних даних, пов’язаною з поширенням таких новітніх технологій, як “Інтернет речей” [2, с. 85-91], “Хмарні технології” [3, с. 47-59], “Великі Дані” [4, с. 58-63], що надають можливість отримання, несанкціонованої обробки, зберігання і використання значних обсягів даних, та їх конвергенція [4, с. 51-67].

Звичайне збирання, обробка та застосування персональних даних, завдяки можливостям соціальних мереж, користувачами яких є 347 млн. європейців [5] (Міжнародний союз електрозв’язку визначає глобальну чисельність користувачів Інтернету в 3,2 млрд. [6]), може надати багато відомостей про окрему людину, яка добровільно їх розміщує в мережі або з примусу надає. Паспортні дані, адреси і поштові зв’язки, номер телефону і телефонні розмови, родичі, наявність домашних тварин, історії хвороб і лікувань, особисті інтереси і бажання, відомості про пересування, про нерухомість та майновий стан, розмір доходів і податків, кредитні картки, купівельна активність, свідоцтва, довідки, квитанції, анкети прийому на роботу, реєстраційні відомості виборця, різні запити з Інтернету, аж до розміру взуття, можуть інкогніто накопичуватися, аналізуватися, фільтруватися, сортуватися і розміщуватися в невідомому докладному електронному досьє (базах даних) на будь-яку людину. Кожного разу після відвідування веб-сайта залишаються електронні сліди, які стають надбанням інших людей, що може бути використано без відома суб’єкта персональних даних для створення його різностороннього, навіть “викривленого портрета”.

В кращому разі збір та обробка персональних даних служать маркетинговим цілям. Комерсанти прагнуть зробити рекламу ефективною, спрямованою на потрібну аудиторію, а значить – адресною. Їм необхідно мати якомога більше персональних даних: стать, вік, рівень доходів, захоплення та багато ін. – все має значення. Звичайно фірми прагнуть відповідати очікуванням клієнтів і пропонують товари, в яких, як вони вважають, є потреба. Масова розсилка даних (інформації) у вигляді реклами та “спаму”, що нав’язується, активно “процвітає” як в Інтернеті, так і у будь-яких ЗМІ.

З іншої сторони, персональні дані збирають та використовують не лише для проштовхування на ринок якогось продукту, але дуже часто й для вимагання коштів, шахрайства, залякування, шантажу, на шкоду репутації і, взагалі, для маніпулювання свідомістю людини з політичною, економічною, навіть, образливою метою.

Сьогодні новітні технології визначають появу нових, значніших ризиків порушення прав на приватність людини. Яскравим прикладом цього є Інтернет речей, завдяки якому може здійснюватися несанкціоноване програмно-автоматизоване збирання та обмін даними між різнофункціональними пристроями. При цьому відомо, що повністю безпечним цифровий пристрій, підключений через мережу до іншого, неможливо зробити у принципі, а уразливість в одному пристрої може спричинити витік даних з іншого. Й це за тих умов діяльності фірм-розробників технологій, коли вони більше стурбовані питанням вартості пристроїв, функціональності і часу виходу на ринок, ніж захистом та безпекою.

В якості іншого прикладу підвищення незахищеності персональних даних громадян в умовах застосування новітніх технологій, можна вказати на так звані “Хмарні технології” з “хмарними сховищами”. При цих моделях обробки та зберігання даних використовуються численні віддалені в мережі сервери, що надаються в користування клієнтам третьою

стороною. Відомості про користувачів обробляється та зберігається в так званому віртуальному сервері. Маючи певні переваги, модель зберігання містить в собі потенційну загрозу безпеці, особливо коли йдеться про приватну інформацію. Фактично вона може бути доступна будь-яким Інтернет-провайдерам і, далі, будь-яким особам.

Вищенаведене, зокрема, й визначає те, що норми Директиви 95/46/ЄС вже не відповідають задачам ефективного захисту та безпеки персональних даних в Інтернеті. Поєднання пристроїв, послуг і мереж технологій Інтернет речей, Хмарних технологій тощо, які функціонують без участі фізичних осіб, призводить до необхідності створення багаторівневої і багатооб’єктної системи забезпечення інформаційної безпеки, що значно складніше, ніж відома донині мережева безпека [7]. Через це ЄС розпочав створення нової, складної правової бази в даній області, яка охоплювала б всі держави-члени ЄС, а також треті країни, які мають ділові стосунки з країнами ЄС.

Метою статті є визначення та узагальнення основних підходів у новому міжнародному та національному порядку захисту та безпеки персональних даних.

Виклад основних положень. 25 травня 2018 року в законодавстві Європейського Союзу у сфері захисту персональних відбулися найбільші за 2 десятиліття зміни. Вступили в дію нові принципи та правила обробки персональних даних. Вони раніше були затверджені Постановою Європейського Парламенту і Ради (2016 р.) і отримали назву “Пакет захисту даних” (з трьох документів), який визначає умови створення узгодженої нормативно-правової бази в усьому європейському регіоні (див. [8, с. 45-57; 9]).

Головним документом сучасних правових стандартів є Регламент (ЄС) 2016/679 від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)” (General Data Protection Regulation) [10; 11, с. 6-106].

Регламент (ЄС) 2016/679 (далі – Регламент) має на меті не просто удосконалення захисту та вільного обігу персональних даних фізичних осіб в межах Союзу, а забезпечення еквівалентного рівня та посилення захисту права всіх громадян ЄС щодо безпеки персональних даних. Основою його вимогою є узгодження законів про недоторканність даних на території ЄС та змін у підходах всіх організацій у всьому регіоні до вирішення проблеми забезпечення обов’язкової конфіденційності відомостей щодо персональних даних. Дотепер компаніям та іншим суб’єктам, що мають справу з персональними даними, доводиться враховувати правила щодо захисту даних 28 різних держав-членів ЄС.

У зв’язку з загальними значними проблемами в упорядкуванні інформаційних відносин, зокрема й в сфері захисту персональних даних, нові принципи та порядок їх забезпечення можуть видатися надто складними, проте вони визначаються серйозними наслідками. Вважаємо, що їх слід враховувати, оскільки вони безпосередньо стосуються будь-яких суб’єктів діяльності, зокрема, й в Україні.

Регламент (ЄС) 2016/679 містить 172 п. Преамбули та 99 статей (102 с.), які визначають 7 основних принципів обробки персональних даних, про які раніше у нас вже йшла мова (див. [10; 11]). Вони, згідно ст. 5 Регламенту, передбачають забезпечення наступного:

- ***“законність, справедливість і прозорість”*** **–** персональні дані мають оброблятися, використовуватися та поширюватися згідно закону, справедливо і прозоро по відношенню до суб’єкта даних. Обробка є законною та справедливою тільки за умови, якщо та тією мірою, якою виконується щонайменше одна з наступних умов:

- суб’єкт даних надав згоду на обробку її або його персональних даних для однієї або декількох конкретних цілей;

- обробка є необхідною для виконання контракту, стороною якого є суб’єкт даних, або для вжиття заходів на запит суб’єкта даних перед укладанням контракту;

- обробка є необхідною для виконання юридичних зобов’язань контролера;
- обробка є необхідною для захисту життєво важливих інтересів суб’єкта даних або іншої фізичної особи;
- обробка є необхідною для виконання завдання в інтересах суспільства або при виконанні службових повноважень, наданих контролеру;
- обробка є необхідною щодо обов’язкових юридичних інтересів контролера або третьої сторони, коли ці інтереси не перекриваються інтересами або основоположними правами та свободами суб’єкта даних, що потребують захисту персональних даних, зокрема якщо суб’єкт даних є дитиною. Цей пункт Регламенту не застосовується до обробки, що здійснюється державними органами при виконанні їх завдань.

Щодо прозорості обробки, то суб’єкт має одержати відомості про особу контролера, мету збору даних, а також бути обізнаний про ризики, захисні заходи та свої права стосовно обробки даних. Будь-яку інформацію про цілі, методи і обсяги обробки персональних даних контролер зобов’язаний висловлювати максимально доступно і простою мовою;

- ***“****обмеження цілей****”*** – персональні дані повинні збиратися лише для конкретних і законних цілей, використовуватися виключно в тих цілях, які заявлені компанією (он-лайн-сервісом) і не піддаватися подальшій обробці, яка несумісна з такими цілями. Якщо із первісної мети випливатиме інша, то згоду має бути дано для обох. Обробка з метою архівування згідно з суспільними інтересами, а також для цілей наукового чи історичного дослідження або статистики не повинна вважатися несумісною з початковими цілями;
- *“мінімізація даних”* – передбачає обмеження тими персональними даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються. Не можна збирати персональні дані в більшому обсязі, ніж це було визначено для цілей обробки;
- *“точність”* – передбачає наявність адекватності персональних даних відомостям про суб’єкта даних, які мають постійно підтримуватися в актуальному стані. Неточні та застарілі персональні дані, з урахуванням цілі, для якої вони обробляються, слід видаляти або виправляти без затримки;
- *“обмеження зберігання”* – персональні дані повинні зберігатися у формі, що дозволяє ідентифікувати суб’єкта даних не довше, ніж це необхідно для цілі, для якої вони обробляються. Персональні дані можуть зберігатися протягом тривалішого періоду виключно для цілей архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей. Регламент також уточнює, що компанії мають проводити регулярні перевірки з метою чищення носіїв даних (інформації);
- *“цілісність і конфіденційність”* – персональні дані повинні оброблятися у спосіб, що забезпечує належний захист, включаючи захист від несанкціонованої та незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів. Це функції контролерів, які повинні бути впевненими, що створені усі умови захисту та безпеки даних;
- *“підзвітність ”* – передбачає діяльність з: призначення у організаціях посадових осіб, що відповідають за захист персональних даних, ведення обліку, записів і перевірки дій з виконання принципів та порядку Регламенту.

Дія Регламенту не поширюється на обробку персональних даних, що стосується:

- обробки персональних даних фізичною особою у ході винятково особистої чи побутової діяльності та не пов’язаної з професійною чи комерційною діяльністю. Проте, Регламент застосовується до контролерів чи осіб, що здійснюють обробку даних, які забезпечують засоби для обробки персональних даних у ході такої особистої чи побутової діяльності;

- юридичних осіб, а також окремих підприємств. Проте, дія Регламенту поширюється на обробку персональних даних контролером або обробником, що пов’язана з пропозицією товарів або послуг та її контроль, які повинні здійснюватися незалежно від того, чи сама обробка відбувається у межах або поза межами Союзу. Моніторинг поведінки суб’єктів обробки даних тією мірою, якою їх дії відбуваються в межах Союзу, передбачає встановлення, чи відбуваються їх дії у мережі Інтернет, у тому числі потенційне використання технологій обробки персональних даних, що складається з профілювання фізичної особи, зокрема з метою прийняття рішень щодо неї чи нього або аналізу та передбачення її/його особистих уподобань, поведінки та настроїв;

- обробки персональних даних компетентними органами влади з метою запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, або виконання кримінальних покарань, у тому числі охорони і запобігання загрозам суспільній безпеці та вільне переміщення таких даних, що є предметом Директиви (ЄС) 2016/680 Європейського Парламенту та Ради [11, с. 107-158];

- файлів або груп файлів, а також їх титульних сторінок, не структурованих за конкретним критерієм;

- сфери національної безпеки та по відношенню до спільної зовнішньої політики та політики безпеки Союзу;

- анонімних відомостей про осіб, що померли;

- до діяльності судів та інших судових органів. Регламентом передбачена можливість доручити функції нагляду за такими операціями з обробки даних окремим органам судових систем держав-членів ЄС.

Розширення понять та визначень.

У Регламенті розширено поняття “персональні дані”, введені поняття “контролер”, “обробник” (“оператор” – *від авт.*), “відповідальний за захист персональних даних”, “профілювання”, “псевдонімізація”, “основна установа”, “наглядовий орган”, “заінтересований наглядовий орган”, встановлено “право на видалення” (“право бути забутим”), “право на переносимість даних”.

Згідно Регламенту “персональні дані” – це будь-яка інформація, яка стосується фізичної особи, що ідентифікована або може бути ідентифікована (“суб’єкт даних”); фізична особа, що може бути ідентифікована – це особа, яка може бути ідентифікована, прямо чи опосередковано, зокрема за такими ідентифікаторами, як ім’я, ідентифікаційний номер, відомості про місце розташування, он-лайн-ідентифікатор або на один чи декілька факторів, специфічних для фізичної, фізіологічної, генетичної, ментальної, економічної, культурної або соціальної ідентичності цієї фізичної особи.

Якщо раніше персональними даними вважалися тільки документи, що містять імена, адреси й т.ін., то зараз це визначення розширено. Дані, пов’язані з IP-адресами, е-поштою та cookie-файли[2], що зберігають суто індивідуальні відомості про користувача мережі також охоплюються положеннями Регламенту.

Існують певні типи персональних даних, що відносяться до категорії особливих або “чутливих” відомостей про особу. Це відомості, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання і членство в профспілках. Крім того, згідно ст. 9 Регламенту, до цієї групи віднесені генетичні та біометричні дані, які можуть використовуватися для ідентифікації фізичної особи.

[2] Cookie – це файли, які автоматично копіюються з Інтернету на комп’ютер користувача і надають відомості про нього. Несанкціоновано отриману від cookie-файлу інформацію можна прив’язати до зібраних раніше файлів баз даних і одержати “портрет” користувача.

Важливим є те, що персональними вважаються тільки ті дані, за якими особу можна *ідентифікувати*. Наприклад, пошта містить ім’я, прізвище і е-адресу, тому відноситься до персональних даних, а окрема адреса е-пошти – ні; ім’я і номер телефону – персональні дані, телефон/адреса самі по собі – просто дані. Якщо з даних стає щось відомо про людину (її місце роботи, контакти і інше), то вони відносяться до персональних. Також, будь-які відомості, до яких було застосовано псевдонім, який може бути віднесено до фізичної особи за допомогою використання додаткової інформації, повинні розглядатися як відомості про фізичну особу, що може бути ідентифікована.

Права суб’єкта даних *(фізичної особи)***.**

Регламент значно розширює права громадян ЄС стосовно контролю за своїми персональними даними. Суб’єкти даних мають право запрошувати підтвердження факту обробки їх даних, місце і мету обробки, категорії оброблюваних персональних даних, яким третім особам вони розкриваються, період, протягом якого дані оброблятимуться, а також уточнюватимуть джерело їх отримання і вимагатимуть їх виправлення. Більш того, суб’єкт даних має право вимагати припинення обробки своїх даних.

Регламент встановлює високі вимоги до формі отримання згоді на обробку даних. Згода людини на обробку її персональних даних повинна бути визначена у формі однозначно чіткого твердження про відповідний дозвіл. Наприклад, повідомлення на сайті про те, що суб’єкт даних автоматично дав згоду на збір і обробку його персональних даних, не є згодою фізичної особи. Згода повинна бути надана в активній дії, наприклад, письмовою заявою, зокрема електронним способом.

Суб’єкт даних має право на виправлення персональних даних, що стосуються його або її. Комісія ЄС відстоює право кожного користувача Інтернету в ЄС мати також **“**право бути забутим**”**, тобто право на видалення його/її персональних даних та припинення обробки. Пошукові системи і соціальні мережі зобов’язані стирати фото-[3] і інші відомості про суб’єкта даних на його вимогу**.** Обробка фотографій не повинна розглядатися як обробка особливих категорій персональних даних**.**

Суб’єкт даних має право заперечувати проти обробки його даних, яка здійснюється з метою прямого маркетингу, у тому числі профілювання, до ступеню, в якому це пов’язано з таким маркетингом, стосовно як початкової, так і подальшої обробки.

Діти заслуговують на особливий захист їх персональних даних. Не можна вимагати згоду на обробку в контексті надання профілактичних або консультаційних послуг безпосередньо у дитини. Згода повинна бути авторизована батьками (або законними представниками дитини). Віковий поріг авторизації встановлюється державами-членами ЄС окремо (від 13 до 16 років).

Фізичні особи повинні бути обізнані про ризики, правила, гарантії та права стосовно обробки персональних даних та здійснення своїх прав стосовно такої обробки.

Кожен суб’єкт даних має право подати скаргу до національного наглядового органу, зокрема у державі-члені, де він чи вона постійно проживає, та право на ефективні засоби правового захисту. У випадку проваджень проти контролера або обробника позивач повинен мати можливість подавати позов до судів держав-членів, де розташовані установи контролера або обробника або де проживає суб’єкт даних, за винятком випадків, коли контролер є державним органом держави-члена, що діє при здійсненні своїх публічних повноважень.

[3] Згідно українського законодавства, зйомка в публічних місцях повністю дозволена, але на території ЄС слід пям’ятати про європейські правила.

Згідно Регламенту, немає конкретних вимог до ступеню, порядку і способу захисту даних – кожен може вибирати правові засоби сам. Найпопулярніші способи анонімізувать їх – шифрування або псевдонімізація. Псевдонімізація – один з технічних та організаційних заходів забезпечення рівня безпеки, який відповідає наявним ризикам. Вона припускає структурну зміну даних таким чином, щоб персональні дані не могли бути віднесені до конкретного суб’єкта. Відділення імені від решти даних і заміна його іншим ідентифікатором також буде псевдонімізацією.

Обробка особливих категорій даних.

Персональні дані, які, за своїм змістом, є особливо чутливими (расове, етнічне і національне походження, політичні, релігійні, світоглядні вірування, членство у політпартіях, профспілках, стан здоров’я, біометричні, генетичні дані, статтева орієнтація, притягнення до адміністративної або кримінальної відповідальності) заслуговують на особливий захист. Однак, обробка може бути необхідною для забезпечення суспільних інтересів у сферах охорони здоров’я, правоохоронної діяльності тощо без згоди суб’єкта даних.

Відхилення від заборони на обробку особливих категорій дозволяється у випадках, коли це передбачено законодавством Союзу або держави-члена та забезпечено відповідними гарантіями, з метою захисту персональних даних та інших прав, якщо це відповідає суспільним інтересам, зокрема – обробка персональних даних в сфері трудового права, законодавства про соціальний захист, у тому числі пенсії та охорона здоров’я, а також моніторинг, сповіщення, запобігання та контроль розповсюдження інфекційних захворювань та інших серйозних загроз здоров’ю. Такі відхилення можуть дозволятися з метою управління послугами в галузі охорони здоров’я, для забезпечення якості та економічної ефективності процедур, що використовуються для розгляду заяв щодо пільг та послуг у системі страхової медицини, або для архівних цілей відповідно до суспільних інтересів, для цілей наукового чи історичного дослідження або статистики. Крім того, відхилення повинно дозволяти обробку таких персональних даних, якщо це необхідно для створення, оформлення або захисту юридичних претензій, як в судовому процесі, так і в ході адміністративної або позасудової процедури.

Якщо в ході електоральної діяльності робота демократичної системи держави-члена потребує від політичних партій компіляції персональних даних щодо політичних переконань населення, обробка таких даних може бути дозволена з міркувань суспільних інтересів, за умови встановлення гарантій індивідуальної конфіденційності.

Обов’язки суб’єктів обробки *(компаній, підприємств, організацій тощо).*

Регламент має екстериторіальну дію для всіх держав-членів ЄС. Суб’єкт обробки буде мати справу тільки з одним національним органом із захисту даних, що знаходиться в країні ЄС, де розташовані їх основні установи.

Встановлено, що будь-які компанії не мають права пропонувати товари або послуги та передавати, у зв’язку з цим, персональні дані до країн ЄС, якщо рівень захисту у них нижчий, ніж в ЄС або якщо вони не дотримуються правил ЄС щодо захисту даних. Передача даних із країн ЄС у треті країни та міжнародні організації передбачено здійснювати тільки у повній відповідності до цього Регламенту.

Виходячи з вищевказаного, діяльність філіалів, представництв українських організацій на території ЄС повинна повністю відповідати його вимогам. Важливим є те, що організації, що обробляють персональні дані європейців в Україні, при здійсненні моніторингу суб’єктів даних, профілюванні окремих осіб, наприклад, для з’ясування їх поведінки і потреб, а також реалізації он-лайн-продажу (наприклад, ж/д-, авіа-, автобусне перевезення, готелі, хостели і ін.), також підпадають під дію Регламенту.

Регламентом визначена заборона на збір персональних даних будь-якою компанією (і державою) без дозволу з боку фізичних осіб – відповідних суб’єктів права на них. Винятки допускаються лише в тому випадку, якщо в країні існують законодавчі положення, які примушують до передачі даних, що містять відповідну інформацію.

Компанії зобов’язані видалити зі всіх своїх баз даних анкаунти і інші дані суб’єкта права на персональні дані за першою його вимогою. Це означає, що таки компанії, як Facebook, Google, Twitter, а також будь-які Інтернет-магазини (он-лайн-магазини), туроператори, транспортні та маркетингові компанії, які знаходяться, зокрема в Україні, та обробляють дані резидентів ЄС мають виконувати правило “право бути забутим” відповідних суб’єктів права на персональні дані. Це право не абсолютне – якщо обробка здійснюється за приписом закону, суб’єкт не може реалізувати це правило. Особливо це стосується правоохоронної та судової діяльності, про що йдеться у іншому документі “Пакету” – у Директиві ЄС 2016/680 [11, с. 107-158].

Суб’єкти обробки даних зобов’язані надавати безкоштовно електронну копію персональних даних іншої компанії на прохання самого суб’єкта персональних даних. Це “право на переносимість даних” також є новацією, що введена Регламентом.

Суб’єкти обробки даних зобов’язані повідомляти наглядові органи (а в деяких випадках і суб’єктів даних) про будь-які порушення, пов’язані з персональними даними, впродовж 72 годин після виявлення такого порушення.

Суб’єкти обробки даних повинні розробити та прийняти внутрішню політику компанії[3] з захисту та обробки персональних даних, включаючи розробку і впровадження Кодексу поведінки у сфері захисту даних (див. [12, с. 27-30]), які відповідають вимогам Регламенту, а також упровадити заходи, що відповідають принципам захисту (зокрема, мінімізація і псевдонімізація обробки персональних даних, надання суб’єктам даних можливості контролювати їх обробку), навчати персонал, проводити перевірки діяльності з обробки даних, вести документацію з процесів обробки, упроваджувати заходи по вбудованій системі захисту даних “за умовчанням” для забезпечення умов конфіденційності інформації.

Загальна організація забезпечення обробки та захисту персональних даних.

Згідно Регламенту, в практичній діяльності організацій щодо захисту персональних даних головними є суб’єкт даних, контролер та процесор (оператор).

Суб’єкт даних – це фізична особа, персональні дані якої обробляються.

Контролер (фізична чи юридична особа, державний орган, агенція або інша установа – т.з. “власник” бази даних), визначає мету і засоби отримання персональних даних і несе велику юридичну відповідальність, ніж процесор. По суті контролери визначають необхідні дії з персональними даними і відповідають за їх обробку**.** Контролер зобов’язаний вести реєстр всіх дій, які здійснюються в процесі обробки персональних даних. Також контролер повинен вжити належні технічні і організаційні заходи для забезпечення того, щоб за умовчанням оброблялися тільки персональні дані, необхідні для кожної конкретної мети обробки.

Процесор (фізична чи юридична особа, державний орган, агенція або інша установа – т.з. “оператори”) є виконавцем обробки (тобто той, хто працює з базою), за дорученням контролера.

Контролер і обробник можуть бути однією особою.

---

[3] У Додатку до цієї роботи надаються рекомендації щодо плану внутрішньої політики забезпечення захисту персональних даних у комерційних організаціях: за матеріалами посібника для бізнесу Федеральної торгової комісії США, які, як вважаємо, будуть корисними будь-кому.

Призначення відповідального за захист персональних даних. Ця вимога обов’язкова для: всіх державних органів; організацій, чиї види діяльності передбачають масштабний і систематичний моніторинг окремих осіб; організацій, чиї види діяльності передбачають обробку спеціальних категорій даних або даних, що відносяться до медичних записів, правопорушень і кримінально-звинувачувальних вироків (судимостей).

Будь-яка організація може призначити співробітника з захисту даних для управління процесами обробки і контролю за дотриманням вимог Регламенту. При цьому організація повинна опублікувати відомості про такого співробітника, а також направити її національному наглядовому органу з захисту персональних даних.

Посадова особа, що відповідає за захист даних, може бути співробітником контролера або процесора, або виконувати завдання на основі контракту про послуги.

Суб’єкти персональних даних можуть звертатись до посадової особи, що відповідає за захист даних, з усіх питань, пов’язаних з обробкою їх персональних даних та з реалізацією їх прав згідно з Регламентом.

Національні служби з захисту персональних даних.

Регламент спрямовано на посилення національних служб із захисту даних за умов повної їх незалежності, що є важливим компонентом захисту фізичних осіб у зв’язку з обробкою їх персональних даних. Згідно ст. 51, 53, 57 Регламенту, кожна держава-член законодавчо забезпечує та покладає на один або декілька незалежних публічних органів (“наглядові органи”) відповідальність за виконання завдань, встановлених цим Регламентом, для того, щоб захистити фундаментальні права та свободи фізичних осіб у сфері обробки та сприяти вільному руху персональних даних у межах Союзу. Компетенція наглядових органів не поширюється на контроль операцій з обробки в судах, що діють у якості судового органу (ст. 55 Регламенту).

Якщо у державі-члені створено декілька наглядових органів, необхідно на законодавчому рівні створити механізм узгодженості, для забезпечення ефективної їх діяльності. При цьому, держава-член зобов’язана визначити наглядовий орган, що діятиме як головна контактна особа.

Повноваження наглядових органів повинні включати в себе можливість накладати тимчасові або остаточні обмеження, у тому числі заборони, на обробку персональних даних. Повноваження для розслідування в частині доступу до приміщень повинні бути реалізовані відповідно до конкретних вимог процедурного права держави-члена, таких як вимога отримання попереднього судового дозволу.

Кожен наглядовий орган діє абсолютно незалежно під час виконання своїх завдань та здійснення повноважень згідно з Регламентом. Кожна держава-член повинна забезпечити наглядовий орган кадровими, технічними та фінансовими ресурсами, приміщеннями та інфраструктурою, необхідними для ефективного виконання їх завдань та реалізації повноважень. Кожен наглядовий орган повинен мати окремий публічний щорічний бюджет, який може бути частиною загального державного бюджету.

Що стосується повноважень наглядових органів отримувати від контролера або обробника доступ до персональних даних та до їх приміщень, держави-члени мають приймати підзаконні акти, в межах цього Регламенту, що встановлюють правила з метою гарантування професійних зобов’язань збереження таємниці, тією мірою, якою це необхідно для узгодження права на захист персональних даних, із зобов’язанням збереження професійної таємниці. Це не повинно обмежувати існуючі зобов’язання держав-членів щодо прийняття правил збереження професійної таємниці, як цього вимагає законодавство Союзу.

За порушення Регламенту, кожен наглядовий орган повинен мати повноваження для накладання адміністративних штрафів. Крім того, держави-члени мають можливість встановлювати правила щодо кримінальних покарань, за порушення національних правил, прийнятих в рамках Регламенту, а також в позбавленні вигоди, отриманої через порушення його приписів.

Санкції. Регламентом посилюється відповідальність за порушення його правил як до компаній в ЄС, так і до зарубіжних фірм, якщо вони обробляють персональні дані фізичних осіб, що знаходяться в ЄС – розмір штрафу встановлено до 20 мільйонів Євро або 4 % від загального річного обігу компанії за попередній фінансовий рік, залежно від того, яка сума більше.

Загально-соціальне упорядкування відносин.

Регламент визначає необхідність узгодження правил, що врегульовують свободу слова та інформації, у тому числі включаючи публіцистичну, академічну, художню та/або літературознавчу форму, з правом на захист персональних даних. Обробка та зберігання персональних даних виключно для цілей журналістики або для академічного, художнього чи літературного виразу повинна підлягати звільненням від деяких положень цього Регламенту, якщо це необхідно для узгодження права на захист персональних даних та “права на свободу висловлювати свою думку і свободи інформації”, закріплених Статтею 11 Хартії (Статуту – *від авт.*) основоположних прав Європейського Союзу [13]. Це також стосується і обробки персональних даних у аудіо- та візуальній формі, у архівах новин та прес-бібліотеках. Винятки та відхилення повинні прийматися враховуючи права суб’єкта даних, контролера та обробника, передачу персональних даних до третіх країн або міжнародних організацій, незалежність наглядових органів та узгодженість в їх співпраці. Якщо такі винятки та відхилення відрізняються у різних державах-членах, повинен застосовуватися закон тієї держави-члена, яким керується контролер. Для врахування важливості права на свободу слова у будь-якому демократичному суспільстві, необхідна широка інтерпретація понять, що стосуються такої свободи, наприклад, у журналістиці.

Зберігання персональних даних має також бути законним, якщо це необхідно, для виконання юридичних зобов’язань або при виконанні службових повноважень, наданих контролеру, на підставі суспільного інтересу в галузі охорони здоров’я, або для архівних цілей, для цілей наукового чи історичного дослідження або статистики, або для створення, оформлення або захисту юридичних претензій.

Обробка персональних даних для архівних цілей відповідно до суспільних інтересів, для цілей наукового чи історичного дослідження або статистики має бути забезпечена відповідними гарантіями для прав і свобод суб’єкта даних згідно з цим Регламентом. Ці гарантії повинні мати технічні та організаційні заходи з метою забезпечення, зокрема, принципу мінімізації даних. Зазначена обробка персональних даних також повинна виконуватись за умови проведення контролером оцінки доцільності досягнення таких цілей через обробку даних, що не допускають ідентифікації суб’єктів даних, за умови існування відповідних гарантій (таких як, наприклад, псевдонімізація даних). Держави-члени повинні мати повноваження вводити, за особливих умов та за наявності відповідних гарантій для суб’єктів даних, специфікації та відхилення стосовно інформаційних вимог та прав на виправлення, видалення, права бути забутим, на обмеження обробки, на переносимість даних та права на заперечення при обробці персональних даних для архівних цілей відповідно до суспільних інтересів, для цілей наукового чи історичного дослідження або статистики. Умови та гарантії, про які йде мова, можуть вимагати особливих процедур для суб’єктів даних з метою реалізації таких прав, якщо це доцільно з урахуванням цілей

особливої обробки разом з технічними та організаційними заходами, спрямованими на мінімізацію обробки персональних даних на виконання принципів пропорційності та необхідності. Обробка персональних даних для наукових цілей також повинна відповідати іншим діючим законодавчим актам, таким як закони щодо клінічних випробувань. При цьому необхідно, зокрема, встановити особливі умови стосовно публікації або іншого способу розкриття персональних даних. Статистичні цілі передбачають, що результати обробки для цілей статистики не є персональними даними, але є узагальненими даними, і що її результат не використовується для рішень стосовно конкретної фізичної особи.

Згідно Регламенту доступ громадськості до офіційних документів може вважатися таким, що відповідає суспільним інтересам.

Підходи до захисту персональних даних в США.

Впродовж багатьох років Сполучені Штати і Європа по-різному підходять до захисту персональних даних. Деякі посадовці Сполучених Штатів стверджують, що не дивлячись на різні підходи, результати рівні. *“Сума форм захисту приватного життя в США рівна або більше, ніж одна форма у всьому Європейському Союзі”*, вважає Камерон Ф. Керрі [14], головний радник Міністерства торгівлі, що керує Агентством, зусилля якого спрямовані на допомогу різним галузевим групам, розробникам додатків, чия робота дуже слабо регулюється і особливо часто призводить до несанкціонованого збору і використання відомостей про споживачів, що є основною причиною гострих дискусій між американською корпорацією Google та представниками Комісії ЄС. Більш того, американські урядовці, торгові групи і технічні керівники, закликали законодавців Брюсселя переглянути реформу, яка здійснюється, оскільки, як вони вважають, єдине регулювання і універсальний підхід не можуть бути ефективними. Американські представники галузі телекомунікацій відзначають, що немає нічого більш прийнятного для торгівлі, ніж вільний Інтернет. “*Це не мудро мати одне надмірно широке регулювання, що закріплює підхід – “один розмір для всіх”, який перешкоджатиме або підриватиме здібність компаній до інновацій в глобальній економіці”,* говорить Кевін Річардс, старший віце-президент Федерального уряду, що відповідає за TechAmerica – торгову групу, яка представляє інтереси таких компаній, як Google і Microsoft. Для посадовців Сполучених Штатів і торгових груп деякі положення реформи здаються дуже жорсткими. Вони стверджують, що американський підхід, де застосовуються галузеві закони про конфіденційність на додатки до саморегулювання і контролю з боку органів Федеральної торгової комісії – є вдаліший.

У 2012 р. Президент США Барак Обама запропонував “Біль про право споживачів на конфіденційність” (Consumer Privacy Bill of Rights), який надав американцям багато з тих же базових прав і форм захисту, що і правила, які містяться в Регламенті ЄС. Вони включають: право на доступ до записів персональних даних в компаніях, право на виправлення цих записів і право обмеження персональних даних, які компанії збирають і зберігають. Але у 2017 р. Палата представників Конгресу і, далі, Сенат США проголосували резолюцію про скасування цього закону, що зобов’язує, зокрема, Інтернет-провайдерів одержувати дозвіл на використання персональних даних (запитувати) користувачів, включаючи, таке, як місцеположення клієнта і історія його перегляду Інтернет-сайтів. Прихильники скасування закону (Verizon, AT&T, Comcast і ін. представники крупних корпорацій ринку комунікацій) стверджують, що це підвищить конкуренцію на ринку. Але критики зазначають, що скасування закону сильно ударить по правам суб’єктів даних. Ричард Блументал, член Демократичної партії і сенатор США від Коннектикуту, назвав цю резолюцію *“прямою атакою на права людей, на приватність і на*

правила, які забезпечують, сприйманий як належне, базовий захист від нав’язливого і незаконного втручання корпорацій у використання соцмереж і веб-сайтів” [15].

Виходячи з того, що закон 2012 р. з великою вірогідністю буде остаточно скасований і Палатою представників, і Президентом Трампом, необхідна розробка нового набору правил забезпечення конфіденційності для Інтернет-провайдерів. Вони, можливо, будуть схожі на старі, накладаючи обмеження на використання відомості про дітей та про здоров’я, але в них не буде обмежень використання історії проглядання веб-сторінок, несанкціонованого застосування для комерції та ін. Тобто, Інтернет-провайдери одержать саме те, що хочуть, тоді як персональні дані суб’єктів даних знову будуть збиратися та продаватися.

Про поширення у світі активної комерціалізації персональних даних вже не раз повідомлялося, і Україна не виняток [16; 17]. Процес збору, обробки і поширення персональних даних давно перетворився на процвітаючий бізнес, а ринок персональних даних ще у 2006 р. досягав не менш як 3 млрд. доларів у рік [18]).

Крупні в США компанії по збору персональних даних, наприклад, Metromail, First Data Solution, Acxiom, володіють даними не менш як про 90 млн. сімей і 140 млн. людей. У їх базах зберігається, обробляється, а потім продаються відомості про ім’я, дні народження, адреси, паспортні дані, номера телефонів та телефонні дзвінки, родичів, свідоцтва, довідки, зміст різних квитанцій, розмір доходів і податків, об’єкти та предмети власності, подорожи, хвороби людини і ліки, які вона приймає та багато ін.

Легальні фірми з продажу інформації в США, як правило, засновані приватними детективами, що були поліцейськими або співробітниками служб безпеки. Те, що вони продають, часто не вважається секретною інформацією. Більш того, жоден федеральний закон США не захищає конфіденційність відомостей щодо історій хвороби, банківських рахунків, телефонних номерів і рахунків за телефонні послуги тощо. А суб’єкти підпільної мережі збирають і продають персональні дані, навіть якщо вони одержані незаконним шляхом. Складність боротьби з такою діяльністю полягає у тому, що багато фірм, що займаються інформаційним бізнесом, приходить і йде, міняє назви, закриває свої вузли в Інтернет і відкриває нові. Поки та якщо який-небудь представник влади захоче придивитися до такої діяльності, підпільний торговець міняє свою адресу та зникає.

Стан справ в Україні.

В Україні основним законом, що регулює відповідні відносини, є Закон України “Про захист персональних даних” від 2010 р. Проаналізувавши положення його різних редакцій (див. [9]), можна вважати українське законодавство прогресивним в контексті напрямів приписів Регламенту (зокрема включаючи принципи обробки, порядок отримання згоди суб’єкта, перелік категорій персональних даних із спеціальним статусом, прав суб’єктів і обов’язків володільців/розпорядників та ін.).

Проте, законодавство України поки не повністю відповідає деякім приписам Регламенту, зокрема, які передбачають обов’язкову наявність у державі системно-незалежної організаційної структури забезпечення захисту персональних даних, здатної ефективно працювати в умовах застосування інформаційно-комунікаційних технологій і великомасштабних мережевих систем передачі даних.

Відсутність ефективної загальнодержавної організаційної системи і дієвих механізмів захисту персональних даних, за умов обов’язкової відповідальності за правопорушення інформаційних відносин, ускладнюється низькою правовою поінформованістю громадян про можливості боротьби з несанкціонованим використанням та продажем їх персональних даних у різних, не виключено, шахрайських та маніпулятивних інтересах. В умовах слабкої організаційної активності держави в практичній боротьбі з порушеннями законодавства, люди, з різних обставин, зокрема, судово-процесуальними складнощами, не дуже

бажають займатися захистом та безпекою своїх персональних даних, хоча вони можуть складати предмет не тільки адміністративного, але й кримінального злочину. Як зазначається у [19]: *“…по діючому у нас закону “Про захист персональних даних” штрафні санкції за порушення складають максимум 200 неоподатковуваних мінімумів доходів громадян, а це 3,4 тис. грн. При цьому, керівнику фірми, що розповсюдив персональні дані громадян без їх згоди, можуть на перший раз просто виписати розпорядження – як би покартати. Якщо порушення повториться, то справа може дійти і до штрафу. А постраждалий через розповсюдження його персональних даних може звернутися до суду, зажадавши від кривдника виплатити йому моральний збиток. Якщо він доведе, як сильно постраждав через поширену інформацію, то може навіть одержати компенсацію морального збитку. Але це для нас – тільки теорія”.*

Головне тут у тому, що різні уявлення різних суб’єктів про тлумачення понять та категорій продовжує залишатися і, мабуть, завжди буде проблемою.

Суб’єкт даних (наприклад, постраждалий) може трактувати захист своїх персональних даних, як сам хоче. Питання у тому – а чи будуть компетентні органи тлумачити так само, і чи зуміє він в суді відстояти саме своє тлумачення?

Сьогодні чинними є понад 100 міжнародно-правових актів (Конвенцій, Протоколів, Директив, Рекомендацій ООН, РЄ, ЄС, ОБСЕ тощо), які прямо або опосередковано відносяться до правового регулювання захисту персональних даних (деякі з них див. у посібнику [1]). Вони мають дуже значну кількість декларацій та приписів, які не завжди сприймаються однозначно й зрозуміло, створюють можливість різних суб’єктивних тлумачень. При цьому вважається, що “заклики” та приписи повинні спрямовуватися на охоплення усіх випадків використання персональних даних людини у різноманітності життя. Але у всіх них ***відсутнє головне – вони не визначають універсально-загального критерію, як визначального фактора та мирила оцінки різних суб’єктивних уявлень***, на базі чого має оцінюватися та здійснюватися захист персональних даних людини в контексті її основоположних прав і свобод. Можливість запровадження вказаного критерію, в принципі, передбачена ще в 1981 році ст. 11 Конвенції РЄ № 108: *“Жодне з положень цієї глави не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб’єктам даних більший ступінь захисту, ніж передбачено цією Конвенцією”.*

На початку розробки проекту Закону України “Про захист персональних даних”, пропонувалось та аргументувалось (ще у 1998 р. та далі у інших роботах, зокрема у [20 – 23]) можливість запровадження у законодавство України такого, як ми вважали, *універсального критерію – “право власності людини на свої персональні дані”*, за умов обов’язкового забезпечення інтересів національної безпеки, економічного добробуту та прав людини. Іншими словами, пропонувалось основу захисту персональних даних розглядати, як *предмет особливо-унікального виду*, який юридично має *умовну форму права власності*, монополія на яке обмежується виключно законом.

Пізніше було запропоновано дещо інше визначення вищезазначеної категорії – *“право приватної власності людини на свої персональні дані”*, про що йдеться у [24].

Відповідь була та є незмінною – “персональні дані відносяться до особистих немайнових прав”. Й це стверджується у часи, коли завдяки сучасним інформаційним технологіям персональні дані людини активно та не санкціоновано збирають, пропонують у мережах та продають. Для будь-якої діяльності, зокрема пов’язаною з комерцією, персональні дані давно стали предметом та товаром, які не тільки збільшують матеріальні цінності і практично використовуються як звичайний об’єкт продажу/покупки, але вже є складовою світового ринку.

Проте, у законодавстві України до них продовжують застосовувати поняття “немайнові права”[4], з пристосуванням до нього слова “особистих”.

Початок цього було покладено в ЦКУ, а потім потрапило і в різні закони, зокрема, щодо персональних даних. Загальне словосполучення сприймається як тавтологія – “масло масляне” (у логіці – це помилка “порочного кола”) та сприяє підтримці “системи захисту”, яка в умовах застосування електронно-інформаційних засобів може функціонувати на підставі суб’єктивних уявлень вибіркової модальності про предмет судження.

Таким чином, з одного боку, маємо не вирішену юридичну суперечність між економічними реаліями використання персональних даних і їх статусом в законодавстві, а з іншого – поширену публічну риторику необхідності боротьби за свободи і права, хоча, нерідко, це має характер боротьби проти свободи і прав інших. І це все при тому, що захист цінової вартості відомостей, які складають інформаційний продукт під назвою “персональні дані”, не тільки забезпечує соціальний захист прав і свобод людини, але і складає економічний аспект у безпеці людини, які завжди пов’язані між собою.

До вказаного можна додати, у 2015 році було повідомлення [25] про те, що в Раді Європи почала здійснюватися робота по модернізації Конвенції Ради Європи № 108 та розробці *“універсальних норм розвитку соціальної взаємодії”*.

Висновки.

1. У травні місяці 2018 року вступили у дію нові екстериторіального принципу дії правила і порядок захисту персональних даних (“Пакет захисту даних”) для держав-членів ЄС, а також рекомендації до їх впровадження іншими країнами, що співпрацюють з ЄС, які так чи інакше обробляють дані осіб, що знаходяться в ЄС. Головним документом “Пакету” є Регламент ЄС 2016/679 від 27 квітня 2016 року.

Нові вимоги до обробки та захисту персональних даних досить серйозні та складні. Але в них є важлива позитивна сторона: легше дотримуватися єдиного набору правил захисту, обробки та поширення даних, ніж враховувати національні нюанси щодо персональних даних кожної окремої країни ЄС, як це доводилося робити до введення Пакету. Дотримання одного правила замість 28 (країн-членів ЄС) створює умови допомоги малим підприємствам і фірмам, що розвиваються, вийти на нові ринки. Комісія ЄС запевняє, що реформа спрямована на стимулювання економічного зростання шляхом скорочення витрат і бюрократії для компаній, що працюють в ЄС.

Для усіх держав-членів ЄС визначається необхідність підняття рівня організаційно-правової діяльності та суттєвого удосконалення національних механізмів захисту персональних даних в умовах розвитку та поширення інформаційно-комп’ютерних технологій. Це, перш за все, стосується необхідності підвищення ефективності у діяльності національних уповноважених (наглядово-регулюючих) органів.

2. Україна в питаннях захисту персональних даних спирається на європейські правові стандарти та міжнародно-правовий досвід. Але загальна організація захисту персональних даних в Україні потребує реформування. У держави немає достатньої законодавчої бази і єдиної структурно-регулятивної системи захисту персональних даних, що не сприяє поліпшенню та ефективності роботи в сучасних технологічних умовах. Держава, на жаль, не дуже проявляє активність у боротьбі з правопорушеннями у цій сфері.

Новий порядок захисту та забезпечення безпеки персональних даних, що визначається Регламентом (ЄС) 2016/679, встановив одну з головних умов – рівень та організація захисту прав фізичних осіб стосовно обробки їх персональних даних повинні

[4] До речі, ні в одному з міжнародно-правових актів або національних законів застосування до персональних даних такого словосполучення як *“особисті немайнові права”* взагалі не існує.

бути еквівалентними не тільки в усіх державах-членах ЄС, але і у інших країнах, яки мають з ними будь-які стосунки. Інакше відмінності у захисті прав фізичних осіб, зокрема того, що стосується обробки, використання та поширення персональних даних, можуть стати на заваді вільному обігу персональних даних та бути перешкодою для здійснення економічної діяльності з державами-членами Союзу. Ці обставини вимагають більш узгодженої структури загальнодержавної організації захисту персональних даних, за умов жорсткого контролю дотримання правил європейських правових стандартів, що може сприяти розвитку цифрової економіки у межах внутрішнього ринку та співпраці з державами ЄС.

Головне – фізичні особи в Україні повинні мати законодавчу можливість контролю застосування своїх персональних даних та гарантій про надання на це особисто-визначеної ними інформованої згоди. Цьому може сприяти запровадження в українське законодавство універсально-загального критерію – *“право приватної власності людини на свої персональні дані”*, монополія на яку обмежується виключно законом в інтересах національної безпеки, економічного добробуту та прав людини.

На превеликий жаль, задача примусити більше хвилюватися про це законодавця продовжує залишатися актуальною.

Додаток

Забезпечення захисту персональних даних у комерційних організаціях:

за матеріалами посібника для бізнесу Федеральної торгової комісії США [26].

План захисту персональних даних базується на 5 основних принципах:

1. ***Здійснення інвентаризації.*** Необхідно знати, які персональні дані та особисті відомості зберігаються у ваших архівах та на комп’ютерах.
2. ***Зменшення обсягів особистих відомостей та даних, що зберігаються.*** Необхідно зберігати тільки те, що потрібно для здійснення вашого бізнесу.
3. ***Захист відомостей та даних.*** Необхідно забезпечити захист особистих відомостей та відповідних даних у захищеному від стороннього доступу місці.
4. ***Видалення даних***. Необхідно ретельно ліквідувати те, що вам більше не потрібно.
5. ***Планування.*** Необхідно мати план реагування на випадки порушення захисту та безпеки даних.

Стаття 1. Здійснення інвентаризації

Ефективний захист даних починається з оцінки того, яку інформацію ви маєте, і з визначення того, хто має доступ до неї. Розуміння того, як персональні дані потрапляють до компанії, як переміщуються всередині і як виходять з неї, а також, хто має або може мати доступ до них, є важливим для оцінки слабких місць в системі захисту даних. Тільки після дослідження, як персональні дані переміщуються, можливо визначити способи для їх захисту.

1. Інвентаризуйте всі комп’ютери, ноутбуки, флеш-диски, диски, домашні комп’ютери та інше обладнання для того, щоб визначити, чи зберігає ваша компанія дані, які визначають інформаційну конфіденційність. Також необхідно здійснити структурування даних, якими ви володієте, за типом та місцезнаходженням: файли з даними і комп’ютерні системи є основними носіями даних або ваша компанія отримує персональні дані багатьма способами – через веб-сайти, від підрядників, через кол-центри і тому подібне. Щодо даних, які зберігаються на ноутбуках, домашніх комп’ютерах персоналу та флеш-дисках, інвентаризація буде вважатися закінченою тільки після того, як буде перевірено всі дані, які мають конфіденційність.

2. Відслідковуйте персональні дані у вашій компанії шляхом розмов з відділами продаж, персоналом з відділу інформаційних технологій, відділом кадрів, бухгалтерією і іншими відділами, що надають послуги. Отримайте повну картину щодо того:

(a) ***Хто відправляє персональні дані у вашу компанію*** – чи отримуєте ви її від клієнтів?; компаній, що займаються кредитними картками?; банків чи інших фінансових інститутів?; кредитних бюро?; інших компаній?

(b) ***Як ваша компанія отримує персональні дані*** – вони потрапляють через: веб-сайти?; електронну пошту?; пошту?, передаються через касові апарати в магазинах?

(c) ***Який вид інформації ви отримуєте на кожній вхідній точці*** – чи отримуєте ви інформацію щодо кредитних карток через Інтернет?; чи зберігає ваш бухгалтерський відділ інформацію про рахунки клієнтів до запитання?

(d) ***Де ви зберігаєте інформацію, що отримуєте на кожній вхідній точці*** – чи це централізована електронна база даних на індивідуальних ноутбуках, на дисках чи дискетах, в папках, філіях?; Чи знаходяться будь-які файли з даними вдома у ваших працівників?

(e) ***Хто має або може мати доступ до персональних даних*** – хто з працівників має дозвіл на доступ до даних?; чи може хтось ще отримати його? – зокрема щодо компаній, які встановлюють та оновлюють програмне забезпечення, яке ви використовуєте для обробки даних з кредитними картками?

3. Різні види даних – різні ризики. Звертайте особливу увагу на те, як ви зберігаєте дані, що ідентифікують особу: номери соціального захисту, інформацію щодо кредитних карт, фінансову інформацію та персональні дані. Це те, що злодії використовують найчастіше для того, щоб здійснити шахрайство чи крадіжку.

Стаття 2. Зменшення обсягів інформації, що зберігається

Якщо для бізнесу не має необхідності в силу дії законодавства у зберіганні персональних даних, не зберігайте їх. А краще, не збирайте їх. Якщо ж для бізнесу необхідні певні персональні дані, зберігайте їх тільки до тих пір, допоки вони вам необхідні.

1. Використовуйте номери соціального захисту тільки для необхідних та законних цілей, наприклад, для звітів про податки із сум, що виплачуються працівникам.

2. Закон вимагає від вас скоротити чеки по кредитних та дебетних картках, які надаються в електронному вигляді вашим клієнтам. Ви можете включити не більше ніж п’ять останніх значень картки, і повинні видалити дату закінчення.

3. Не зберігайте дані щодо кредитних карток клієнтів, якщо ці дані не потрібні для вашого бізнесу. Наприклад, не зберігайте номер рахунку та дату закінчення, якщо не маєте суттєвої потреби для їх зберігання. Зберігання такої інформації довше ніж це необхідно – підвищує ризик того, що відомості можуть бути використані через крадіжку чи шахрайство.

4. Перевіряйте стандартні налаштування вашого програмного забезпечення, яке зчитує номери кредитних карток клієнтів і обробляє трансакції. Іноді воно налаштоване на постійне зберігання даних. Змініть стандартні налаштування, для того щоб впевнитись, що ви не зберігаєте дані, які вам не потрібні.

5. Якщо необхідно зберігати дані для вашого бізнесу або у силу дії законодавства, розробіть задокументовану політику такого зберігання для того, щоб визначити, які дані повинні зберігатися, як захистити їх, як довго їх зберігати і як розпорядитись ними, забезпечуючи безпеку таких даних, коли вони вам більше не потрібні.

Стаття 3. Зберігання інформації у захищеному від стороннього доступу місці

Який найкращий спосіб захисту персональних даних, які необхідно зберігати? Це залежить від виду даних та того, як вони зберігаються. Найбільш ефективні плани зберігання даних базуються на ключових елементах: фізична безпека, електронна безпека, навчання персоналу та практика щодо безпеки підрядників та постачальників послуг.

3.1. Фізична безпека

1. Зберігайте паперові документи чи файли, а також CD-диски, жорсткі диски, драйвери, касети і резервні копії, що містять персональні дані, в кімнатах, що закриваються на замок, та в закритих папках. Обмежте доступ працівників тільки доступом для законних цілей необхідних для бізнесу. Контролюйте, хто має ключі і їх кількість.

2. Вимагайте, щоб відомості, які містить персональні дані, зберігалися в закритих папках. Нагадуйте працівникам не залишати документи з конфіденційною інформацією на столах та відкриті файли з персональними даними, після того як вони залишають свої місця.

3. Вимагайте від працівників класти документи на місце, вимикати їх комп’ютери і закривати папки з файлами і офісні двері по закінченню робочого дня.

4. Впроваджуйте необхідний контроль за доступом до будівлі вашої компанії. Розказуйте працівникам, що робити і кому дзвонити, якщо вони бачать незнайому особу.

5. Якщо є склади, обмежте доступ працівників тільки доступом у законних цілях, необхідних для бізнесу. Відслідковуйте, хто і коли має доступ до даних, що зберігаються на складі.

6. Якщо ви пересилаєте конфіденційну інформацію, використовуючи зовнішніх кур’єрів чи підрядників, зашифруйте дані і сформуйте перелік даних, що пересилаються.

3.2. Електронна безпека

Безпека комп’ютера є не тільки справою персоналу відділу інформаційних технологій. Ви повинні знати уразливості вашої комп’ютерної системи і слідувати порадам експертів у цій сфері.

3.2.1. Загальна безпека інформаційної мережі

1. Визначте комп’ютери чи сервери, де зберігаються персональні дані.

2. Визначте всі можливості підключення до комп’ютерів, де зберігаються персональні дані. Це може бути Інтернет, електронні касові апарати, комп’ютери у ваших філіях, комп’ютери, що використовуються вашими постачальниками послуг з підтримкою вашої інформаційної мережі, і бездротові пристрої, наприклад, стільникові телефони.

3. Оцініть слабкі місця для загальновідомих та обґрунтовано передбачуваних нападів під час кожного підключення.

4. Не зберігайте персональні дані на будь-якому комп’ютері, що підключений до Інтернету, окрім випадку, якщо це необхідно для ведення бізнесу.

5. Зашифровуйте персональні дані, які ви надсилаєте іншим особам по загальній мережі (Інтернет), і відслідковуйте зашифровані дані, що зберігаються у вашій мережі або на дисках чи портативних пристроях зберігання даних. Відслідковуйте відправлення електронної пошти в рамках вашої бізнес-діяльності, якщо вони містять персональні дані.

6. Регулярно встановлюйте сучасні антивірусні програми на персональних комп’ютерах і серверах вашої мережі.

7. Регулярно перевіряйте спеціалізовані веб-сайти і сайти ваших продавців програмного забезпечення на предмет наявності нових версій і впроваджуйте політику встановлення оновлень, що затверджені продавцями.

8. Перевіряйте комп’ютери вашої мережі на предмет визначення робочих систем та послуг мережі. Якщо ви знайдете програми, які вам не потрібні, деактивуйте їх, щоб запобігти потенційним проблемам щодо безпеки. У разі якщо електронна пошта чи Інтернет не потрібен на конкретному комп’ютері, розгляньте можливість закриття портів для таких послуг на цьому комп’ютері для того, щоб запобігти неавторизованому доступу до цього комп’ютера.

9. Коли ви отримуєте дані щодо переказів по кредитних картках і інші фінансові дані, використовуйте Протокол захищених сокетів[5] або інші види безпечного зв’язку, які захищають дані під час відправки.

10. Звертайте особливу увагу на безпеку ваших Інтернет-додатків – програмного забезпечення, що використовується для того, щоб надати дані відвідувачам вашої веб-сторінки і для отримання даних від них. Інтернет-додатки можуть частково бути пошкоджені хакерськими нападами. Під назвою “напад шляхом ін’єкції” хакери встановлюють команди, які націлені на зловмисні дії, що виглядають як законний запит даних. При цьому хакери у вашій системі пересилають дані з вашої мережі на їх комп’ютери. Відносно легкий захист від таких нападів доступний з багатьох ресурсів.

[5] Протокол, що гарантує безпечну передачу даних через мережу, комбінуючи криптографічну систему з відкритим ключем і блочне шифрування даних.

3.2.2. Управління паролями

1. Контролюйте доступ до даних, що містять конфіденційну інформацію, шляхом встановлення вимоги до працівників використання “сильних” паролів. Експерти з технічної безпеки кажуть, що чим довший пароль, тим це краще. Так як легкі паролі, такі як часто вживані слова, можна легко вгадати, вимагайте, щоб працівники вибирали паролі, які міститимуть літери, числа і символи. Вимагайте, щоб логін та пароль були різними і часто змінювалися.

2. Пояснюйте працівникам, чому надання будь-кому свого паролю або його запис будь-де за межами робочого приміщення є дією проти компанії.

3. Використовуйте програму захисту екрану, яка автоматично виключає комп’ютер працівника після певного періоду його не активності.

4. Відключайте користувачів, які ввели неправильний пароль певну кількість разів.

5. Попереджайте працівників про можливі крадіжки персональних даних шляхом запиту паролів. Повідомляйте працівникам, що запит їх пароля являється незаконною дією і що ні в кого не повинні вимагати розкриття їх пароля.

6. При інсталяції нового програмного забезпечення одразу ж змініть стандартні паролі продавців або постачальників на більш безпечні і надійні паролі.

7. Застерігайте працівників відправляти персональні дані (зокрема, номери соціального захисту, паролі, дані щодо рахунків) електронною поштою. Незашифровані електронні листи не є безпечним способом відправки даних.

3.2.3. Безпека ноутбуків

1. Обмежуйте використання ноутбуків тільки тими працівниками, які потребують їх для виконання їх роботи.

2. Оцініть, чи потрібно персональні дані дійсно зберігати на ноутбуці. Якщо ні, видаліть їх спеціальною програмою з їх очистки. Видалити файли, використовуючи стандартні команди, недостатньо, тому що дані можуть залишитися на жорсткому диску ноутбуку. Програми з очистки даних можливо придбати в більшості спеціалізованих магазинів.

3. Вимагайте від працівників збереження ноутбуків у безпечних місцях.

4. Дозволяйте користувачам ноутбуків мати лише доступ до персональних даних, а не зберігати їх на ноутбуках. Дані мають зберігатися на головних комп’ютерах, ноутбуки повинні використовуватися тільки як пристрої, що відображають дані з головного комп’ютера, але не зберігають їх. Інформація може бути також захищена шляхом використання смарт-карт, засобів зчитування відбитків пальців та ін., а також паролів для доступу до головного комп’ютера.

5. Якщо ноутбук містить дані, шифруйте та кодуйте їх так, щоб користувачі не могли завантажити програмне забезпечення або змінити налаштування щодо захисту без погодження спеціалістів відділу програмного забезпечення компанії. Розгляньте можливість використання автоматично функції знищення для того, щоб дані на комп’ютері, які викрадено, були знищені, як тільки грабіжник намагатиметься використовувати їх в Інтернеті.

6. Навчайте працівників дотримуватися безпеки даних під час подорожі. Вони ніколи не повинні залишати ноутбуки в машинах на видноті, в місцях для багажу в готелях або здавати в багаж, якщо тільки це не вимагається безпекою аеропорту. Кожен, хто проходить через безпеку аеропорту, повинен слідкувати за своїм ноутбуком.

3.2.4. Захисна система

1. Використовуйте захисні системи для того, щоб захистити ваш комп’ютер від нападів хакерів, якщо він підключений до Інтернету. Захисні системи є програмним забезпеченням або обладнанням, яке розроблено для того щоб блокувати входження хакерів на ваш комп’ютер. Належним чином налаштована захисна система зробить важчим можливість хакерів знайти ваш комп’ютер та ввійти у ваші програми та файли.

2. Визначте, чи необхідно вам встановлення “обмеженої” захисної системи під час підключення до Інтернету. “Обмежена” захисна система відділяє вашу локальну мережу від Інтернету і може запобігти нападам шляхом спроб увійти в комп’ютер, де ви зберігаєте персональні дані. Встановіть “контроль за входом” – налаштування, що визначають, хто

пройшов через захисні системи і що вони бажають побачити – для того щоб дати можливість заходити до мережі тільки тим працівникам, до яких є довіра і їм необхідний такий доступ для законних потреб вашого бізнесу.

3. Якщо деякі комп’ютери вашої мережі зберігають персональні дані, а інші не зберігають, розгляньте можливість використання додаткових для них захисних систем або засобів.

3.2.5. Бездротовий та дистанційних доступ

1. Визначте, чи використовуєте ви бездротові пристрої, такі як сканери або стільникові телефони, що підключені до вашої комп’ютерної мережі або якими передаються персональні дані.

2. Якщо ви використовуєте бездротові пристрої, розгляньте можливість їх обмеженого підключення до вашої комп’ютерної мережі. Шляхом обмеження бездротових пристроїв, що можуть підключатися до вашої мережі, ви зробите доступ незнайомців до мережі важчим.

3. Для того щоб ускладнити для сторонніх осіб можливість читати документи, що містять конфіденційну інформацію, розгляньте можливість їх шифрування за допомогою електронних засобів.

4. Розгляньте також можливість використання шифрування, якщо вам необхідний дистанційний вхід до вашої комп’ютерної мережі, працівниками або постачальниками послуг, такими як компанії, що виявляють неполадки та оновлюють програмне забезпечення, що ви використовуєте для того, щоб обробляти покупки по кредитних картках.

3.2.6. Виявлення порушень

1. Якщо трапляються порушення в роботі мережі, розгляньте можливість використання систем, що визначають такі порушення. Для їх ефективності вони потребують частого оновлення для того, щоб бути націленими на нові типи хакерства.

2. Підтримуйте центральні реєстраційні файли даних конфіденційної інформації з метою перевірки діяльності в мережі для відслідковування та реагування на напади. Якщо на мережу здійснено напад, в такому файлі будуть міститися дані про комп’ютери, яким загрожують ризики.

3. Перевіряйте вхідний трафік, на який хтось з хакерів намагається скоїти напад. Слідкуйте за діяльністю нових користувачів, кількістю спроб невідомих користувачів або комп’ютерів увійти в систему, а також більш високим та більшим, ніж середній трафіком у незвичний для цього час доби.

4. Перевіряйте вихідний трафік з ціллю відслідковування порушень захисту персональних даних. Звертайте увагу на занадто великі розміри даних, що передаються з вашої системи до невідомих користувачів. Якщо велика кількість даних передається з вашої мережі, впевніться, що така передача здійснена на законних підставах.

5. У відповідь на порушення захисту даних вам необхідно мати і впроваджувати план дій.

3.3. Навчання персоналу

Ваш план захисту персональних даних може виглядати дуже гарним на папері, але він буде настільки сильним, наскільки сильний персонал, що впроваджує його. Виділіть час для того щоб пояснити правила вашому персоналу і навчити їх виявляти слабкі місця в безпеці даних. Періодичні тренінги підкреслюють важливість практичного застосування захисту даних. Добре навчена робоча сила являється найкращим захистом проти порушень захисту даних.

1. Перевіряйте біографію перед тим, як наймати працівників, які матимуть доступ до конфіденційної інформації.

2. Вимагайте від кожного з ваших нових працівників підписання договору щодо дотримання стандартів захисту персональних даних та забезпечення їх безпеки. Впевніться, що вони розуміють, що дотримання плану захисту та безпеки даних вашої компанії є суттєвою частиною їх обов’язків. Регулярно нагадуйте працівникам про політику вашої компанії та будь-які законодавчі вимоги зберігання відомостей про клієнтів у захищеному місці.

3. Майте інформацію щодо того, хто з працівників має доступ до персональних даних клієнтів. Звертайте особливу увагу на такі дані, як номери соціального захисту та номери рахунків. Обмежуйте доступ до персональних даних працівників.

4. Ваша компанія повинна мати процедури, які забезпечуватимуть, щоб працівники, які звільняються або переходять до іншого підрозділу, не мали доступу до конфіденційної

інформації. Обмежуйте термін дії їх паролів, зберігайте в безпечному місці ключі та ідентифікаційні відомості, як частину звичайного режиму перевірки.

5. Розповідайте працівникам про політику компанії стосовно дотримання захисту та безпеки даних. Впевніться, що ваша політика донесена до працівників, що мають доступ до персональних даних з дому чи іншого місця.

6. Попереджайте працівників про телефонний фішинг[6]. Навчайте їх бути обережними з незнайомими людьми, що телефонують, вимагають номер рахунку для оброблення замовлення або які запитують контактні дані клієнтів чи ваших працівників. Зробіть стандартною практикою подвійну перевірку шляхом контакту з компанією, що використовує номер телефону, який ви знаєте.

7. Вимагайте, щоб працівники повідомляли вас негайно, якщо є небезпека порушення захисту даних, наприклад, втрата чи крадіжка ноутбуку.

8. Впровадьте дисциплінарне покарання за порушення заходів безпеки.

3.4. Практика щодо безпеки підрядників та постачальників послуг

Практика компанії щодо безпеки даних залежить від людей, які впроваджують її, включаючи підрядників та постачальників послуг.

1. Перед тим як ви передасте будь-які функції вашого бізнесу (веб-хостинг, клієнтські кол-центри обробки даних), вивчіть практику їх захисту і порівняйте з вашими стандартами.

2. Під час укладання контрактів з вашими постачальниками послуг звертайте увагу на положення щодо безпеки даних в таких контрактах.

3. Вимагайте, щоб постачальники послуг повідомляли вам про кожний випадок порушення безпеки, що стався, навіть якщо такий випадок не завдав фактичної шкоди.

Стаття 4. Видалення даних

Те, що для вас купа сміття, може бути золотою знахідкою для грабіжника даних. Залишення рахунків по кредитних картках або паперів чи дисків з персональними даними в ящику для сміття посилює можливість вчинення злочину і піддає клієнтів ризику викрадення їх персональних даних. Шляхом правильного використання конфіденційної інформації ви забезпечуєте, щоб її не було прочитано чи відновлено.

1. Впроваджуйте практику, яка необхідна для запобігання несанкціонованому доступу до персональних даних, їх обробці, використанню та несанкціонованому поширенню.

2. Знищуйте паперові записи, використовуючи спеціальне обладнання та спалюючи їх. Зробіть так, щоб обладнання для подрібнення паперу не було доступне на робочих місцях.

3. При ліквідації старих комп’ютерів та засобів зберігання даних використовуйте програми для стирання даних. Вони недорогі та більш результативні при перезапису жорсткого диску, здійснюючи це таким чином, щоб файли неможливо було більше відновити. Видалення файлів, використовуючи клавіатуру або команди миші, як правило неефективне тому, що файли можуть продовжувати існування на жорсткому диску і можуть були відновлені.

4. За можливістю, впевніться, що працівники, які працюють вдома, дотримуються тих же процедур з ліквідації відомостей і даних щодо конфіденційної інформації, що зберігаються на їх комп’ютерах та засобах зберігання даних.

5. Якщо використовуєте кредитну історію клієнтів для цілей вашої діяльності, на вас поширюються правила ліквідації даних Федеральної торгової комісії.

Стаття 5. Попереднє планування

Здійснення заходів з захисту даних, що знаходяться у вашому розпорядженні, з метою запобігання порушенням системи безпеки може зайняти довгий період часу. Тим не менш, порушення можуть траплятися. Нижченаведеними способами ви можете зменшити такий вплив на вашу діяльність, ваших працівників та ваших клієнтів:

[6] Різновид Інтернет-шахрайства, вивідування інформації, що дає змогу здійснити викрадення персональних даних.

1. З метою реагування на випадки порушення захисту та безпеки майте відповідний план реагування. Призначте одного з ваших працівників головним по координації і впровадженню відповідного плану.

2. Якщо до вашого комп’ютера було здійснено несанкціонований доступ, відключіть його негайно від локальної мережі або Інтернету.

3. Одразу ж розслідуйте випадки порушення захисту чи безпеки та вживайте необхідних заходів блокування слабких місць в системі захисту даних або загроз безпеці персональних даних.

4. Визначтесь, кого потрібно повідомити, як всередині вашої організації, так і зовнішні інстанції, якщо трапився випадок порушення безпеки даних. Можливо, вам необхідно буде повідомити покупців, правоохоронні органи, клієнтів, кредитні бюро та інші компанії, на яких може вплинути таке порушення. Окрім того, багато регулюючих органів держав та федеральних банків мають закони або посібники щодо порушення захисту даних.

Використана література

1. Про захист осіб у зв’язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.1981 р. № 108 : у кн. “Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних” : посіб. / [В. Брижко, М. Швець та ін.]. – Кн. 2. – К. : ТОВ “ПанТот”, 2006. – 509 с.

2. Захист персональних даних в сфері Інтернет речей / О. Баранов, В. Брижко // Інформація і право. – № 2(17)/2016. – С.85-91.

3. Приватність даних у хмарних технологіях / В. Брижко // Інформація і право. – № 4(19)/2016. – С. 47-59.

4. Конвергенція новітніх технологій : стан і перспективи змін у інформаційних відносинах / В. Брижко, В. Фурашев // Інформація і право. – № 1(20)/2017. – С. 58-67.

5. Защита персональных данных в Интернете в странах Европейского Союза. – Режим доступу : https://ru.wikipedia.org

6. 4 преграды на пути Интернета вещей. – Режим доступа : http://ubr.ua/ukraine-and-world/technology/4-pregrady-na-puti-interneta-veshei-362374

7. S. Chen et al. A Vision of IP : Applications, Challenges and Opportunities With China Perspective IEEE / Internet of Things Journal, vol. 1, No. 4. – Pp. 349-359. – August 2014. – Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6851114

8. Сучасні основи захисту персональних даних в європейських правових актах / В. Брижко // Інформація і право. – № 3(18)/2016. – С. 45-57.

9. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / [В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник] ; за ред. В.М. Брижка, В.Г. Пилипчука. – К. : ТОВ “Видавничий дім “АртЕк”, 2017. – 226 с.

10. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Reglament (EU) 2016/679 of the European Parlament and of the Council, of 27 April 2016 / Регламент (ЄС) 2016/679 від 27.04.16 р. – Available at: http://eur-lex.europa.eu/legal-content /EN/ TXT/HTML/?uri=CELEX:32016 R0679&from= EN

11. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних : зб. документів ; [неоф. пер. з англ. І. Майстренко] ; за ред. В. Брижко ; передмова В. Пилипчука. – (НДІ інформатики і права Національної академії правових наук України). – К. : ТОВ “Видавничий дім “АртЕк”, 2018. – 180 с.

12. Корпоративні механізми (Кодекси поведінки) у сфері захисту персональних даних : в кн. “Інформаційне право та правова інформатика у сфері захисту персональних даних” / [В. Брижко, М. Швець та ін.] ; за ред. М. Швеця. – К. : ТОВ “ПанТот”, 2005. – 451 с. – С. 27-30.

13. Charter of Fundamental Rights of the European Union, of 7 December 2000. – Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

14. Подходы к защите персональных данных в ЕС и США. – Режим доступу : https://euroua.com/humrights/violations/1723-podkhody-k-zashchite-personalnykh-dannykh-v-es-i-ssha

15. – Режим доступу : http://itc.ua/news/senat-ssha-podderzhal-zakonoproekt-kotoryiy-pozvolit-internet-provayderam-ispolzovat-personalnyie-dannyie-polzovateley-bez-ih-soglasiya

16. До питання е-торгівлі та захисту персональних даних / В. Брижко // Правова інформатика. – № 1(13)/2007. – С. 14-28; Економічні та правові аспекти проблеми захисту персональних даних / В. Брижко // Правова інформатика”. – № 1(29)/2011. – С. 25-35.

17. Послугу з e-mail розсилки існуючої бази клієнтів. – Режим доступу : https://kiev.all.biz/baza-mobilnyh-nomerov-kieva-ukraina-bazy-klientov-g5081769

18. Економічний аспект захисту персональних даних у контексті права власності на інформацію / В. Брижко // Правова інформатика. – № 1(9)/2006. – С. 47-57.

19. Три скользких момента в законе ЕС о защите персональных данных. – Режим доступу : http://www.aif.uasociety/social/tri_skolzkih_momenta_v_zakone_es_o_zashchite_personalnyh_dannyh

20. Защита персональных данных / [А. Баранов, В. Брыжко, Ю. Базанов]. – К. : Национальное агентство по вопросам інформатизації при Президенте Украины, ВАТ КП ОТІ, 1998. – 128 с. – С. 41-42, 84.

21. Права человека и защита персональных данных / [А. Баранов. В. Брыжко, Ю. Базанов]. – Харьков : Фолио, 2000. – 280 с. – С. 169-176, 220-221, 233. – (Финансовая помощь и содействие в издании Харковской правозащитной группы и Национального фонда поддержки демократии (США).

22. е-майбутнє та інформаційне право / [В. Брижко, Ю. Базанов, М. Швець та ін.] ; за ред. доктора економічних наук, професора, члена-кореспондента Академії правових наук України М. Швеця. – [2-е вид., доп.]. – К. : НДЦПІ АПрН України. – 2006. – 233 с. – С. 131.

23. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія / В. Брыжко. – К. : ТОВ “ПанТот”, 2012 р. – 304 с. – (Про захист персональних даних. – С. 117-130).

24. Інформаційна безпека та приватність у сфері захисту персональних даних / В.Г. Пилипчук, В.М. Брижко // Інформація і право. – № 4(19)/2016. – С. 60-70;

Pylypchuk Volodymyr, Bryzhko Valery, 2016. PRIVACY AND HUMAN SECURITY IN THE PROTECTION OF PERSONAL DATA. Social and Human Sciences. Polish-Ukrainian scientific journal, 04(12). – Available at: http://sp-sciences.io.ua/s2596466/pylypchuk _volodymyr_ bryzhko_valery_2016._privacy_and_human_security_in_the_protection_of_personal_data._social_and_human_sciences._polish-ukrainian_scientific_journal_04_12_ (accessed 08 January 2017)

25. – Режим доступу : http://www.eurasialegal.info/index.php?option=com_content&view=article&id=5192:2017-02-20-06-48-58&catid=314:2015-02-05-10-21-50

26. Забезпечення захисту персональних даних у комерційних організаціях : за матеріалами посібника для бізнесу Федеральної торгової комісії США / [пер. з англ. Віри Брижко] ; за ред. В.М. Брижко. – Режим доступу : //www.ftc.gov/bcp/edu/pubs/business/ idtheft/bus69.pdf

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~