УДК 342.951

КРАСНІКОВ С.А., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-6548-5457.

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ТА ОСОБЛИВОСТІ ЛОКАЛІЗАЦІЇ ПЕРСОНАЛЬНИХ ДАНИХ: КРАЩІ ПРАКТИКИ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *Розглянуто загальносвітові тенденції та особливості локалізації персональних даних у деяких зарубіжних країнах (ЄС, США, Індонезія, Малайзія, Індія, Узбекистан, Казахстан, РФ). Узагальнено деякі аспекти здійснення зберігання, обробки та передачі персональних даних у межах юрисдикції держав. Деталізовано законодавче забезпечення штрафних санкій за порушення нормативних вимог локалізації персональних даних, їх конфіденційності та приватності. Визначено позитивні аспекти та здобутки використання світового сервісу "InCountry". Регламентовано особливості здійснення передачі персональних даних на умовах аутсорсингу. Окреслено шляхи удосконалення вітчизняного законодавства у сфері локалізації персональних даних.*

Ключові слова: *персональні дані, приватність, конфіденційність, локалізація, захист, IT-технології, провайдери, оператори, аутсорсингові послуги.*

Summary. *The global trends in the localization of personal data are considered. Peculiarities of localization of personal data in some foreign countries (EU, USA, Indonesia, Malaysia, India, Uzbekistan, Kazakhstan and Russian Federation) are investigated. Some aspects of the storage, processing and transfer of personal data within the jurisdiction of states are summarized. The legislative support of penalty sledges for violation of regulatory requirements for localization of personal data, their confidentiality and privacy is detailed. The positive aspects and achievements of using the world "InCountry" service are identified. The peculiarities of outsourcing of personal data transfer are regulated. The directions of improvement of the domestic legislation in the field of personal data localization are outlined.*

Keywords: *personal data, privacy, confidentiality, localization, protection, IT technologies, providers, operators, outsourcing services.*

Аннотация. *Рассмотрены общемировые тенденции и особенности локализации персональных данных в некоторых зарубежных странах (ЕС, США, Индонезия, Малайзия, Индия, Узбекистан, Казахстан, РФ). Проведено обзор некоторых аспектов осуществления хранения, обработки и передачи персональных данных в пределах юрисдикции государств. Детализировано законодательное обеспечение штрафных санкций за нарушения нормативных требований локализации персональных данных, их конфиденциальности и приватности. Определены положительные аспекты и достижения использования мирового сервиса "InCountry". Регламентированы особенности осуществления передачи персональных данных на условиях аутсорсинга. Определены пути усовершенствования отечественного законодательства в сфере локализации персональных данных.*

Ключевые слова: *персональные данные, приватность, конфиденциальность, локализация, защита, IT-технологии, провайдеры, операторы, аутсорсинговые услуги.*

Постановка проблеми. Одним з найбільш проблемних правових питань в еру інформаційних технологій є захист персональних даних. До того ж у світі, поглибленому глобалізацією, дані користувача однієї країни можуть використовувати треті особи з будь-якого куточка світу, у тому числі й незаконно.

Останнім часом світова спільнота активно переймається питаннями локалізації персональних даних у межах національних кордонів з метою забезпечення їхнього збереження у форматі захисту цифрових прав громадян, особливо щодо приватних та конфіденційних відомостей користувачів пристроїв. На цьому фоні невиконання вимог щодо локалізації інформаційних баз з персональними даними створює певну загрозу для захисту та безпеки громадян, безперебійного функціонування критичної інформаційної інфраструктури, мінімізує ефективність заходів боротьби з тероризмом, нівелює здобутки щодо забезпечення національної безпеки держави. У зв'язку з цим для будь-якої країни сучасного світу необхідним є прискорення в удосконаленні відповідних нормативно-правових актів, які мають регламентувати порядок та умови впровадження такої локалізації, з одночасним запровадженням санкцій та відповідальності за правопорушення прав людини. Динамічне розширення сфери застосування сучасних технологій та комунікацій створює додаткові умови для зростання рівня кіберзлочинності.

Глобальні та кардинальні зміни у сфері ІТ-технологій, що відбуваються останнім часом, вимагають адекватного коригування та адаптації вітчизняного законодавства з метою встановлення превентивних заходів щодо профілактики та попередження протиправних дій у зв'язку з поширенням несанкціонованих обробки та використання персональних даних. За таких умов, розгляд зарубіжних законодавчих ініціатив, які впроваджуються щодо посилення процесів локалізації персональних даних та підвищення рівня відповідальності операторів ІТ-ринку за такі порушення, є своєчасним та логічним.

Результати аналізу наукових публікацій. Питання організаційно-правових засад інституціоналізації та локалізації персональних даних, сучасні методи їх обробки та збереження досліджували у своїх наукових працях такі вчені, як: В. Брижко, В. Пилипчук [1], П. Гуйван [2], К. Мельник [3], Т. Обуховська [4], А. Тарасюк [5] та інші. Проте висвітлення кращих практик зарубіжного досвіду у сфері законодавчого забезпечення щодо локалізації персональних даних потребує подальших досліджень, зокрема щодо висвітлення особливостей роботи всесвітнього сервісу "InCountry".

Метою статті є визначення сучасних законодавчих ініціатив у провідних країнах світу з метою впровадження концептуальних засад локалізації персональних даних для їх забезпечення дотримання принципів приватності та конфіденційності у сучасних європейських правових стандартах.

Виклад основного матеріалу. Персональні дані – не тільки ім'я чи контактні дані певної фізичної особи, це також й IP-адреса, MAC-адреса, геолокація, які можуть використовувати персональні дані для відстеження контактів. Ще декілька років тому компанії, незалежно від юрисдикції держав, зберігали дані своїх користувачів де завгодно: деякі у межах країни, а інші – поза межами, в інших державах, або на серверах та площадках міжнародних ІТ-гігантів, на кшталт "Google", "Facebook" тощо.

Адже траплялося чимало випадків несанкціонованого або спеціального витоку персональних даних або їх використання у злочинних цілях, що привезло до необхідності посилення заходів збереження та обробки персональних даних. Таким чином, загальноприйнятим трендом в сучасному світі є активізація процесу локалізації персональних даних з дотриманням вимог політики конфіденційності та приватності. Метою політики конфіденційності й приватності є забезпечення захисту прав і свобод людини і громадянина при обробці його персональних даних, в тому числі захисту прав на недоторканність приватного життя від несанкціонованого доступу і розголошення. По мірі того, як активно прогресує та просувається інформаційна епоха, важливість географічного місцязнаходження для конфіденційності даних стає дедалі важливішою. На цьому фоні актуальним питанням стає така ознака як резидентність даних, тобто їхня

локалізація у межах певної держави. Так, останнім часом, у багатьох країнах світу таких, як ЄС, Канада, Австралія, США, Аргентина та інших, компанії, які мають доступ до обробки та зберігання персональних даних громадян, зобов'язані зберігати їх виключно на території своїх країн, тобто в межах їх національних юрисдикцій. Тому кожна держава світу розробляє та впроваджує власні системні заходи з метою збереження персональних даних громадян у межах національних сегментів кіберпростору. Також кожна країна розробляє норми регулювання персональних даних з метою встановлення правил їх зберігання та використання.

В травні 2018 року для міжнародного ІТ-ринку усіх держав-членів ЄС було запроваджено оновлені правила обробки персональних даних на підставі Загального Регламенту ЄС 2016/679 "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)" від 27 квітня 2016 року (General Data Protection Regulation – GDPR) [6].

Загальний Регламент захисту даних встановив більш суворі вимоги до принципів обробки та використання персональних даних. Вони полягають в тому, що персональні дані мають збиратися законно, правомірно, прозоро та відповідно до цільового призначення. В умовах поширення глобалізації та прискореного інформаційно-технологічного прогресу стало конче необхідним посилити захист основоположних прав людини в сфері захисту персональних даних за умов впровадження заходів, які мають гарантувати недоторканність приватного життя та забезпечити цифрові права пересічених громадян. Тобто виконання приписів GDPR передбачає для усіх держав-членів ЄС схвалення нових національних програм захисту персональних даних з чіткою системою контролю, яка має орієнтуватися на виконання принципів та правил забезпечення приватності та конфіденційності [7].

Що стосується питання захисту персональних даних в інших країнах, традиційно, найбільш розвиненою юрисдикцією вважається США. Однією із причин необхідності розвитку такого законодавства є значна кількість порушень у сфері персональних даних. У зв'язку з цим у 2020 році у штаті Каліфорнія був прийнятий новий Закон про захист персональних даних. Насамперед, його важливість полягає в тому, що в Каліфорнії знаходяться такі компанії, як "Facebook", "Google", "Apple", що працюють з персональними даними користувачів по всьому світу. Завданням цього законодавчого акту стала необхідність посилення захисту персональних даних, які обробляють юридичні особи приватного права та є розпорядниками такої інформації. Саме тому цим Законом користувачам надається право дізнатися відомості про те, як компанія розпоряджається їхніми даними, а також можливість вимагати видалення інформації про себе та зупинення її розповсюдження. За невиконання нормативних вимог закону передбачені значні штрафи, навіть, якщо компанія порушує законодавство через необережність. Таким чином, завдяки впровадженню цього Закону Каліфорнія підвищила дисциплінованість та відповідальність юридичних осіб під час збирання та обробки персональних даних фізичних осіб [8].

Так, у 2012 році в Індонезії уряд схвалив нормативний акт, спрямований на дотримання вимог державними організаціями, установами та закладами, які надають відповідні електронні послуги, зокрема створення центрів обробки даних на території цієї країни. Встановлено, що експлуатація державної електронної операційної системи передбачає створення Центру аварійного реагування. Окрім того, Міністерство зв'язку цієї країни запровадило загальну вимогу щодо функціонування Центрів обробки даних для більш широкого кола державних інституцій, які використовують інформаційні

технології з метою надання відповідних послуг громадянам. Також електронний системний оператор має забезпечити зберігання даних про усі трансакції в Індонезії. Вимога щодо зберігання персональних даних між постачальниками електронних систем та їх клієнтами в Індонезії застосовується як приватними, так і публічними постачальниками електронних систем.

У Малайзії Законом про захист персональних даних ще з 2010 року запроваджено заборону на передачу персональних даних за межі країни. Транскордонна передача персональних даних можлива лише за умови виконання певних передумов і тільки у виключних випадках. За фабулою Закону повинна бути отримана згода суб'єктів персональних даних, якщо існує необхідність виконання договору між суб'єктом та оператором, який було укладено за запитом або в інтересах суб'єкта персональних даних.

В Індії, згідно із засадами державної інформаційної політики, обробка усіх даних, які зібрані з використанням державних ресурсів, має віжбуватися виключно на території Індії. Також встановлена вимога щодо провайдерів послуг електронної пошти стосовно розміщення своїх серверів тільки у цій країні. В сучасних умовах у рамках закону Індії про телекомунікації, уся інформація про клієнтів та користувачів, окрім інформації про наданий роумінг, повинна зберігатися тільки у межах цієї країни, а віддалений доступ до такої інформації заборонений з-за кордону.

В Узбекистані у 2019 році набули чинності зміни до законодавства про персональні дані, що зобов'язують зберігати такі дані виключно на території цієї країни. Законодавчо встановлено, що персональні дані громадян повинні оброблюватися на технічних засобах та пристроях, які фізично розташовані на території Узбекистану та зареєстровані у відповідному Державному реєстрі. Вимоги щодо локалізації даних поширюються на обробку даних з використанням інформаційних технологій, у тому числі й за допомогою мережі Інтернет. Нормативний обов'язок щодо зберігання даних покладається на володільця або оператора бази даних, при цьому володільцем є власник бази даних, а оператором – особа, яка обробляє персональні дані. Вимога щодо локалізації передбачає збір, систематизацію та зберігання персональних даних.

Згідно із Законом Узбекистану "Про персональні дані", який набув чинності 1 жовтня 2019 року, персональні дані – це зафіксована на електронному, паперовому або іншому матеріальному носії інформація, яка відноситься до певної фізичної або юридичної особи, яка надає змогу провести її ідентифікацію. Запроваджено систему санкцій за порушення законодавства про локалізацію персональних даних, включаючи настання кримінальної відповідальності – позбавлення волі на строк до 3 років. Законом покладено обов'язок щодо локалізації серверів з персональними даними виключно на території Узбекистану.

У Казахстані Закон "Про персональні дані" був прийнятий у 2013 році, а у 2015 році до нього були внесені зміни у зв'язку із запровадженням загальної вимоги про зберігання (локалізацію) персональних даних у цій країні. Вимога щодо зберігання персональних даних у Казахстані набула чинності з 1 січня 2016 року. Хоча у Законі відсутні вимоги щодо передачі персональних даних до інших держав світу, у випадку передачі даних за кордон, обов'язковим є копіювання та зберігання такої інформації на серверах на території Казахстану. У Казахстані Законом "Про персональні дані" передбачається як адміністративна, так і кримінальна відповідальність за порушення вимог щодо їхнього захисту. Під санкції підпадають дії, спрямовані на незаконний збір, обробку персональних даних, недотримання власником, оператором або третьою особою заходів щодо захисту таких даних, несвоєчасне забезпечення власником або

володільцем інформаційних систем, які містять персональні дані заходів щодо їх фізичного захисту тощо. Кримінальна відповідальність настає у випадку спричинення значної шкоди правам та законним інтересам особам в результаті незаконного збору або обробки персональних даних. Законодавчо встановлено, що зберігання є активною поведінкою суб'єкта щодо повноцінного забезпечення одночасно приватності й конфіденційності персональних даних.

Загальновідомо, що до персональних даних відносяться: стан здоров'я, розмір заробітної плати, інша інформація, яка не підлягає розголошенню у форматі тексту, фотографій або відео. Інформація про релігійну належність, світогляд, політичні переконання, стиль приватного життя, дані про судимість та стан здоров'я є спеціальними персональними даними та їхня обробка забороняється, крім випадків власного навмисного поширення у загальнодоступних джерелах. Більшість сервісів як мінімум оброблюють персональні дані – мобільні оператори, Інтернет-магазини, соціальні мережі, пошукові системи тощо. Наприклад, кожен раз, коли людина здійснює у сервісах "Google" будь-які дії, ця компанія автоматично збирає та зберігає дані про неї. Аналіз нормативних актів різних країн світу засвідчує, що оптимальним рішенням локалізації даних є перенесення персональних даних, їхня обробка, збір та зберігання з використанням можливостей саме дата-центрів або буферного серверу у межах певної країни.

В сучасних умовах отримав світове схвалення та визнання сервіс "InCountry" [9]. Він став першим постачальником послуг з локалізацією масивів даних, який надає змогу впроваджувати свою послугу навколо світу, управляти даними у понад 90 країнах. Завдяки цьому сервісу надійно зберігаються персональні відомості у межах національних кордонів. Геопросторові дані між браузерами користувачів та веб-додатками глобально проксируються через смуги присутності у чітко визначених країнах.

Сервіс "InCountry" пропонує швидкі та ефективні рішення з метою інтеграції персональних даних. Його впровадження сприяє локалізації даних та є оптимальним рішенням для компаній, які прагнуть здійснювати масштабування та повинні дотримуватися законодавчих вимог щодо зберігання персональних даних. Повноцінна робота з постачальниками послуг у форматі "InCountry" є запорукою гарантування, що інформація буде збиратися, оброблюватися та зберігатися у відповідності до національних вимог й стандартів тієї чи іншої країни. За допомогою сервісу "InCountry" до персональних даних, які можуть збиратися та оброблятися відносяться: дані про співробітників, фінансові й податкові дані, дані про стан здоров'я, платіжні дані.

Підтримка локалізації даних дає два потужних сигнали: по-перше, бізнес підтримує локалізацію даних та поважає конфіденційність; по-друге, цей сервіс відповідає встановленим регіональним вимогам захисту даних та конфіденційності.

Загалом локалізація даних має різноманітні форми, у той час як деякі країни запроваджують повну заборону на таку передачу даних, багато з них відносяться до конкретних секторів, включаючи особисті та фінансові дані, податкові та медичні відомості тощо. Сервіс "InCountry" підтримується глобальними компаніями, які стикаються з обмеженнями встановленими регіональними законами про забезпечення конфіденційності, тому партнерство з "InCountry" – найшвидший спосіб дотримуватися нормативних правил розміщення даних.

Практика застосування чинного законодавства переконливо свідчить про недостатню ефективність існуючих заходів реагування на правопорушення у сфері інформаційних технологій та поширення інформації в інформаційно-комунікаційних мережах. У зв'язку з цим політичне керівництво провідних держав світу посилює заходи

відповідальності за порушення у сфері обробки даних та поширення інформації з урахуванням кращих практик міжнародного та зарубіжного досвіду у цій площині.

Так, у Німеччині за порушення провайдерами телекомунікаційних послуг запитів про передачу інформації, що запитується, у тому числі й у випадку порушення механізмів шифрування, уповноважений компетентний орган може накласти штраф у розмірі до 500 тис. Євро, частково або повністю зупинити діяльність провайдера.

У Великобританії штраф за порушення вимог уповноважених органів складає до 50 тис. фунтів, а також передбачена кримінальна відповідальність до двох років тюремного ув'язнення.

У Туреччині законодавчо встановлений штраф за невиконання норм про умови зберігання інформації та організації доступу до неї у розмірі до 100 тис. турецьких лір, відмова обмежити доступ до інформації – до 300 тис. турецьких лір.

У 2019 році в Росії був схвалений Федеральний Закон про введення штрафів за порушення вимог локалізації обробки персональних даних громадян. Законом передбачено, що за перше порушення вимог про локалізацію компанія, яка обробляє дані громадян РФ, може бути піддана штрафу на 2-6 млн. російських рублів, а за повторне – 6-18 млн. російських рублів. Альтернативою штрафів є можливість внесення доменних імен та мережевих адресатів у реєстр порушників прав суб'єктів персональних даних. Відповідно до нормативних вимог про локалізацію, під час збору персональних даних, у тому числі й з використанням мережі Інтернет, оператор зобов'язаний забезпечити запис, систематизацію, накопичення, зберігання та уточнення (оновлення, зміна) персональних даних. Вимоги про виконання правил локалізації не є перепоною для передачі персональних даних в зарубіжні країни. Персональні дані першочергово вносяться до бази даних на території РФ та актуалізуються, а згодом можуть надалі передаватися до баз даних, які розташовані за межами РФ. Головне завдання, щоб під час такої передачі виконувалися загальні вимоги щодо транскордонної передачі персональних даних (наприклад, для передачі даних до США необхідно отримати письмову згоду відповідного суб'єкта). Вимога про локалізацію даних застосовується до іноземних компаній без фізичної присутності у РФ, якщо вони проводять діяльність у цій країні. Так, наприклад, Інтернет-сайт вважається таким, що проводить діяльність у РФ у таких випадках: сайт використовує доменне ім'я, пов'язане з РФ, сайт має російськомовну версію, сайт надає можливість сплачувати за товар у російських рублях; на сайті можливо укласти договори з виконавцем у РФ, на сайті ведеться реклама російською мовою, інші обставини, які переконливо демонструють інтерес власника сайтів до аудиторії. Технічно закон про локалізацію даних застосовується до усіх російських компаній, філій та представництв іноземних компаній та корпорацій, має відношення до інших юридичних осіб, поширюється на операторів, зареєстрованих за межами РФ, які не мають офіційної присутностіі, проте здійснюють господарську діяльність на місцевих ІТ-ринках.

Також слід вказати, що чимало іноземних ІТ-холдингів стикаються з проблемою локалізації персональних даних, коли постає питання щодо їхнього використання головною організацією, тобто материнською компанією, яка перебуває за кордоном тієї чи іншої країни, тобто поза межами її юрисдикції. У такому випадку важливо розуміти спектр заходів, які можуть здійснюватися щодо захисту персональних даних за кордоном в умовах забезпечення нормативного процесу суцільної локалізації.

На цьому фоні актуальною проблемою залишаються передачі персональних даних за допомогою аутсорсингової компанії. Останнім часом, послуги аутсорсингу стають дедаля більш затребуваними. Однак, здійснюючи передачу провайдеру певних функцій, досить часто йому передають доступ до персональних даних, у зв'язку з чим постає

питання щодо виконання провайдером правил їх локалізації, оскільки він не є відповідальним за збереження та захист персональних даних. Так, якщо компанія-оператор персональних даних надає аутсорсинговій компанії тільки виключно доступ до своїх баз даних для виконання певних функцій за договором (наприклад, для здійснення рекламних розсилок), то у цьому випадку відповідальність щодо захисту персональних даних покладається на замовника. У випадку, коли компанія передає свою базу даних організації-аутсорсеру (наприклад, у випадку надання бухгалтерських послуг), то у договорі необхідно вказати про права провайдера щодо аутсорсингових послуг та визначити його обов'язки щодо застосування заходів захисту отриманих персональних даних та конфіденційності інформації. У такому випадку саме аутсорсингова компанія стає оператором персональних даних, який зобов'язаний дотримуватися нормативних вимог про їх локалізацію.

Висновки.

1. Тренди на світових ринках кібербезпеки формуються під впливом динамічного розвитку міжнародного та національного законодавства й масштабів поширення загроз. Локалізація персональних даних та окремих процесів обробки персональних даних – необхідна вимога сучасності. На цьому фоні кожна держава світу здійснює активну законотворчу роботу, яка нормативно спрямовується на розробку та впровадження додаткових вимог, у першу чергу, щодо посилення захисту та локалізації персональних даних в інформаційних та інформаційно-комунікаційних системах, впровадження нормативних вимог та правил у сфері локалізації персональних даних. Посилаючись на позитивний зарубіжний досвід, можно констатувати, що усі компанії – постачальники електронних послуг зобов'язані локалізувати свої сервери, у іншому випадку настають санкції – штрафи та блокування їх роботи, формування державою "чорних списків" провайдерів.

Узагальнючи викладене, можна визначити важливі кроки, які фіксуються у законодавствах передових країн світу, практична реалізація яких сприятиме активізації процесів локалізації персональних даних у межах національних кордонів, зокрема, це:

- проведення інвентаризації усіх інформаційних систем або баз даних;
- визначення місця знаходження інформаційних систем та баз даних, їхніх серверів за принципом екстериторіальності, оскільки обов'язкова вимога щодо локалізації персональних даних означає, що саме на території відповідної держави має відбуватися первинний збір таких даних, хоча обробка та зберігання ймовірно можуть здійснюватися й за кордоном;
- запровадження штрафів та санкцій з посиленням відповідальності порушників нормативних вимог.

2. Для України в сучасних реаліях масштабного переходу на дистанційний режим роботи в умовах пандемії коронавірусу та запровадження локдауну, тематика локалізації персональних даних є досить актуальною.

Вітчизняні суб'єкти господарювання й підприємці, які використовують відповідні сервіси, збирають персональні дані українців, навіть не повідомляючи останніх про те, що їхні дані досить часто передаються за кордон. Більш того, особи, які використовують такі сервіси у власній діяльності, зазвичай не мають будь-яких внутрішніх норм про обробку даних, обмеження щодо кола осіб, які мають доступ до таких даних. Такі особи іноді не дуже звертають увагу на проблеми захисту персональних даних. Переважно суб'єкти даних не обізнані про те, як використовують і поширюють їхні дані, або взагалі не мають відомостей, у які країни їх дані передаються й, звичайно, де перебувають відповідні сервери.

Отже, з точки зору вимог вітчизняного законодавства, досить часто відбуваються його порушення, що потребує посилення відповідальності за недотримання нормативів приватності та конфіденційності персональних даних.

На практиці мінімізація ризиків здійснюється наступним чином: локалізація відповідного сервісу; розроблення належної документації в сфері обробки персональних даних; постійний контент-аналіз процесу здійснення обробки персональних даних. З цією метою доцільно періодично проводити аудит порядку обробки персональних даних для усунення недоліків, якщо такі були виявлені.

За таких умов, потребує удосконалення Закон України "Про захист персональних даних" з урахуванням: загальносвітових тенденцій посилення спроможностей держав у напрямку суцільної локалізації персональних даних; встановлення більш жорстких правил щодо забезпечення приватності та конфіденційності, які відповідають нормативним стандартам захисту персональних даних у державах-членах ЄС; посилення штрафних санкцій за порушення законодавчих вимог приватності та конфіденційності.

Використана література

1. Защита персональных данных / В. Брыжко, Ю. Базанов та ін. Київ: Национальное агентство по вопросам информатизации при Президенте Украины, 1998 г. 128 с.; Права человека и защита персональных данных / В. Брыжко, Ю. Базанов та ін. – (Государственный комитет связи и информатизации Украины). Харьков: Фолио, 2000. 280 с.; Становлення і розвиток правових основ та системи захисту персональних даних в Україні / В.Г. Пилипчук, В.М. Брижко та ін.: монографія. – (НДІ інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

2. Гуйван П.Д. Особливості національного та міжнародного регулювання обробки окремих категорій персональних даних. *Журнал європейського і порівняльного права.* 2018. № 2. С. 42-56.

3. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних. *Інформаційна безпека людини, суспільства, держави*. 2013. № 2. С. 97-103. URL: http://nbuv.gov.ua/UJRN/iblsd_2013_2_18

4. Обуховська Т.М. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. *Вісник Національної академії державного управління при Президентові України*. 2014. № 1. С. 95-103. URL: http://nbuv.gov.ua/UJRN/Vnadu_2014_1_17

5. Тарасюк А.В. Вплив загального регулювання захисту даних на контролерів та процесорів персональних даних – резидентів України. *Інформація і право*. №1(24)/2018. С. 28-35.

6. The General Data Protection Regulation (GDPR). URL: https://ec.europa.eu/info/law/law-topic/data-protection_en; – (переклад) Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів / пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука. – (НДІ інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 180 с.

7. Брижко В.М., Пилипчук В.Г. Безпека персональних даних: правові стандарти Європейського Союзу та сучасні прикладні проблеми. *Інформація і право*. № 1(36)/2021. С. 17-28.

8. Фісун В. Проблеми захисту персональних даних: досвід України та інших країн. *Юридична газета*. 2020. № 10 (716). URL: https://yur-gazeta.com/publications/practice/informaciyne - pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html

9. Global Apps, Local Compliance. URL: https://incountry.com

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