

DOI: <https://doi.org/10.15407/bv2022.02.018>

УДК: 1:340.1:316.324.8

Олена Лопата,

<https://orcid.org/0000-0002-1386-3409>,

молодша наукова співробітниця,

Національна бібліотека України імені В. І. Вернадського (м. Київ, Україна)

просп. Голосіївський, 3, Київ, 03039, Україна,

e-mail: lopata@nbuv.gov.ua;

Забезпечення безпеки даних користувачів бібліотек у контексті нових правових стандартів Європейського Союзу

Мета дослідження – визначити та охарактеризувати ключові засади нового міжнародного та національного порядку безпеки даних й узагальнити їх правові приписи щодо створення цілісної системи захисту особистих даних у бібліотечній сфері. **Методологія** дослідження ґрунтується на системному та структурному підходах, методах порівняльного, логічного та джерелознавчого аналізу, із залученням міждисциплінарного підходу. **Наукова новизна**. Розглянуто низку актуальних кінцевих документів Європейського Парламенту та Ради Європейського Союзу щодо підготовки адаптивної нормативно-правової бази у сфері захисту персональних даних та її реалізації у державах-членах ЄС. Проаналізовано основні Закони, що регулюють відповідні відносини в Україні. Узагальнено нові правила захисту особистих даних громадян ЄС. Вирізнено й охарактеризовано сім основних «принципів» обробки персональних даних, а саме: законність, справедливість та прозорість; обмеження цілей; мінімізація даних; точність; обмеження зберігання; цілісність та конфіденційність; підзвітність. Сформульовано три основні принципи та ключові завдання організації системи інформаційної безпеки та захисту особистих даних. Поручено нагальні питання практичної діяльності книгозбірень у галузі захисту персональних даних. **Висновки**. Узагальнюючи нормативно-правові ініціативи Європейського Парламенту та Ради ЄС, законодавчі акти та постанови України, положення «Пакету захисту даних» та Конвенції РЄ № 108 – організацію системи безпеки даних, на сьогодні потрібно розглядати та вибудовувати, спираючись на сутнісні зв'язки, чинні інформаційні нормативно-правові акти та кожного конкретного суб'єкта. НБУВ бере ефективну участь у реалізації означених положень у практичній роботі книгозбірень.

Ключові слова: трансформація, персональні дані, безпека даних, захист даних, обробка інформації, система захисту персональних даних, правові стандарти.

Актуальність. Одним із визначальних досягнень демократичних перетворень у багатьох країнах світу стала гарантованість права на інформацію, її відкритість, доступність, свобода обміну, правомірність одержання, використання, поширення та зберігання тощо. Влада провідних європейських країн, здійснюючи державну політику в реляційній сфері, запроваджує правові механізми забезпечення доступу до інформації, що нині є основним нематеріальним продуктом та визначальним знанневим ресурсом будь-якого цивілізованого суспільства [1; 8; 9; 12; 17; 24]. Політика держав у сфері захисту інформації реалізується у багатьох напрямках. Особливе місце відводиться інформаційній безпе-

ці та захисту даних. За умов російської агресії, повномасштабної війни та воєнного стану в Україні ці питання, як неодноразово підкреслював у своїх щоденних зверненнях до українського народу Президент держави – В. О. Зеленський, є одними з найактуальніших та такими, що потребують невідкладного вирішення.

Історико-бібліотечознавчий аналіз свідчить, що Національні закони з питань регулювання автоматизованої обробки та захисту особистих відомостей, про які раніше вже йшла мова [8; 9], у країнах Західної Європи та США почали розроблятися із кінця 60-х років минулого сторіччя [1; 12; 17].

Необхідність врегулювання суспільних відносин у цій сфері насамперед була пов'язана з об'єктивною потребою усунення порушень та передумов недотримання права людини на її персональні дані; розвитком е-комерції (е-бізнесу, е-торгівлі та ін.) та гармонізації відносин із захисту особистих даних відповідно до приписів континентального права та європейських правових стандартів тощо [1, с. 37].

Наприкінці ХХ – на початку ХХІ ст. у більшості країн-членів Європейського Союзу (далі ЄС) було прийнято базові закони про захист персональних даних та створено передумови для узгодження національних законодавств у цій царині [3; 10; 23; 25; 28; 29; 30; 31]. Водночас, незважаючи на розбіжності правових систем, в основу законодавства про захист даних покладено ідентичні принципи, викладені у спільних правових стандартах. Захист персональних даних як у країнах ЄС, так і Великобританії та США – суспільних інституціях із різними громадянськими та політичними та відносинами – розглядається як невід'ємний складник демократичної правової держави. Більшість законів європейських країн у цій царині мають типову назву – закон про захист даних. В англо-американській традиції «право на приватність» (*privacy*) розглядається як моральний принцип поваги до особистої свободи. Аналіз цієї проблематики здійснювався такими видатним вченими, як А. Міллер, Р. Холлборг, І. Вельдером, Д. Лоу, М. Блан-Монмейєр, Ж. Дурі-Боне та іншими.

В Україні питання інформаційної безпеки та захисту даних (В. Мусіяка, О. А. Баранов, В. М. Брижко, Ю. К. Базанов, К. С. Мельник, В. А. Проценко, В. Пилипчук, Ю. С. Максименко, В. С. Ковальський) найбільш активно всебічно досліджувалися та широко обговорювалися у 1996–2013 рр. (напередодні прийняття відповідних регулятивних Законів та типових Правил) [7]. У зв'язку із запровадженням нових правових стандартів ЄС щодо захисту персональних даних та можливого прискореного надання Україні статусу членства в Європейському Союзі ця проблематика й надалі буде актуалізуватися.

Метою цієї статті є визначення та розгляд ключових засад нового міжнародного та національного порядку безпеки даних й узагальнення їх правових приписів щодо створення цілісної системи захисту персональних даних у бібліотечній сфері.

У зв'язку з численністю документів, що суттєво відрізняються між собою у опрацюванні, визначальними **методами** цього дослідження обрано джерелознавчий та порівняльний аналіз.

Виклад основного матеріалу. Найбільші за два десятиріччя зміни у сфері захисту персональних даних у законодавстві Європейського Союзу відбулися

25 травня 2018 р. – цього дня набрали чинності нові принципи та правила обробки персональних даних (далі ПД) громадян ЄС. Зазначені норми раніше були ухвалені Постановою Європейського Парламенту та Ради ЄС (2016) й отримали назву «**Пакет захисту даних**» (із трьох документів), який окреслив основні засади підготовки адаптивної нормативно-правової бази та її реалізації у державах-членах ЄС й був рекомендований до впровадження іншим країнам, що співпрацюють з ЄС. Європейський Парламент та Рада ЄС, як зазначалося у травні 2016 р., схвалили нові правила та порядок захисту персональних даних, передбачаючи умови створення сильної та більш координованої структури захисту персональних даних у Союзі. «Пакет захисту даних» долучає такі документи [20]:

- **Регламент (ЄС) 2016/679** Європейського Парламенту та Ради «Про захист осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальний Регламент щодо захисту даних)» від 27.04.2016 р.;

- **Директиву (ЄС) 2016/680** Європейського Парламенту та Ради «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади з метою запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, або виконання кримінальних покарань та про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ЖНА» від 27.04.2016 р. (далі Директива) [2];

- **Директиву (ЄС) 2016/681** Європейського Парламенту і Ради від 27.04.2016 р. «Про використання даних записів реєстрації пасажирів (PRN) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину».

Головним документом сучасних правових стандартів визнано **Регламент (ЄС) 2016/679 від 27.04.16 р.** (далі Регламент) – «Загальні положення про захист даних» (*General Data Protection Regulation*) [18]. Регламент ЄС має на меті не лише удосконалення захисту та безперешкодний обіг відомостей, що стосуються фізичних осіб в межах Союзу, а й гарантування еквівалентного рівня інформаційної безпеки всіх громадян ЄС. Основною його вимогою є узгодження законів про недоторканість даних на території ЄС та змін у засадах «усіх організацій у всьому регіоні» щодо вирішення проблеми забезпечення обов'язкової конфіденційності персональних даних. Доти організаціям та іншим суб'єктам, які працюють з персональними даними, необхідно було враховувати правила щодо захисту даних 28 різних держав-членів ЄС.

«Пакет захисту даних» (далі Документи) встановлює більш жорсткі організаційні, юридичні та чисто технічні вимоги до їх захисту, а також передбачає впровадження єдиної правової політики у цій сфері не тільки для держав-членів ЄС, але й для інших країн, які мають політичні, економічні та соціальні зв'язки з ЄС.

Екстериторіальні приписи правил ЄС – досить ґрунтовні та складні. Проте в них є й важлива перевага: будь-яким інституціям, серед них – і книгозбірням простіше дотримуватись єдиного комплексу правил та настанов, ніж враховувати національні особливості щодо захисту, поширення та опрацювання ПД кожної

окремої країни ЄС, як це було до запровадження Документів. Реформа спрямована й на стимулювання розробки та впровадження *паритетної моделі захисту персональних даних* шляхом скорочення витрат та управлінського апарату для установ, які працюють в ЄС (чи співпрацюють з ЄС).

Нові приписи Європейського Парламенту та Ради ЄС підлягають обов'язковому опрацюванню й впровадженню у національне законодавство та державоустрій у контексті реалізації договору про асоціацію між Україною та ЄС. Зазначене, власне, зумовлює й визначає потребу та напрями удосконалення системи захисту ПД в Україні.

Основними Законами, що на цей час регулюють відповідні відносини у державі, є закони України: «Про захист персональних даних» [14], «Про інформацію» [15], та «Про доступ до публічної інформації» [13] (далі: Закони), упорядковані та затверджені 13 січня 2011 р. Положення цих Законів системно узгоджені між собою й характеризують загальний порядок та умови опрацювання персональних даних.

Так, Закон України «Про інформацію» з'ясовує основні принципи, суб'єкти та об'єкти інформаційних відносин в Україні, поняття інформації, її види. Закон України «Про захист персональних даних» встановлює вимоги до обробки та захисту персональних даних, зокрема і в електронному середовищі. Зазначені вимоги відображають положення, запроваджені Конвенцією Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (відома як Конвенція РЄ № 108 згідно з порядком у серії Європейських договорів) [10] та розвинуті у Директиві Європейського Парламенту та Ради 95/46/ЄС «Про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних» [3], й інших рекомендаційних документах керівних органів Євросоюзу [30; 23; 25].

Закон «Про доступ до публічної інформації» затверджує систему здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень та інших розпорядників публічної інформації, визначених цим Законом, й інформації, що становить суспільний інтерес [13]. Тобто регламентує загальний порядок, за яким можна отримати потрібну (затребувану) інформацію.

Норми Законів поширюються на органи державної влади, інші державні органи, других суб'єктів, а також на юридичних осіб, котрі фінансуються із державного та місцевих бюджетів, осіб, які виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, зокрема надання освітніх, соціальних або державних послуг й суб'єктів господарювання, які володіють інформацією, що становить суспільний інтерес (суспільно необхідною інформацією), також і в частині оприлюднення та надання інформації за запитом [13].

Цілком закономірно, що під вимоги цих Законів потрапляють і наукові бібліотеки, зокрема, національні книгозбірні – як основні зберігачі інтелектуального та культурного надбання нації та хранителі приватної інформації, що стосується її користувачів.

Закон «Про доступ до публічної інформації» зобов'язує всіх розпорядників інформації надавати й оприлюднювати публічну інформацію, відображену та задокументовану будь-якими засобами та на будь-яких носіях, що була отримана або створена у процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень та інших розпорядників інформації [13].

Об'єктами адміністративно-правового захисту інформації визначено будь-які види інформації, з приводу якої суб'єкти права вступають у певні правові відносини та здійснюють свої права та обов'язки [15, ст. 650].

Усі види такої інформації, згідно з чинним українським законодавством, мають певний порядок доступу, що надає їй відповідний правовий статус. Так, відповідно до Ст. 20 Закону України «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію й інформацію з обмеженим доступом [15].

Саме остання має спеціальний режим адміністрування (особливо в період запровадження надзвичайного та воєнного станів, проведення військових операцій тощо), що покликаний захищати відомості (дані), вільний обсяг яких може порушити права та інтереси держави, суспільства, окремої особи. Характерною ознакою надання інформації обмеженого доступу є законодавчо визначена процедура її охорони як із боку держави, так і іншого власника інформації (суб'єкта), у нашому випадку – бібліотеки. Що стосується публічної інформації з обмеженим доступом, то нею згідно із Законом «Про доступ до публічної інформації» [13, ст. 21] є:

- конфіденційна інформація;
- таємна інформація;
- службова інформація.

Відповідно до ч. 2. ст. 21 Закону України «Про інформацію», конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою владних повноважень. Конфіденційна інформація може поширюватися за бажанням (волею, згодою) певної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених Законом.

Особи, які вважають, що їхні права та законні інтереси порушені розпорядниками інформації, мають право на оскарження рішень, дій чи бездіяльність розпорядників інформації до суду, яке здійснюється відповідно до Кодексу адміністративного судочинства України, а також на відшкодування матеріальної та моральної шкоди у порядку, визначеному законом.

Зважаючи на норми цих Законів, було ухвалено «**Типовий порядок обробки персональних даних у базах персональних даних**», затверджений наказом Міністерства юстиції України від 30.12.2011 р. № 3659/5, що на сьогодні втратив чинність на підставі Наказу Міністерства юстиції № 2523/5 від 28.11.2013 р. [22]. Орієнтовним рекомендованим документом із опрацювання персональних даних донині був «**Типовий порядок обробки персональних даних**», затверджений Наказом Уповноваженого Верховної Ради України з прав людини В. В. Лутковською від 08.01.2014 р. № 1/02-14 [21].

Проаналізувавши положення названих документів, українське право слід вважати прогресивним у контексті приписів Регламенту (зокрема, щодо принципів обробки інформації, порядку отримання згоди особи, переліку категорій ПД із особливим статусом тощо). Утім, законодавство України на сьогодні не повністю відповідає усім регламентним нормам, приміром – тим, що передбачають обов'язкове існування у державі системно-незалежної організаційної структури забезпечення захисту ПД. Це зобов'язує провідні національні інституції самостійно вибудовувати систему безпеки ПД відповідно до приписів Законів України [6; 11; 13; 14; 15] та Європейського права, а у разі бібліотечної діяльності – й з урахуванням стандартів: ISO, IFLA, ALA та AALL [26; 27; 32].

Об'єктивна необхідність удосконалення захисту особистих відомостей у бібліотечній справі визначається й розповсюдженим явищем неправомірних та несанкціонованих дій із персональними даними, які продовжують мати місце на міжнародному та національному рівнях. Сучасне поширення використання новітніх інформаційних технологій (Інтернет речей, Хмарних технологій, Великих Даних тощо), їх поєднання та накопичення, за впровадження у країні надзвичайного та воєнного станів вирішення проблеми безпеки даних значно ускладнили.

Це вимагає додаткових ресурсів та ухвалення оптимальних рішень щодо підвищення ефективності захисту персональних даних (особистих відомостей) і вироблення дієвих форм його забезпечення відповідно до сучасних європейських норм та континентального права.

Ратифіковані Європейським Парламентом та Радою ЄС правила захисту персональних даних громадян ЄС анонсують такі **нововведення**.

За Регламентом створюється Рада Європи із захисту даних як окремий орган ЄС. Склад Ради формується із представників контролюючих (наглядових) рад кожної держави-члена ЄС, Європейського супервайзера (інспектора) із захисту даних та представника Європейської Комісії, яка й призначає голову Ради.

Згідно з положеннями Конвенції № 108 Ради Європи [4;10] та «Пакету захисту даних», у всіх країнах-членах ЄС та державах, пов'язаних економічними відносинами з країнами-членами ЄС, мають бути створені спеціальні державні інституції із нагляду та контролю за дотриманням прав у сфері захисту даних. Національні наглядові органи повинні стимулювати розробку кодексів поведінки у сфері захисту персональних даних і вироблення механізмів удосконалення захисту даних з урахуванням специфіки сфер діяльності та конкретних потреб державних установ, корпорацій, підприємств тощо, а також здійснювати моніторинг їх виконання.

Відповідно до положень вказаних Документів Ради Європи та Європейського Союзу, **персональні дані** за будь-яких умов **не повинні** потрапляти до загальнодоступних інформаційних ресурсів. У контексті зазначеного вважається за необхідне звернути увагу на проблему впровадження у державне законодавство права приватної власності на особисті персональні дані.

Згідно Регламенту (містить 172 пункти Преамбули та долучає 99 статей) й Директив Європейського Союзу передбачено **виконання вимог щодо оброблення персональних даних**:

- **«законність, справедливість і прозорість»** – ПД мають оброблятися, використовуватися й поширюватися законно, справедливо та відкрито стосовно суб'єкта даних;

- **«обмеження цілей»** – ПД повинні збиратися для певної, конкретної та законної мети й не підлягати додатковій обробці, яка несумісна з цією метою; подальша обробка з метою архівації згідно з суспільними інтересами, для наукових, дослідницьких, історичних та статистичних цілей не повинна вважатися несумісною з початковою метою;

- **«мінімізація даних»** – встановлює обмеження тими ПД, які відповідають і є необхідні для досягнення мети обробки даних. Не можна збирати ПД у більшому обсязі, ніж це було визначено для цілей опрацювання;

- **«точності»** – регулює відповідність ПД відомостям про суб'єкта даних. ПД мають бути точними та, за необхідності, актуалізованими (слід уживати усіх обґрунтованих заходів, щоб забезпечити невідкладне видалення або виправлення неточних чи застарілих персональних даних, з урахуванням мети опрацювання даних);

- **«обмеження зберігання»** – ПД повинні зберігатися у формі, що дозволяє ідентифікацію суб'єкта даних (користувача) не довше, ніж це необхідно для мети обробки персональних даних. Персональні дані припустимо зберігати упродовж тривалішого періоду за умови, що їх обробка здійснюється винятково з метою збереження «згідно із суспільними інтересами»; для цілей архівації, а також наукового чи історичного дослідження або статистики – за умови впровадження відповідних технічних та організаційних заходів і гарантування прав та свобод суб'єкта даних. Регламент також уточнює, що установи мають проводити регулярні перевірки з метою очищення носіїв інформації;

- **«цілісність та конфіденційність»** – ПД повинні оброблюватися у спосіб, що забезпечує відповідний рівень безпеки персональних даних, зокрема захист від несанкціонованої або незаконної обробки й випадкової втрати, знищення або пошкодження з використанням відповідних технічних або організаційних заходів;

- **«підзвітність»** – характеризує діяльність із призначення в організаціях посадових осіб, які відповідають за захист персональних даних; ведення обліку, записів і перевірки дій та нормативної документації з виконання приписів та порядку Регламенту [20, с. 132–133].

Як свідчить аналіз вступних та заключних приписів Регламенту, задекларовані принципи є обов'язковими та універсальними для усього Європейського Союзу.

У Преамбулі Документів наголошується, що розгляд будь-якого складного питання може бути успішним лише за наявності системи понять, завдяки яким розкриваються сутнісні елементи цього явища. Відповідно до приписів п. 7.4.2.7 (третьої) редакцію міжнародного стандарту ISO 704:2009, у якому сформульовано вимогу мовної правильності терміна (*linguistic correctness*), Регламентом конкретизовано термін «персональні дані», введено поняття «контролер», «обробник» («оператор»), встановлено «право на видалення» («право бути забутим») тощо.

Якщо раніше ПД уважалися тільки документи, що зберігають імена, адреси тощо, то сьогодні це визначення значно розширено. Дані, пов'язані з IP-адресами,

е-поштою та cookie-файли, які містять приватні відомості стосовно користувача також охоплюються положеннями Регламенту. До категорії «особливих» або «чутливих» відомостей про особу віднесені генетичні та/або біометричні дані. Характерним є те, що ПД вважаються тільки ті дані, за якими особу ймовірно ідентифікувати.

Під «захистом даних» (*data protection*) розуміються будь-які правові, організаційні та технічні засоби захисту інформації персонального змісту, а для комплексного захисту даних на міжнародному рівні застосовується термін «безпека даних» (*data security*). «Втручання у персональні дані» означає порушення режиму безпеки, що тягне за собою випадкове або незаконне знищення, втрату, зміну, несанкціоноване розкриття або надання доступу до персональних даних, які передаються, зберігаються чи іншим чином зазнають оброблення [20; с. 132].

Регламент значно розширює права громадян (суб'єкта даних, фізичної особи) стосовно контролю за своїми ПД та встановлює суттєві вимоги до форми отримання згоди на обробку даних. Згода особи на обробку її ПД повинна бути визначена у формі однозначно чіткого твердження на відповідний дозвіл. Суб'єкт має право на виправлення ПД. Більш того, суб'єкт має право вимагати припинення обробки своїх даних.

Зокрема, Регламент закріплює за суб'єктом ПД «право бути забутим» (*right to be forgotten*). Конкретизовано можливість видалення даних та з'ясовано умови використання «права бути забутим», тобто права на видалення персональних даних та припинення їх опрацювання. Крім того, передбачено право на обмеження обсягів обробки ПД.

Пошукові системи та соціальні мережі повинні видаляти фотознімки, світлинки, відбитки, зображення, відтворення та інші відомості, які стосуються суб'єкта даних на його вимогу. Обробка фотокарток не має розглядатися як обробка особливих категорій персональних даних. Характерно, що згідно з чинним українського законодавством зйомка у публічних місцях донині була дозволена, але на території ЄС уже діяли вказані норми.

Фізичні особи мають бути обізнані про небезпеки, правила, гарантії та права стосовно оброблення своїх ПД і реалізації своїх прав щодо подібного опрацювання. Значну увагу у тексті Регламенту приділено питанню «безпеки персональних даних» та «оцінці впливу захисту даних».

Згідно Регламенту, немає конкретних вимог щодо ступеню, порядку та способу захисту даних – кожен суб'єкт обробки (організація, підприємство, компанія тощо, у нашому випадку – книгозбірня) може обирати правові механізми та засоби самостійно залежно від наявних загроз та ризиків і їх класифікації (*classification*). Визначальне правило – технічні та організаційні заходи гарантування рівня безпеки мають бути співвідносні наявним ризикам й узгоджуватися з чинними правовими приписами та стандартами.

У чинних в Україні стандартах – «ISO/IEC 20001. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки» [19] й «ISO/IEC 38500:2016 (ISO/IEC 38500:2015, IDT) [5], «Інформаційні технології. Управління

ІТ в організації» передбачено можливі шляхи реалізації загроз та регламентовані терміни, пов'язані з інформаційною безпекою та захистом даних, які безпосередньо стосуються систематизації загроз. Відповідно до зазначених документів, загрози можуть здійснюватись: технічними каналами, каналами спеціального впливу, несанкціонованим доступом. Тому, на нашу думку, цілком логічним для бібліотеки є класифікація загроз: загрози витоку інформації, загрози порушення цілісності інформації, загрози блокування інформації.

Сьогодні визначені типові алгоритми локалізації загроз й етапи формування системи захисту даних, які застосовуються при створенні цілісної системи безпеки даних у будь-якій країні. Цілісна система інформаційної безпеки, згідно з Документами, повинна охоплювати як профілактичну, так і внутрішню оперативну роботу. Профілактична робота передбачає використання технічних методів і способів контролю. Внутрішня оперативна робота – це процес ідентифікації джерел загроз та виявлення інформації небезпечного характеру.

Згідно з Регламентом, у практичній діяльності організації щодо захисту ПД головними є суб'єкт даних, контролер та процесор (оператор, обробник). Суб'єкт даних – це фізична особа, ПД якої обробляються. Контролер – фізична чи юридична особа, т. з. «власник» бази даних. Контролери визначають необхідні дії з ПД та відповідають за їх обробку. Процесор – фізична чи юридична особа, виконавець обробки за дорученням контролера. Контролер та обробник можуть бути однією особою.

Будь-яка організація може призначити співробітника (Уповноважену особу) із захисту даних для управління процесами обробки та контролю за дотриманням вимог Регламенту. Ця вимога обов'язкова для: всіх державних органів; організацій, чий види діяльності передбачають масштабний і систематичний моніторинг окремих осіб; організацій та установ, чий типи функціонування передбачають обробку спеціальних категорій даних.

Суб'єкти ПД мають право звертатися до посадової особи, котра відповідає за захист даних, з усіх питань, пов'язаних з обробкою їх ПД та реалізацією їхніх прав відповідно до Регламенту.

Регламентом посилюється відповідальність за порушення його принципів як до організацій в ЄС, так і до зарубіжних інституцій, якщо вони обробляють ПД фізичних осіб, що перебувають в ЄС – розмір штрафу встановлено до 20 млн Євро або 4% від загального річного обігу установи за попередній фінансовий рік залежно від того, яка сума є більшою.

Важливим є й те, що реалізація положень нового порядку захисту даних потребує нових підходів та докорінних змін практичної діяльності не тільки у державах-членах ЄС, але й у всіх інших країнах-партнерах держав ЄС, у багатьох з яких рівень захисту ПД і раніше не завжди відповідав основним принципам європейських правових стандартів.

Національна бібліотека України імені В. І. Вернадського (далі НБУВ) як провідна державна інституція бере оперативну участь у запровадженні нових європейських стандартів безпеки даних – технічних та організаційних – у практичній роботі.

На базі НБУВ реалізовано нову технологію запису у середовищі АБІС «ІРБІС» та розроблено першорядні регламентуючі документи – «Анкету для реєстрації користувачів НБУВ» (далі Анкета) й «Інструкцію щодо захисту та збереження персональних даних користувачів НБУВ» (далі Інструкція). Вироблено єдину фактографічну основу для запису до бібліотеки громадян України та інших держав (визначальне положення Документів).

Одним із завдань, що вирішувалось у процесі організації автоматизованого робочого місця пункту запису читачів (далі АРМ ПЗЧ), було розроблення технічних засобів для гарантування цілісності та конфіденційності облікової бази читачів НБУВ. Із цією метою Відділом програмно-технічного забезпечення комп'ютерних мереж НБУВ (далі ВПТЗКМ НБУВ) та Відділом комплексного бібліотечного обслуговування НБУВ (далі ВКБО НБУВ) було передбачено заходи для: забезпечення достовірності даних; управління доступом до інформації; керування паралельним виконанням різних дій з опрацювання інформації; відновлення облікової бази після будь-яких апаратних чи/та програмних збоїв.

Усі ПД отримуються безпосередньо у читача (згідно Регламенту: суб'єкта даних). Одночасно збережено картку реєстрації користувача НБУВ, контрольні листки та ручну реєстрацію відвідувачів бібліотеки, що дозволяє уникнути похибки стосовно особистих відомостей читача, кількості візитів та загального числа користувачів НБУВ.

Картка реєстрації користувача НБУВ містить певні особисті дані: ПІБ, рік народження, серія та номер паспорта, освіта, науковий ступінь, місце праці чи навчання, посада, місце реєстрації, телефон та підпис.

Відповідно до європейських стандартів паспортні дані, зображення обличчя та власний підпис є обов'язковою інформацією для ідентифікації особи. Інша інформація у картці реєстрації є факультативною (допоміжною) та надається особою на власний розсуд. Персональні дані щодо національності та місця народження користувача, його політичних, релігійних, конфесійних переконань, а також відомості, що стосуються здоров'я або особистого життя (одна з фундаментальних вимог розглянутих Документів та Конвенції РЄ № 108) – читачами НБУВ не надаються й не підлягають автоматизованій обробці.

Опрацювання та збереження ПД читачів НБУВ відбувається лише за їхньої згоди, що зафіксовано у «Загальних правилах користування Національною бібліотекою України імені В. І. Вернадського». При записі до НБУВ особа своїм підписом у реєстраційній картці надає дозвіл на використання персональних даних із метою її ідентифікації як користувача Бібліотеки.

Персональні дані, надані користувачем та занесені до БД «Читачі НБУВ», є різновидом конфіденційної інформації, тобто інформації з обмеженим доступом, що вимагає відповідної організації роботи з нею, а саме: вона не може бути порушена («принцип цілісності»), оприлюднена без згоди сторін та має бути надійно захищеною.

Забезпечення цілісності та конфіденційності БД «Читачі НБУВ» регульовано з управлінням доступу до інформації. Оброблення ПД здійснюється тільки

визначеними працівниками (згідно з Регламентом: процесором, оператором, обробником) – співробітниками Сектору запису читачів та контролю відвідувань НБУВ. Посадові особи НБУВ, котрі мають доступ до ПД, зобов'язуються використовувати інформацію щодо особистих відомостей користувачів НБУВ винятково для цілей, пов'язаних із виконанням своїх службових обов'язків. Використання ПД читачів НБУВ дозволене в історичних, статистичних та науково-дослідних цілях, виконується тільки у знеособленому вигляді.

Відповідно до підсумкових приписів законодавства ЄС, наказом генерального директора НБУВ призначається співробітник із захисту даних (згідно Регламенту: Уповноважена особа) – головний бібліотекар Сектору запису читачів та контролю відвідувань НБУВ, для управління процесами обробки ПД і контролю за дотриманням вимог Інструкції. Користувачі НБУВ (згідно Регламенту: суб'єкти даних) можуть звертатися до нього з усіх питань, пов'язаних з обробкою їхніх особистих даних та реалізацією їхніх прав згідно з положеннями Інструкції, а також приписами й нормами українського та європейського законодавств.

Співробітники НБУВ, які працюють із персональними даними, інформуються головним бібліотекарем Сектору запису читачів та контролю відвідувань НБУВ і беруть зобов'язання про нерозголошення особистих даних, які їм було довірено або які стали відомі у зв'язку з виконанням посадових обов'язків.

Персональні дані, які надходять до БД «Читачі НБУВ», обробляються із застосуванням комплексної системи захисту інформації та згідно з положеннями регулятивних Законів України, правових приписів та стандартів ЄС.

Отже, **цілісна система захисту ПД у бібліотечній галузі** має базуватися на таких основних принципах:

- захист особистих даних від несанкціонованого доступу та незаконної обробки;
- зменшення обсягів особистих відомостей та даних, що зберігаються;
- виконання контролюючих та превентивних заходів;
- виправлення та/чи видалення даних;
- вироблення плану реагування на загрози з використанням відповідних організаційних та технічних заходів (особливо важливо – за надзвичайного чи воєнного станів).

Висновки. Дотримуючись прикінцевих законодавчих актів та постанов України, приписів Конвенції РЄ № 108, положень «Пакету захисту даних», зважаючи на особливості надзвичайного та воєнного стану, що були запроваджені у країні – організацію системи безпеки даних на сьогодні потрібно розглядати та вибудовувати, виходячи з сутнісних зв'язків, чинних інформаційних нормативно-правових актів та загроз щодо кожного конкретного суб'єкта.

Рівень та побудова захисту особистих даних користувачів мають бути еквівалентними в усіх книгозбірнях. Інакше відмінності в організації системи безпеки даних, зокрема того, що стосується обробки, використання та зберігання особистих відомостей можуть стати на заваді вільному обігу ПД та бути перешкодою для здійснення міжбібліотечної інтеграції. Ці обставини вимагають більш

узгодженої структури загальнобібліотечної організації захисту ПД за умов жорсткого контролю дотримання приписів європейських та українських правових стандартів, що своєю чергою підтримуватиме розвиток цифрових ресурсів та послуг у межах внутрішнього забезпечення й сприятиме співпраці з іншими бібліотечними установами держав ЄС.

Читачі повинні мати можливість контролю застосування своїх ПД та гарантій щодо надання на це визначеної ними особисто відповідної згоди. Цьому може сприяти запровадження у практику бібліотечної роботи універсально-загального європейського критерію – «право власності особистості (користувача) на свої персональні дані», монополія, на яку обмежується винятково в інтересах національної безпеки, суспільної необхідності та прав людини. А це вимагає вироблення відповідної нормативно-методичної бази й єдиної структурно-регулятивної системи захисту ПД користувачів бібліотек.

Важливо організувати наукову розробку актуальних проблем захисту ПД, зокрема щодо: приведення понятійного апарату у відповідність до визначень та формулювань «Пакету захисту даних»; теоретико-правових проблем захисту приватності та права приватної власності користувача на свої ПД як складники загальної системи безпеки даних; правового обмеження дій бібліотечних установ щодо «вимагання» у користувачів їхньої згоди на обробку та надання третім особам їх ПД; закріплення права користувачів контролювати та відкликати, уточнювати чи видаляти свої ПД у будь-яких бібліотечних системах та базах даних.

Національна бібліотека України імені В. І. Вернадського бере ефективну безпосередню участь у реалізації означених завдань та принципів. Технологічні та організаційні рішення, інструктивні матеріали, отримані у процесі розробки засобів для гарантування безпеки, забезпечення цілісності та конфіденційності облікової бази читачів НБУВ, можуть бути застосовані у процесі розробки й налагодження системи захисту ПД у інших книгозбірнях й сферах діяльності.

Список бібліографічних посилань

1. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3. С. 31–48.

2. Директива (ЄС) 2016/680 Європейського Парламенту та Ради «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади з метою запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, або виконання кримінальних покарань та про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ІНА» від 27.04.2016 р. *Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: збірник документів / неофіційний пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука*. Київ : ТОВ «Видавничий дім «АртЕк», 2018. С. 108–159.

3. Директива 95/46/ЄС Європейського парламенту і Ради Європейського Союзу від 24 жовтня 1995 року «Про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних». *Інформація і право*. 2013. № 3. С. 152–171.

4. Додатковий протокол до Конвенції Ради Європи № 108 від 8 листопада 2001 року «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та трансграничних потоків даних» (Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal data regarding supervisory authorities and transborder data flows). *Інформація і право*. 2013. № 3. С. 150–151.

5. *ДСТУ ISO/IEC 38500:2016 (ISO/IEC 38500:2015, IDT) Інформаційні технології. Управління IT в організації* : веб-сайт. URL: <http://document.ua/informaciini-tehnologiyi-upravlinnja-it-v-organizaciyi-nor31760.html>.

6. Законодавче забезпечення розвитку інформаційного суспільства в Україні (Рекомендації парламентських слухань): Постанова Верховної Ради України від 03.07.14 р. № 1565-VII. *Відомості Верховної Ради України (ВВР)*. 2014. № 33. Ст. 1163.

7. *Защита персональных данных* / А. Баранов, В. Брыжко, Ю. Базанов. Национальное агенство по информатизации при Президенте Украины. Киев : ВАТ КП ОТИ, 1998. 128 с.

8. Коваль Т. М., Лопата О. М. Нормативно-правова база та система стандартів ЄС та IFLA щодо збереження персональних даних користувачів бібліотек. *Бібліотека. Наука. Комунікація: 100-річчя Національної бібліотеки України імені В. І. Вернадського*. Матеріали міжнар. наук. конф. (Київ, 6–8 лист. 2018 р.). Київ, 2018. С. 48–55.

9. Коваль Т. М., Лопата О. М. Особливості механізму захисту персональних даних користувачів бібліотек в законодавстві ЄС та системі стандартів IFLA. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. Київ, 2019. Вип. 56. С. 135–157.

10. Конвенція Ради Європи від 28 січня 1981 року № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Amendment to Convention ETS No. 108 allowing the European Communities to accede). *Інформація і право*. 2013. № 3. С. 143–149.

11. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. *Відомості Верховної Ради України (ВВР)*. 1996. № 30. Ст. 32.

12. Мельник К. С. Теоретико-правовий зміст терміну «персональні дані». *Інформація і право*. 2013. № 3. С. 49–63.

13. Про доступ до публічної інформації: Закон України від 13.01.11 р. №2939-VI. *Відомості Верховної Ради України (ВВР)*. 2011. № 32. Ст. 314.

14. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI. *Відомості Верховної Ради України (ВВР)*. 2010. № 34. Ст. 481.

15. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. *Відомості Верховної Ради України (ВВР)*. 1992. № 48. Ст. 650.

16. Про ратифікацію Адміністративних домовленостей щодо охорони інформації з обмеженим доступом між урядом України та Організацією Північноатлантичного договору: Закон України від 24.05.17 р. № 2068-VIII. *Відомості Верховної Ради України (ВВР)*. 2017. № 26. Ст. 299.

17. Проценко В. А. Особливості механізмів захисту персональних даних в законодавстві ЄС. *Правова інформатика*. 2012. № 2. С. 45–50.

18. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради «Про захист осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальний Регламент щодо захисту даних)» від 27.04.16 р. *Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: збірник документів / неофіційний пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука*. Київ: ТОВ «Видавничий дім «АртЕк», 2018. С. 7–107.

19. *Стандарт ISO/IEC 27001: 2013 «Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки»* : веб-сайт. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf.

20. *Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: збірник документів / неофіційний пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука*. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 180 с.

21. Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини В. В. Лутковською від 08.01.2014 № 1/02-14 : веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.

22. Типовий порядок обробки персональних даних у базах персональних даних, затверджений наказом Міністерства юстиції України від 30.12.2011 № 3659/5 : веб-сайт. URL: <https://zakon.rada.gov.ua/laws/show/z0001-12#Text>.

23. 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC : веб-сайт. URL: <http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:EN:NOT>.

24. Ayala Daniel. Security and Privacy for Libraries in 2017: веб-сайт. URL: <http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=9&sid=19da8a90-0ab8-4f83-8a4e-0605a2a76986%40sessionmgr102>.

25. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) : веб-сайт. URL: <https://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT>.

26. IFLA Code of Ethics for Librarians and other Information Workers : веб-сайт. URL: <http://www.ifla.org/news/ifla-code-if-ethics-for-librarian-and-other-information-workers-full-version>.

27. IFLA Trend Report : веб-сайт. URL: <https://trends.ifla.org/2013-timeline>.

28. Protection of personal data : веб-сайт. URL: https://www.europa.eu/legislation_summaries/information_society/data_protection/114012_en.htm.

29. Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights adopted on 7 September 1999/ The Working Party on the Protection of Individuals with regard to Processing of Personal Data. Brussels, 1999 : веб-сайт. URL: <http://www.ec.europa.eu/justice/policies/privacy/doc/wpdocs/1999/wp26en.pdf>.

30. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data : веб-сайт. URL: <http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:NOT>. – 37.

31. Right to Privacy in the Digital Age : веб-сайт. URL: <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>.

32. Statement on Privacy in the Library Environment : веб-сайт. URL: <https://www.ifla.org/node/9803>.

References

1. Bryzhko, V. M. (2013). Zakhyst personalnykh danykh: realiyi ta praktyka suchasnosti [Personal data protection: realities and contemporary practice]. *Informatsiia i pravo*, 3, 31-48. [In Ukrainian].

2. Yevropeyskyi Parlament (2016). Dyrektyva (EC) 2016/680 Yevropeiskoho Parlamentu ta Rady vid 27 kvitnia 2016 roku "Pro zakhyst fizychnykh osib u zviazku z obrobkoiu personalnykh danykh kompetentnymy organamy vlady z metoiu zapobihannia, rozsliduvannia, vyjavlennia chy sudovoho peresliduvannia kryminalnykh pravoporushen, abo vykonannia kryminalnykh pokaran ta pro vilne peremishchennia takykh danykh, i skasuvannia Ramkovogo rishennia Rady 2008/977/JHA" [On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA: Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016]. In *Suchasni pravovi standarty Yevropeiskoho Soiuzu u sferi zakhystu personalnykh danykh: zbirnyk dokumentiv* [The Current Legal Standards of the European Union in the Field of Personal Data Protection: collection of documents] (Editor Bryzhko, V., translator Maistrenko, I., introduction Pylypchuk, V., pp. 108-159). Kyiv, Ukraine: TOV "Vydavnychiy dim "ArtEk". [In Ukrainian].

3. Yevropeyskyi Parlament (1995). Dyrektyva 95/46/leS Yevropeiskoho Parlamentu i Rady Yevropeiskoho Soiuzu vid 24 zhovtnia 1995 roku "Pro zakhyst osib u zviazku z obrobkoiu personalnykh danykh i vilnym obihom tsykh danykh" [Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data]. *Informatsiia i pravo*, 2013, 3, 152-171. [In Ukrainian].

4. Rady Yevropy (2001). Dodatkovyi protokol do Konventsii Rady Yevropy No 108 vid 8 lystopada 2001 roku «Pro zakhyst osib u zviazku z avtomatyzovanoiu obrobkoiu personalnykh danykh shchodo orhaniv nahliadu ta transkordonykh potokiv danykh» [Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows]. *Informatsiia i pravo*, 2013, 3, 150-151. [In Ukrainian].

5. (2016). *DSTU ISO/IEC 38500:2016 (ISO/IEC 38500:2015, IDT) Informatsiini tekhnologii. Upravlinnia IT v organizatsii* [web-site]. [Information Technology. IT management in the organization]. Retrieved from http://document.ua/informaciini-tehnologiyi_upravlinnja-it-v-organizaciyi-nor31760.html. [In Ukrainian].
6. Verkhovna Rada Ukrainy (2014, Lypen 3). Zakonodavche zabezpechennia rozvytku informatsiinoho suspilstva v Ukraini (Rekomendatsii parlamentskykh slukhan): Postanova Verkhovnoi Rady Ukrainy No 1565-VII [web-site]. [On the Zakonodavche zabezpechennia rozvytku informatsiinogo suspilstva v Ukrainy: Resolution of the Verkhovna Rada of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 33, Art. 1163. [In Ukrainian].
7. Baranov, A., Bryzhko, V., & Bazanov, Yu. (Eds). (1998). *Zashchita personalnykh danykh* [Personal Data Protection]. Kyiv, Ukraine: VAT KP OTI. [In Ukrainian].
8. Koval, T. M., & Lopata, O. M. (2018, November). Normatyvno-pravova baza ta systema standartov YeS ta IFLA shchodo zberezhennia personalnykh danykh korystuvachiv bibliotek [Regulatory framework and system of EU and IFLA standards to preserve personal data library users]. In *Library. Science. Communication. Proceedings of the International Scientific Conference* (pp. 48-55), Vernadsky National Library of Ukraine. Kyiv, Ukraine. [In Ukrainian].
9. Koval, T. M., & Lopata, O. M. (2019). Osoblyvosti mekhanizmu zakhystu personalnykh danykh korystuvachiv bibliotek v zakonodavstvi YeS ta systemi standartiv IFLA [Singularities of the mechanism to protection of patron data library visitors in the legislation of EU and system of standards IFLA]. *Naukovi pratsi Natsionalnoi biblioteky Ukrainy imeni V. I. Vernadskogo*, 56, 135-157. Kyiv, Ukraine. [In Ukrainian].
10. Rada Yevropy (1981). Konventsiiia Rady Yevropy vid 28 sichnia 1981 roku No 108 «Pro zakhyst osib u Zviazku z avtomatyzovanoi obrobkoiu personalnykh danykh» [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Amendment to Convention ETS No 108 allowing the European Communities to accede]. *Informatsiia i pravo*, 2013, 3, 143-149. [In Ukrainian].
11. Verkhovna Rada Ukrainy (1996, Cherven 28). Konstytutsiia Ukrainy: Zakon Ukrainy No 254k/96-VR [The Constitution of Ukraine: Law of Ukraine No 254 k/96 – BP]. *Vidomosti Verkhovnoi Rady Ukrainy*, 30, Art. 32. [In Ukrainian].
12. Melnyk K. S. (2013). Teoretyko-pravovyi zmist terminu «personalni dani» [Theoretical and legal content of the term "personal data"]. *Informatsiia i pravo*, 3, (pp. 49-63). [In Ukrainian].
13. Verkhovna Rada Ukrainy (2011, Sichen 13). Pro dostup do publichnoi informatsii: Zakon Ukrainy No 2939-VI [About access to public information: Law of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 32, Art. 314. [In Ukrainian].
14. Verkhovna Rada Ukrainy (2010, Lypen 13). Pro zakhyst personalnykh danykh: Zakon Ukrainy No 2939-VI [On the protection of personal data: Law of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 34, Art. 481. [In Ukrainian].
15. Verkhovna Rada Ukrainy (1992, Zhovten 2). Pro informatsiiu: Zakon Ukrainy No 2657-XII [About the information: Law of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 48, Art. 650. [In Ukrainian].
16. Verkhovna Rada Ukrainy (2017, Traven 24). Pro ratyfikatsiiu Administratyvnykh domovlenosti shchodo okhorony informatsii z obmezhnym dostupom mizh uriadom Ukrainy ta Orhanizatsieiu Pivnichnoatlantychnoho dohovoru: Zakon Ukrainy No 2068-VIII [On the Ratification of the Administrative Arrangements for the Protection of Restricted Information Between the Government of Ukraine and the North Atlantic Treaty Organization: Law of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 26, Art. 299. [In Ukrainian].
17. Protsenko V. A. (2012). Osoblyvosti mekhanizmiv zakhystu personalnykh danykh v zakonodavstvi YeS [Peculiarities of mechanisms for protection of personal data in the EU legislation EU]. *Pravova informatyka*, 2, 45-50. [In Ukrainian].
18. Yevropeyskyi Parlament (2016). Reglament (EC) 2016/679 Yevropeiskoho Parlamentu ta Rady vid 27 kvitnia 2016 roku "Pro zakhyst osib u zviazku z obrobkoiu personalnykh danykh ta pro vilne peremischennia tsykh danykh, a takozh pro skasuvannia Dyrektyvy 95/46/leS (Zagalnyi Reglament shchodo zakhystu danykh)" [On the protection of natural persons with regard to the processing of personal data and on the movement of such data, and repealing Directive 95/46/EC (General Data Protection

Regulation); Regalement (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016]. In *Suchasni pravovi standarty Yevropeiskoho Soiuzu u sferi zakhystu personalnykh danykh: zbirnyk dokumentiv* [The Current Legal Standards of the European Union in the Field of Personal Data Protection: collection of documents] (Editor Bryzhko, V., translator Maistrenko, I., introduction Pylypchuk, V., pp. 7-107). Kyiv, Ukraine: TOV "Vydavnychiy dim "ArtEk". [In Ukrainian].

19. (2013). *Standart ISO/IEC 27001: 2013 "Informatsiini tekhnologii. Metody zakhystu. Systemy menedzhmentu informatsiinoi bezpeky"* [web-site]. [Information Technology. Methods of protection. Information security management system]. Retrieved from https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf. [In Ukrainian].

20. Maistrenko, I., Bryzhko, V., & Pylypchuk, V. (Translator, Editor & Introduction). (2018). *Suchasni pravovi standarty Yevropeiskoho Soiuzu u sferi zakhystu personalnykh danykh: zbirnyk dokumentiv* [The Current Legal Standards of the European Union in the Field of Personal Data Protection: collection of documents]. Kyiv, Ukraine: TOV "Vydavnychiy dim "ArtEk", Ukraine. [In Ukrainian].

21. (2014). *Typovyi poriadok obrobky personalnykh danykh, zatverdzhenyi Nakazom Upovnovazhenoho Verkhovnoi Rady Ukrainy z prav liudyny V. V. Lutkovskoiu vid 8 sichnia 2014 r. No 1/02-14.* [web-site]. [Standard procedure for processing personal data, approved by the Order of the Commissioner of the Verkhovna Rada of Ukraine for Human Rights V. V. Lutkovska dated 08.01.2014 № 1 / 02-14]. Retrieved from https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text. [In Ukrainian].

22. (2011). *Typovyi poriadok obrobky personalnykh danykh u bazakh personalnykh danykh, zatverdzhenyi nakazom Ministerstva yustytzii Ukrainy vid 30 grudnia 2011 r. No 3659/5* [web-site]. [Standard procedure for processing personal data in personal databases, approved by the order of the Ministry of Justice of Ukraine dated 30.12.2011 No 3659/5]. Retrieved from <https://zakon.rada.gov.ua/laws/show/z0001-12#Text>. [In Ukrainian].

23. (2001). 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC. Retrieved from <http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:EN:NOT> [In English].

24. Ayala Daniel. *Security and Privacy for Libraries in 2017*. Retrieved from <http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=9&sid=19da8a90-0ab8-4f83-8a4e-0605a2a76986%40sessionmgr102> [In English].

25. European Parliament (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Retrieved from <https://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT> [In English].

26. (2012). IFLA Code of Ethics for Librarians and other Information Workers. Retrieved from <http://www.ifla.org/news/ifla-code-if-ethics-for-librarian-and-other-information-workers-full-version> [In English].

27. (2013) IFLA Trend Report. Retrieved from <https://trends.ifla.org/2013-timeline> [In English].

28. (2012) Protection of personal data. Retrieved from https://www.europa.eu/legislation_summaries/information_society/data_protection/114012_en.htm [In English].

29. (1999). The Working Party on the Protection of Individuals with regard to Processing of Personal Data (1999, September 7). Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights. Brussels. Retrieved from <https://www.ec.europa.eu/justice/policies/privacy/doc/wpdocs/1999/wp26en.pdf> [In English].

30. European Parliament (2000). Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Retrieved from <http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:NOT> [In English].

31. (2013, 2014) Right to Privacy in the Digital Age. Retrieved from <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx> [In English].

32. (2015). Statement on Privacy in the Library Environment. Retrieved from <https://www.ifla.org/node/9803> [In English].

Olena Lopata,

<https://orcid.org/0000-0002-1386-3409>,

Junior Researcher,

V. I. Vernadskyi National Library of Ukraine (Kyiv, Ukraine)

**ENSURING THE SECURITY OF LIBRARY USERS' DATA IN THE CONTEXT
OF NEW LEGAL STANDARDS OF THE EUROPEAN UNION**

The purpose of this research. The piece of writing about basic tendencies in principles and mechanisms of a new order of protection and safety of the personal data in the European legal standards, introduction to the national legislation of universal criterion for the person's data protection. Modern issues of personal data security and European Union (hereinafter: EU) data security safeguarding mechanisms provided by law. **Methodology** of the research is based on systemic and structural approaches, on methods of comparative, logical and source analysis, including interdisciplinary approach. **Scientific novelty.** The main cause of this article is to study the legal norms «On the protection of natural persons with regard to the processing of personal data and on the movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): Regalement (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016» and «On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA: Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016» in modern conditions and compilation of legal requirements to establish an integrated system of protection of personal data in the library area. This publication analyzes the state of the Ukrainian legislation as related to restriction of the access to personal information, its compliance with the principles of international law in the European integration of Ukraine and examines the state of European law in this field. The article outlines current issues of processing and protection of personal data in modern conditions, as well as analyses the problematic aspects of privacy in the practical activities of libraries. The classification of database integrity restrictions is given. **Conclusions.** The organization of the data security system today, needs to be considered and built: based on the essential links, current information regulations and each individual entity. The role of the Vernasky National Library of Ukraine in realization of European standards of data protection – organizational and technical, in the practice of library work is emphasized.

Keywords: transformation, personal data, data security, data protection, information processing, personal data protection system, legal standart.

V. I. Vernadskyi National Library of Ukraine
3, Holosiivskyi ave, Kyiv, 03039, Ukraine
e-mail:lopata@nbuv.gov.ua

Стаття надійшла до редакції 25.05.2022 р.