ISSN 2707-1898 (print)
Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2021.02.051
Article received 06.08.2021 p.
Article accepted 23.11.2021 p.
UDK 004.6:341

Correspondence author
M. M. Shabatura
mariia.m.mandrona@lpnu.ua

М. М. Шабатура, Р. О. Салашник
Національний університет "Львівська політехніка", м. Львів, Україна

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЗА УКРАЇНСЬКИМ ЗАКОНОДАВСТВОМ ТА GDPR

Розглянуто та охарактеризовано проблему стрімкого розвитку сучасних технологій, через які є актуальне питання щодо захисту персональних даних користувачів мережі Інтернет. Проаналізовано сучасний стан забезпечення захисту персональних даних за вимогами українського законодавства та Загального регламенту про захист персональних даних (англ. *General Data Protection Regulation*, GDPR). Визначено, які саме дані належать до персональних даних та чому підлягають захисту. З'ясовано, що персональні дані – це вид інформації з обмеженим доступом, тому обробляти ці дані потрібно тільки у системах, на яких встановлено комплексну систему захисту інформації, що має сертифікат відповідності. Оскільки Україна – одна з перших країн, яка впровадила електронний паспорт, розглянуто додаток "Дія". Проаналізовано Кодекс України про адміністративні правопорушення та Кримінальний Кодекс України за порушення вимог та недотримання закону щодо захисту персональних даних, описано штрафні санкції. Проаналізовано вимоги до оброблення та захисту персональних даних за Європейським стандартом GDPR, а саме: процедуру псевдонімізації, анімізації, шифрування та ін. Розглянуто комплекс технічних рішень та інструментів кібербезпеки для впровадження відповідності нормам GDPR. Підкреслено важливість організаційних заходів безпеки, таких як: навчання персоналу, створення політики конфіденційності, правильна організація процесів, надання доступу до персональних даних тільки уповноваженим працівникам та інші. З'ясовано міру покарання за порушення недотримання вимог GDPR. Наголошено, що для покращення рівня захищеності персональних даних важливим фактором є підвищення рівня обізнаності, які часто ігнорують проблеми, пов'язані зі захистом особистих даних, зокрема через неповне розуміння законодавчих стандартів та вимог у цій сфері.

Ключові слова: персональні дані; оброблення; додаток "Дія"; захист; GDPR.

Вступ

З огляду на стрімкий розвиток новітніх технологій, питання захисту інформації у сучасному світі набуло значної уваги. У 2021 р. кожен має доступ до будь-яких інформаційних каналів та джерел, не задумуючись, які наслідки спричинять надмірний та неконтрольований доступ до особистої інформації для необмеженої кількості користувачів. Несанкціонований доступ до інформації, неналежно захищений доступ до особистих даних – це широкомасштабна проблема, яку варто порушувати та вирішувати. Так, легкий доступ до інформації справді полегшує життя та надає більше можливостей для комфортного існування, але швидкий розвиток інформаційно-комунікаційних технологій потребує розроблення та впровадження адекватних захисних механізмів, які будуть спроможні захистити особисті дані та права людей, щоб кожен, хто застосував цей механізм у своєму житті, був впевнений у безпеці своїх даних, а відтак – у безпеці свого життя.

Для досягнення цієї мети 25 травня 2018 р. було введено положення Загального регламенту захисту даних (англ. *General Data Protection Regulation*, далі – GDPR) щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони, а також експорту персональних даних за їхні межі.

Підвищення рівня обізнаності громадян про захист персональних даних та постійний контроль за оновленням та вдосконаленням механізмів захисту є не просто обов'язком держави, а й предметом державно-правового регулювання, що потрібно розглядати водночас із захистом прав та свобод людини, зокрема захистом права на повагу до приватного життя. Створення дієвої системи захисту персональних даних належить до міжнародних зобов'язань України, в т. ч. пов'язаних із європейською інтеграцією нашої держави.

Об'єкт дослідження – персональні дані.

Предмет дослідження – методи та засоби захисту персональних даних в інформаційно-комунікаційних системах.

Мета роботи – проаналізувати механізми захисту персональних даних за вимогами українського законодавства та вимогами GDPR.

Для досягнення зазначеної мети визначено такі *основні завдання дослідження*:

- проаналізувати стан проблеми;
- з'ясувати, що належить до персональних даних;
- проаналізувати вимоги українського законодавства щодо захисту персональних даних;
- з'ясувати вимоги щодо оброблення та захисту персональних даних відповідно до GDPR;
- сформувати механізми захисту персональних даних.

Наукова новизна отриманих результатів дослідження – отримано подальший розвиток питання щодо захисту персональних даних в інформаційно-комунікаційних системах.

Практична значущість результатів дослідження – полягає у підвищенні ефективності використання методів захисту персональних даних у роботі суб'єктів владних повноважень.

Аналіз останніх досліджень та публікацій. Аналіз наукової літератури дає змогу стверджувати, що проблемам захисту персональних даних приділяли увагу в

наукових дослідженнях як вітчизняні, так і зарубіжні вчені. Зокрема питання міжнародної та національної інформаційної безпеки розглядали такі автори: Легка О. В. [10], Бем М. В., Данченко Т., Грозян В. [1], Блінова Г. О., Баранов О. А. [2], Вілсон С. [17], Дукато Р. [4], Mengesa F., Latzob T., Vielbertha M. [11] та ін. В усіх зазначених публікаціях розглядали захист персональних даних з юридичного погляду. Тому в цій статті ми досліджуємо питання організаційно-технічної складової захисту персональних даних.

Матеріали та методи дослідження. Дослідження спираються на аналізі відомих законодавчих нормативних актів та положень щодо правил оброблення та механізмів захисту персональних даних для українців та громадян Європейського Союзу. Інформація про механізми, які країни використовують для захисту прав та персональних даних своїх громадян, знаходиться у відкритому доступі в мережі Інтернет. На основі всієї інформації, зібраної з різноманітних офіційних джерел, дослідили, проаналізували та з'ясували основні технології, якими користуються країни, щоб вберегти особисту інформацію від дій зловмисника.

Результати дослідження та їх обговорення

Відповідно до Закону України, персональні дані (далі – ПД) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [18]. Це будь-яка інформація, що відноситься до ідентифікованої фізичної особи, за якою прямо або опосередковано можна її визначити. Ці дані окремо або в сукупності дають змогу володільцеві цих даних чітко ідентифікувати конкретну особу.

Відповідно до ДСТУ 3389-96, до персональних даних належать [15]:

- ідентифікаційні дані (ім'я, адреса, телефон тощо);
- паспортні дані;
- особисті відомості (вік, стать, сімейний стан тощо);
- склад сім'ї;
- освіта;
- професія;
- біометричні дані (зріст, вага, особливі прикмети тощо);
- психологічні дані (особистість, характер тощо);
- житлові умови;
- спосіб життя;
- життєві інтереси та захоплення;
- споживчі звички;
- фінансова інформація;
- електронні ідентифікаційні дані (трафік, IP-адреса тощо);
- електронні дані про локалізацію (GSM, GPS тощо);
- запис зображень (фото, відео);
- звукозапис;
- інші персональні дані.

Особливі (чутливі) ПД:

- расова приналежність;
- політичні погляди;
- релігійні переконання;
- світоглядні переконання;
- членство в політичних партіях та професійних спілках;
- стан статевого життя;
- стан здоров'я.

Механізми захисту персональних даних відповідно до законодавства України. Першу згадку про ПД в українському законодавстві описано у Конституції України, а саме статтю 32 "*не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і тільки в інтересах національної безпеки, економічного добробуту та прав людини.*"

Відповідно до Закону України "Про доступ до публічної інформації" [19], інформація про особу належить до конфіденційної інформації (рис. 1).

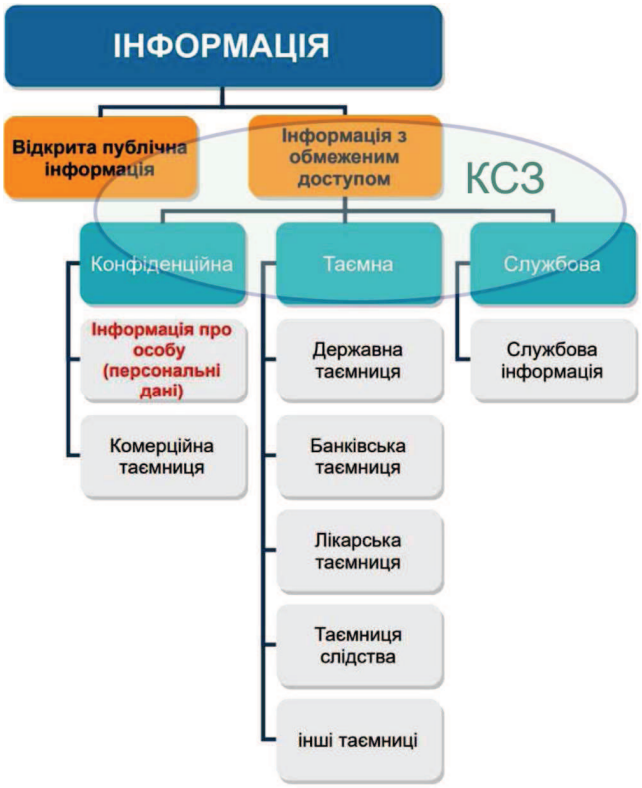

Рис. 1. Класифікація інформації відповідно до Закону України

Проаналізували ЗУ "Про захист інформації в інформаційно-телекомунікаційних системах", де написано: "*Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством*" (стаття 8) [20].

Крім цього, існує окремий закон, що стосується питання особливостей оброблення та захисту персональних даних, ЗУ "Про захист персональних даних", який набув чинності з 1 січня 2011 р. [18]. Цей Закон України встановлює відповідні вимоги до оброблення та захисту персональних даних (рис. 2).

Персональні дані повинні оброблятися з дотриманням вимог щодо захисту інформації. Інформаційна система, в якій обробляються персональні дані, має бути належно захищена (п. 7 ст. 8 Закону України "Про захист персональних даних"). У простих випадках – це забезпечення доступу до приміщень та до інформаційних систем тільки тих осіб, які мають на це право, розмежування доступу з використанням паролів, реалізація мінімальних вимог щодо реєстрації подій в інформаційній системі відповідно до встановлених на підприємстві

процедур. Для великих і малих підприємств, які ставлять за мету мінімізувати ризики, – це створення й незалежна оцінка системи управління інформаційною безпекою відповідно до міжнародних і національних стандартів, створення й оцінення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, застосування широкого переліку рекомендованих заходів [8], [12], [13], [19], [20].

Рис. 2. Вимоги до оброблення персональних даних

Оброблення баз персональних даних в електронній формі здійснюється за допомогою автоматизованих систем, до яких належать локальні або корпоративні комп'ютерні мережі, сервери баз даних тощо. Власник бази персональних даних обробляє дані в складі інформаційної (автоматизованої) системи, у якій забезпечується захист цих даних відповідно до вимог закону, за допомогою комплексної системи захисту інформації (КСЗІ) [19], [20], [8], [12], [13].

Порядок захисту персональних даних у складі інформаційної (автоматизованої) системи, що визначений нормативно-правовими актами України, передбачає такі заходи [13]:

- створення служби захисту інформації в автоматизованій системі (АС) чи інформаційно-телекомунікаційній системі (ІТС) або призначення посадової особи, що виконує ці функції;
- укладання угоди про створення комплексної системи захисту інформації (КСЗІ) з організацією – виконавцем робіт;
- обстеження АС та розроблення Плану захисту інформації в АС;
- формування вимог до КСЗІ та розроблення технічного завдання для створення КСЗІ в АС;
- розроблення та впровадження КСЗІ в АС згідно з НД ТЗІ 3.7-003-05;
- подання заявки в Держспецзв'язку України на проведення державної експертизи КСЗІ;
- проведення державної експертизи організатором експертизи та складання експертного висновку;
- реєстрація експертного висновку в Держспецзв'язку України та видача замовнику атестату відповідності;
- введення автоматизованої системи в експлуатацію.

Методичну допомогу під час створення систем захисту інформації надає Адміністрація Держспецзв'язку України та її регіональні органи в областях.

До слова, в Україні створили сервіс, який містить персональні дані громадян, відомий як "Дія" (рис. 3), у якому більшість українців уже зареєструвалися та надали доступ до своїх документів: паспортів, водійських прав, студентських квитків. Авжеж, це більш зручно, аніж носити з собою величезну кількість паперових документів, тому додаток "Дія" став хорошою альтернативою. Е-права та е-техпаспорт формуються автоматично за наявності в єдиній інформаційній системі МВС усіх відомостей, що зазначаються у посвідченні водія та свідоцтві про реєстрацію транспортного засобу, зокрема фотографії.

Рис. 3. Логотип сервісу "Дія"

Основні переваги цифрових документів – простота отримання, зручність використання та захищеність від підробок. Створювати додаток "Дія" допомагали 35 спеціалістів-волонтерів від найбільшої в Україні аутсорсингової IT-компанії EPAM Systems. Вони приділили особливу увагу захисту персональних даних. Додаток "Дія" можна безкоштовно завантажити у App Store та Play Market. Ідентифікація користувачів відбувається за допомогою технології BankID [3] (рис. 4) через систему Національного банку та Приватбанку.

Авторизація здійснюється через BankID, застосунок побудовано відповідно до кращих практик індустрії, усі дані передаються та зберігаються на смартфоні користувача виключно у зашифрованому вигляді, посилено процедуру автентифікації між додатком та сервером. Варто зазначити про міри покарання [9], [16] у випадках порушення законодавства щодо ПД (табл. 1).

В Україні захищати персональну інформацію покликані кіберполіція та уповноважений Верховної Ради з прав людини. Саме він може скласти адміністративний протокол у разі порушення права людини на захист персональних даних якоюсь установою чи органом. Кіберполіція займається вже кримінальними правопорушеннями [16].

***Механізм захисту за* GDPR.** На території Європейського Союзу діє єдиний державний апарат захисту персональних даних. Починаючи з 25 травня 2018 р., в юридичному полі Європейського Союзу набув чинності нормативний акт Загальний Регламент Захисту Даних, більш відомий як GDPR (англ. *General Data Protection Regulation*) [6]. Євросоюз перейшов на нові правила поводження з персональними даними, а Регламент стосується будь-якої роботи з персональними даними, зокрема збирання, зберігання, передачі. Вимоги надто широкі й покривають усі особливості – від управління до зобов'язань за контрактом.

GDPR захищає конфіденційність таких даних:

- основна інформація про особу, така як: ім'я, адреса та ідентифікаційні номери;
- веб-дані, такі як місцезнаходження, IP-адреса, дані cookie та теги RFID;
- дані про здоров'я та генетичні та біометричні дані;
- расові чи етнічні дані, а також політичні думки.

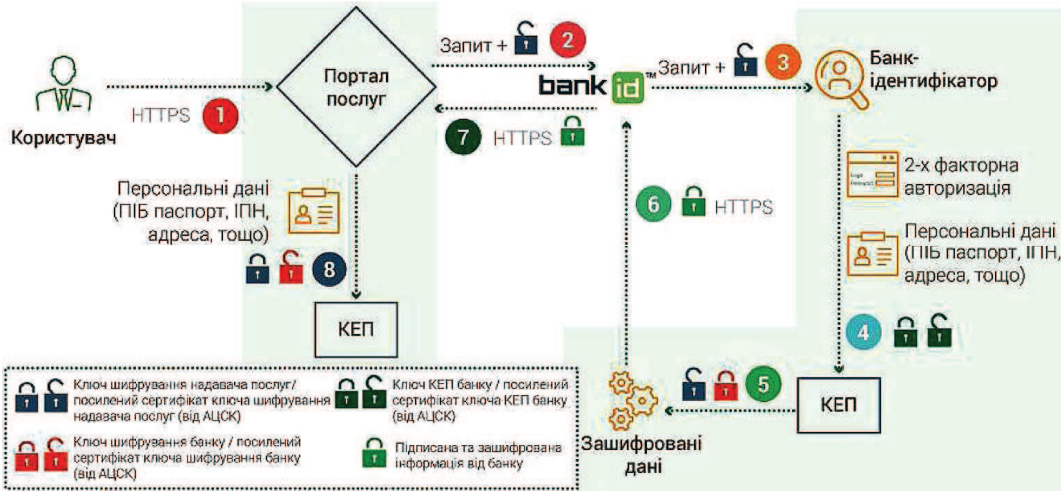

Рис. 4. Схема роботи BankID

Табл. 1. Порушення щодо персональних даних та міри покарання

Норма		Порушення	Покарання / штраф:
Кодекс України про адміністративні правопорушення	Стаття 188-39	Неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про права з огляду на виключення його персональних даних до бази персональних даних, про мету збирання цих даних і осіб, яким ці дані передаються	– на громадян у розмірі 3400-5100 грн; – на посадових осіб, громадян-підприємців 5100-6800 грн.
		Неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних.	– на громадян у розмірі 1700-3400 грн; – на посадових осіб, громадян-підприємців 3400-6800 грн.
		Повторне протягом року здійснення аналогічного порушення особою, що вже притягалася до адміністративної відповідальності	– на громадян у розмірі 5100-8500 грн; – на посадових осіб, громадян-підприємців 6800-11900 грн.
		Ухилення від державної реєстрації бази персональних даних	– на громадян у розмірі 5100-8500 грн; – на посадових осіб, громадян-підприємців 8500-17000 грн.
		Недотримання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них.	у розмірі 5100-17000 грн.
	Стаття 188-40	Невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу з питань захисту персональних даних щодо усунення порушень законодавства про захист персональних даних	на посадових осіб, громадян і суб'єктів підприємницької діяльності – 1700-3400 грн.
Кримінальний кодекс України	Стаття 182	Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями ККУ	8500-17000 грн., або виправні роботи на термін до 2 років, або арешт на термін до 6 місяців, або обмеження волі на термін до 3 років
		Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи.	Арешт на термін від 3 до 6 місяців або обмеження волі на термін від 3 до 5 років, або позбавлення волі на той самий термін.

Відповідно до статті 32 GDPR, у якій інформується про вимоги безпечного оброблення даних (рис. 4). Щоразу під час оцінювання відповідного рівня захисту варто враховувати ризики, які спричиняє оброблення, зокрема випадкове або незаконне знищення, втрата, зміна, несанкціоноване розкриття або доступ до персональних даних [6], [7], [14].

Псевдонімізація – це процедура управління даними та деідентифікація, за допомогою якої інформаційні поля, що ідентифікують особу, у записі даних замінюються одним або кількома штучними ідентифікаторами або псевдонімами [7].

Один псевдонім для кожного заміненого поля або колекції замінених полів робить запис даних менш ідентифікованим, залишаючись придатним для аналізу та оброблення даних.

Зазвичай псевдонімізацію використовують експерти з безпеки або державні службовці для приховування інформації, що ідентифікує особу, з метою збереження структури даних та конфіденційності інформації.

Технічні засоби реалізації дотримання норм GDPR мають певний набір рішень, які може реалізовувати компанія Gemalto [14], всесвітньо відомий лідер щодо рішень з інформаційної безпеки. Вона пропонує єдине повне портфоліо продуктів для захисту даних, що працюють спільно для забезпечення стійкого захисту й управління конфіденційними даними, та відповідають нормам GDPR.

GDPR вказує на шифрування, як на основну вимогу безпеки даних. Окрім цього, організаціям потрібно оцінити ризики, а потім вжити заходів, що пом'якшують ризики, які вони виявлять. Оскільки жодна організація не може повністю визначити або передбачити всі ризики для своїх даних, і жоден підхід до периметра безпеки не є надійним, організації повинні шифрувати свої дані, щоб забезпечити відповідність до GDPR. За допо-

могою шифрування, неважливо чи є порушення, дані будуть належно захищені.

Рис. 4. Вимоги до оброблення персональних даних за GDPR

Ядром системи для захисту даних є програмно-апаратний комплекс Keysecure, що призначений для створення, зберігання та управління життєвим циклом криптографічних ключів для шифрування даних. Навколо Keysecure, залежно від типу даних, що мають захищатися, архітектури системи зберігання даних та сервісів, що беруть участь в обробленні, можна застосувати такі програмні продукти Gemalto:

- ProtectV – для шифрування дисків віртуальних машин VMWare, AWS, Azure;
- ProtectDB – для шифрування баз даних Oracle, MS SQL, IBM DB2, Teradata;
- ProtectFile – для вибіркового шифрування папок та файлів на робочих станціях користувачів та файлових серверах Windows або Linux.

Gemalto пропонує широкий вибір продуктів для забезпечення надійної автентифікації користувачів, що складається з автентифікаторів на основі особистого сертифікату користувача (eToken 5110, Smartcard MD Prime), генераторів одноразових паролів (eToken 3000, Mobile PASS), систем для управління процесами автентифікації (SAC, SAM, SAS, Network Logon).

Окрім технічних рішень, важливим питанням є організаційні заходи безпеки, до них належать: навчання персоналу, додавання політики конфіденційності, правильна організація процесів, надання доступу до персональних даних тільки уповноваженим працівникам.

Варто зазначити про міри покарання у випадках недотримання вимог GDPR (табл. 2). Порядок накладення адміністративних штрафних санкцій та їхній розмір передбачено у статті 83 GDPR – "General conditions for imposing administrative fines". У таблиці наведено розміри штрафів, а також критерії, за якими їх визначають.

Табл. 2. Порушення щодо персональних даних та міри покарання за GDPR

Стаття	Порушення	Покарання
GDPR стаття 83 частина 4	– невиконання контролером та обробником персональних даних обов'язків, передбачених статтями 8, 11, 25-39, 42 та 43 GDPR; – неналежне виконання обов'язків щодо сертифікації механізму захисту даних (здебільшого не стосується бізнесу, особливо малого та середнього), а також обов'язків, передбачених частиною 4 статті 41	штраф у розмірі до 10000000 Євро або до 2 % загального світового обороту за рік (застосовується варіант з вищим розміром штрафу)
GDPR стаття 83 частина 5	– порушення основних принципів оброблення персональних даних, включаючи положення Регламенту про порядок надання/отримання згоди суб'єкта (користувача) на обробку персональних даних (положення статей 5, 6, 7 та 9 GDPR); – порушення прав суб'єкта персональних даних, встановлених приписами статті 12 та статті 22 General Data Protection Regulation (у статті 22 йдеться про недопустимість отримання згоди й оброблення особистих даних виключно в автоматизованому режимі з формальним отриманням згоди (наприклад, проставленням (наданням) такої згоди за користувача, без свідомого вибору останнього); – недотримання правил передачі персональних даних до структурних підрозділів компанії або її контрагентів у третіх країнах (статті 44-49 GDPR); – невиконання обов'язків, передбачених законодавством країн-членів ЄС, яке прийняте на виконання положень розділу IX General Data Protection Regulation; – невиконання рішень та вказівок компетентних органів нагляду, прийнятих на підставі приписів частин 1 та 2 статті 58 Регламенту, щодо обмеження на обробку персональних даних або призупинення такої обробки.	штраф до 20000000 Євро або 4 % від світового обороту компанії-порушника за фінансовий рік (стягується штраф з більшим розміром)

Обговорення результатів дослідження. Здійснений аналіз методів захисту персональних даних у рамках законодавства України та Європейського Союзу дав змогу чітко окреслити необхідні дії щодо впровадження розглянутих методів в інформаційно-комунікаційних системах. На сьогодні існує достатньо наукових праць за темою захисту персональних даних, проте вони здебільшого зосередженні на юридичну складову цього питання. Ми у своїй роботі показуємо саме організаційно-технічну складову захисту персональних даних.

Наступним перспективним напрямом дослідження є шляхи підвищення рівня обізнаності громадян та імплементації організаційно-технічного рішення захисту персональних даних.

Висновок

Внаслідок аналізу вимог та механізмів захисту персональних даних, можна чітко заявити, що на сьогодні створено документи на законодавчому рівні, що регламентують правила використання та вимоги до оброблення персональних даних, особливості забезпечення захисту персональних даних та відповідальних сторін.

З'ясували, що обробляти персональні дані потрібно тільки у системах із встановленою комплексною систе-

мою захисту інформації. Розглянули штрафні санкції за порушення та недотримання законів щодо захисту персональних даних в Україні та країнах ЄС. Проте, яка б технічно складна не була система захисту, завжди залишається один нюанс, – людський фактор. Тому вважаємо, що важливим питанням у процесі захисту персональних даних є інформування та навчання громадян базовим правам, що дало б змогу підвищити їхній рівень обізнаності й цим самим не стати жертвою кібершахраїв.

References

[1] Baranov, O. A., & Bryzhko, V. M. (2016). Protection of personal data in the field of the Internet of Things. *Information and Law*, 2, 85–91. http://nbuv.gov.ua/UJRN/Infpr_2016_2_11

[2] Bem, M. V., Gorodisky, I. M., Sutton, G., & Rodionenko, O. M. (2020). Protection of personal data: legal regulation and practical aspects. Kyiv: KIS, Published by the Council of Europe. F-67075 Strasbourg Cedex.

[3] Bezpeka. (2021). Bezpeka ta Zakhyst Informatsii v Systemi BankID NBU. Ofitsiinyi sait natsionalnoho banku Ukrainy. Retrieved from: https://bank.gov.ua/ua/bank-id-nbu/security-data. [In Ukrainian].

[4] Ducato, Rossana. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review, 37*. https://doi.org/10.1016/j.clsr.2020.105412

[5] GDPR. (2021). General Data Protection Regulation. Retrieved from: https://www6.thalesgroup.com/compliance

[6] GDPR. (2021). Ofitsiine Vydannia. Retrieved from: https://gdpr-info.eu/chapter-4. [In Ukrainian].

[7] GDPR. (2021). Pseudonymization according to the GDPR. Retrieved from: https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr

[8] Kabinetu. (2021). Postanova Kabinetu Ministriv Ukrainy Vid 29.03.2006, № 373 "Pro Zatverdzhennia Pravyl Zabezpechennia Zakhystu Informatsii V Informatsiinykh Telekomunikatsiinykh Ta Informatsiino-Telekomunikatsiinykh Systemakh". Retrieved from: https://www.kmu.gov.ua/npas/32791685. [In Ukrainian].

[9] Kodeks. (2021). Kodeks Ukrainy Pro Administratyvni Pravoporushennia. Retrieved from: https://zakon.rada.gov.ua/laws/show/80731-10#Text. [In Ukrainian].

[10] Lehka, O. V. (2021). Actual issues of personal data protection: domestic and international experience. *Legal position, 2*(31), 74–79, https://doi.org/10.32836/2521-6473.2021-2.15

[11] Mengesa, F., Latzob, T., Vielbertha, M., Sobolad, S., Pöhlsc, H., Taubmannc, B., ..., Pernula, G. (2021). Towards GDPR-compliant data processing in modern SIEM systems. *Computers & Security, 103*. https://doi.org/10.1016/j.cose.2020.102165

[12] Nakaz. (2021). Nakaz Ministerstva Yustytsii Ukrainy Vid 30.12.2011. № 3659/5 "Pro Zatverdzhennia Typovoho Poriadku Obrobky Personalnykh Danykh U Bazakh Personalnykh Danykh". Retrieved from: https://zakon.rada.gov.ua/laws/show/z0001-12#Text. [In Ukrainian].

[13] ND TZI 3.7-003-05. (2005) Poriadok provedennia robit iz stvorennia kompleksnoi systemy zakhystu informatsii v informatsiino-telekomunikatsiinii systemi. Retrieved from: https://tzi.com.ua/downloads/3.7-003-2005.pdf. [In Ukrainian].

[14] Salashnik, R. O., & Shabatura, M. M. (2021). Requirements for personal data protection under the rules of GDPR. *Proceedings the XVI International Conference Problems and prospects for the development of life safety system*, 259–261.

[15] Verkhovna Rada Ukrainy. (1996). DSTU 3389-96 "Kartky Identyfikatsiini. Identyfikatsiina Kartka Osoby – Nosii Biometrychnoi Informatsii". Retrieved from: https://zakon.rada.gov.ua/rada/show/v0487609-08#Text. [In Ukrainian].

[16] Verkhovna Rada Ukrainy. (2021). Kryminalnyi Kodeks Ukrainy. Retrieved from: https://zakon.rada.gov.ua/laws/show/2341-14#Text. [In Ukrainian].

[17] Wilson, Simon. (2018). A framework for security technology cohesion in the era of the GDPR. *Computer Fraud & Security, 2018*(12), 8–11 https://doi.org/10.1016/S1361-3723(18)30119-2

[18] Zakon Ukrainy. (2017). Verkhovna Rada Ukrainy. Zakon Ukrainy "Pro zahyst personalnych danych". Retrieved from: https://zakon.rada.gov.ua/laws/show/2297-17#Text. [In Ukrainian].

[19] Zakon Ukrainy. (2017). Verkhovna Rada Ukrainy. Zakon Ukrainy "Pro Dostup Do Publichnoi Informatsii". Retrieved from: https://zakon.rada.gov.ua/laws/show/2939-17#Text. [In Ukrainian].

[20] Zakon Ukrainy. (2021). Verkhovna Rada Ukrainy. Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh". Retrieved from: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text. [In Ukrainian].

M. M. Shabatura, R. O. Salashnyk

Lviv Polytechnic National University, Lviv, Ukraine

ANALYSIS OF PERSONAL DATA PROTECTION METHODS ACCORDING TO UKRAINIAN LEGISLATION AND THE GDPR

The problem of modern technologies rapid development is shown and characterized, which makes the issues of Internet users personal data protection very urgent. The current state of personal data protection in accordance with the requirements of Ukrainian legislation and the General Data Protection Regulation (GDPR) is analyzed. It is also determined which data belong to personal data and why they are subject to protection. According to Ukrainian Laws "On Access to Public Information", "On Personal Data Protection " and "About information protection in information and telecommunication systems" it was found the methods of personal data protection, peculiarities of processing information, storage, and transfer. Personal data is a kind of restricted access information so should be processed only in systems that have a comprehensive information security system possessing a certificate of conformity. Ukraine was one of the first countries, which introduce an electronic passport, so we considered the "DIIA" application. This application contains a huge database of personal data, that is why we investigate it and many interesting facts about the development are presented. The Code of Ukraine on Administrative Offenses and the Criminal Code of Ukraine for violation of requirements and non-compliance with the law on personal data protection in Ukraine are analyzed, penalties are also described. The requirements for personal data protection according to the European standard GDPR, namely, the procedure of pseudonymization, annihilation, encryption, etc. are given. A set of technical solutions and cybersecurity tools for implementing compliance with the GDPR standards is considered. In addition to technical solutions, important issues are security organization measures, these include staff training, adding privacy policies, proper organization of processes, providing access to personal data only to authorized employees. The penalty for violating the GDPR requirements has been clarified. Every country in the world is trying to ensure the protection of the personal data of its citizens at the legislative level by creating laws, regulations, and

orders. It is emphasized, an important factor is to raise the awareness of citizens, who often ignore the problems associated with the protection of their personal data, including due to a lack of understanding of legal standards and requirements in this area.

Keywords: personal data; processing; "DIIA"; protection; GDPR.

Інформація про авторів:

Шабатура Марія Миколаївна, канд. техн. наук, доцент, кафедра безпеки інформаційних технологій.
Email: mariia.m.mandrona@lpnu.ua; https://orcid.org/0000-0003-0814-1855

Салашник Роксолана Олегівна, студентка, кафедра безпеки інформаційних технологій.
Email: roksolana.salashnyk.kb.2019@lpnu.ua

Цитування за ДСТУ: Шабатура М. М., Салашник Р. О. Аналіз методів захисту персональних даних за українським законодавством і GDPR. *Український журнал інформаційних технологій.* 2021, т. 3, № 2. С. 51–57.

Citation APA: Shabatura, M. M., & Salashnyk, R. O. (2021). Analysis of personal data protection methods according to ukrainian legislation and the GDPR. *Ukrainian Journal of Information Technology, 3*(2), 51–57. https://doi.org/10.23939/ujit2021.02.051