# ДЕМОГРАФІЯ, ЕКОНОМІКА ПРАЦІ, СОЦІАЛЬНА ЕКОНОМІКА І ПОЛІТИКА

DOI: https://doi.org/10.32836/2521-666X/2020-67-19
УДК 303.446.33:004

**Шандрівська О.Є.**
кандидат економічних наук, доцент,
Національний університет «Львівська політехніка»
**Шандрівський А.Г.**
кандидат фізико-математичних наук, доцент,
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

**Shandrivska Olena**
Lviv Polytechnic National University
**Shandrivskyy Andrii**
Hetman Petro Sahaidachny National Army Academy

## КОМПАРАТИВНИЙ АНАЛІЗ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ: ПРОБЛЕМАТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

## COMPARATIVE ANALYSIS OF INFORMATION AND COMMUNICATION TECHNOLOGY DEVELOPMENT: PROBLEMS OF PERSONAL DATA PROTECTION

*Досліджено проблеми захисту персональних даних у контексті розвитку інформаційно-комунікаційних технологій. Проведено компаративний аналіз статистичних даних, що за змістом ідентифікують динаміку розвитку середовища формування та обробки баз персональних даних на прикладі низки країн (Індексу поширення Інтернету; Індексу національної кібербезпеки, рівнів цифрового розвитку, поширення Інтернету та використання Facebook, Індексу захисту інтелектуальної власності). На прикладі України проведено оцінювання впливу чинників на сегмент персональних даних у частині забезпечення його безпеки, ідентифікованих показниками: домашні абоненти мережі Інтернет, економічно активне населення, наявний дохід у розрахунку на одну особу та обліковані кіберзлочини. Наведено концептуальну схему ідентифікації безпеки персональних даних, ідентифіковано специфіку формування внутрішньої політики безпеки персональних даних та основні чинники впливу на неї, виявлено проблеми супроводу обробки персональних даних. Запропоновано заходи з нівелювання/мінімізації ризиків витоку персональних даних на рівні окремої особистості, організацій-споживачів та на рівні держави.*

**Ключові слова:** *гібридна агресія, великі дані, проникнення Інтернету, цифровий розвиток, безпека персональних даних, обліковані кіберзлочини.*

*Исследованы проблемы защиты персональных данных в контексте развития информационно-коммуникационных технологий. Проведен компаративный анализ статистических данных, которые по содержанию идентифицируют динамику развития среды формирования и обработки баз персональных данных на примере ряда стран (Индекса распространения Интернета; Индекса национальной кибербезопасности, уровней цифрового развития, распространения Интернета и использования Facebook, Индекса защиты интеллектуальной собственности). На примере Украины проведена оценка влияния факторов на сегмент персональных данных в контексте обеспечения его безопасности, идентифицированных показателями: домашние абоненты сети Интернет, экономически активное население, располагаемый доход в расчете на одного человека и учтенные киберпреступления. Приведена концептуальная схема идентификации безопасности персональных данных, определена специфика формирования внутренней политики безопасности персональных данных и основные факторы влияния на нее, выявлены проблемы сопровождения обработки персональных данных. Предложены меры по нивелированию/минимизации рисков утечки персональных данных на уровне отдельной личности, организаций-потребителей и на уровне государства.*

**Ключевые слова:** *гибридная агрессия, большие данные, проникновение Интернета, цифровое развитие, безопасность персональных данных, учтенные киберпреступления.*

*Active implementation of information and telecommunication technologies in public life has significantly expanded the collection and application of personal data. In connection with the intensification of the formation of automated personal data bases, which is accompanied by a poorly formalized institutional environment for their formation and insufficient control of their further usage by individuals and regulatory authorities, the problem of ensuring the security of personal data has become aggravated. It creates the need to formalize the market of personal data in the context of ensuring the security of the individual, the state and society as a whole. The digitalization of all spheres of public life simplifies the communication and the way of performing transactions for individuals. This allows, for the purposes of comparative analysis, to study the segment of personal data of different countries from the perspective*

*of analyzing the dynamics of such indicators as the Internet User Coverage Rate, due to personal data leaks - trends in the spread of cyber crime, the National Cybersecurity Index and the level of digital development, statistics on the spread of the Internet and the use of Facebook, the Intellectual Property Protection Index, etc., which are analyzed in the work. The authors of the study classified the number of recorded cybercrimes, the number of Internet home subscribers, the level of the economically active population, disposable income per capita as the indicators of the identification and research of the personal data security sector in Ukraine. Based on the analysis of their dynamics, a linear econometric multifactor model for assessing the security of personal data is formed. The personal data segment which should be considered as a component of the information market and cyberspace, information security as a component of the national security of Ukraine, the Internet economy, etc., requires the formation of a conceptual scheme for identifying the security of personal data and the development of an effective mechanism for protecting personal data in the context of identifying the participation of an individual in public and social relations.*

**Keywords: hybrid** *aggression, Big Data, Internet penetration, Digital Development, security of personal data, recorded cyber crime.*

**Постановка проблеми.** Тенденції глобалізації та інформатизації українського суспільства, розвиток індустрії споживчого Інтернету речей (яка, за оцінками Gartner, у 2020 р. зросте до 14 млрд. пристроїв) спричинили суттєве зростання обсягів, методів передачі та напрямів застосування персональних даних у різних сферах суспільного життя [1]. Створення баз даних громадян та відкритий доступ до них, автоматизовані обробка та поширення інформації про осіб без їхнього відома призвели до загострення проблематики інформаційної безпеки особистості, особливо її інформаційного та інформаційно-психологічного складників, громадянського суспільства та держави загалом у сфері захисту персональних даних. Для України, де законодавство щодо володіння та використання персональних даних споживачів є недосконалим, а способи захисту недостатньо захищеними, ця проблема є особливо актуальною.

**Аналіз останніх досліджень і публікацій.** З активним розвитком інформаційно-телекомунікаційних систем і технологій в Україні, за якого інформація набула функцій товару і розглядається як потужний ресурс розвитку, виникла проблема захисту персональних даних. Наприклад, проблематику захисту персональних даних ілюструють такі дані: два мільярди записів даних були скомпрометовані в 2017 р., у першій половині 2018 р. було порушено понад 4,5 млрд. записів [15].

Випереджальні темпи розвитку інформаційно-комунікаційних технологій відносно нормативно-правових актів, які регулюють відносини у цій сфері, транскордонний характер поширення кіберзлочинності, відкритий доступ та публічність великих масивів даних, складнощі ідентифікації суб'єкта злочинної діяльності та доведення його вини ускладнюють нейтралізацію проблематики захисту персональних даних.

У науковій літературі під персональними даними розглядається сукупність відомостей, які дають змогу ідентифікувати фізичну особу. Сучасні системи персональних загальних даних можуть містити прізвище, дату народження, прописку, електронну пошту тощо та особливі дані (членство у політичних партіях/організаціях, медичних, біометричних даних та ін.), які знаходяться не в «даркнеті» (сайти, доступ до яких можна отримати через спеціальне програмне забезпечення, налаштування, авторизацію, де використовують нестандартні, а тому «проблемні» для блокування правоохоронними органами протоколи, такі як Tor, I2P, Freenet тощо), а у відкритому доступі. Це створює широке поле для маніпуляцій, махінацій та інших протиправних дій на всіх стадіях обробки персональних даних: реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення (розповсюдження, реалізації, передачі), знеособлення, знищення тощо.

Положення щодо захисту персональних даних громадян піднімали такі вітчизняні вчені, як А. Анісимова, В. Дзюндзюк, В. Ліпкана, А. Чернобай, В. Гавловський, О. Дмитренко, А. Минькова, О. Оніщенко, В. Брижко, В. Бобрик, В. Степанов та ін. Проблематику персональних даних досліджували також зарубіжні вчені, такі як К. Бенеменченконетт, Д. Гейнзберг, С. Дейвіс, Дж. Фастер, Р. Кларк, В. Котші, М. Кьорбі, В. Лонг, Дж. Ван ден Ховен, К. Беннетт та ін.

Окремі аспекти захисту інформації з обмеженим доступом, насамперед персональних даних, без дослідження проблеми організації захисту інфраструктури від кібернетичних загроз на прикладі Німеччини наведено у праці О. Матяша [5, с. 238–340]. Проте системне бачення захисту персональних даних у контексті упорядкування суспільних інформаційних відносин в умовах множинних, непередбачуваних та хаотичних інформаційних загроз вимагає подальшого дослідження та обґрунтування.

**Мета статті** полягає у дослідженні проблем захисту персональних даних у сфері обробки даних, кібербезпеки та електронних комунікацій для таких основних сегментів, як населення, державні служби, муніципалітети та бізнес, із метою пошуку ефективних шляхів захисту та запровадження превентивних заходів щодо протиправного використання персональних даних, розроблення механізмів формування, використання, регулювання та доступу до персональних даних.

Об'єкт дослідження – персональні дані громадян.

Предмет дослідження – захист від несанкціонованого використання персональних даних.

**Виклад основного матеріалу.** Стрімке поширення інформаційно-комунікаційних технологій уважається базовим ризикоутворюючим чинником у галузі безпеки персональних даних, концептуальну схему якої наведено на рис. 1.

Концептуальна схема ідентифікації безпеки персональних даних представляє такі напрями та складники аналізу, як: інформаційне середовище, яке розглядається як елемент безпекового середовища держави, суб'єкти відносин ринку персональних даних, пов'язані

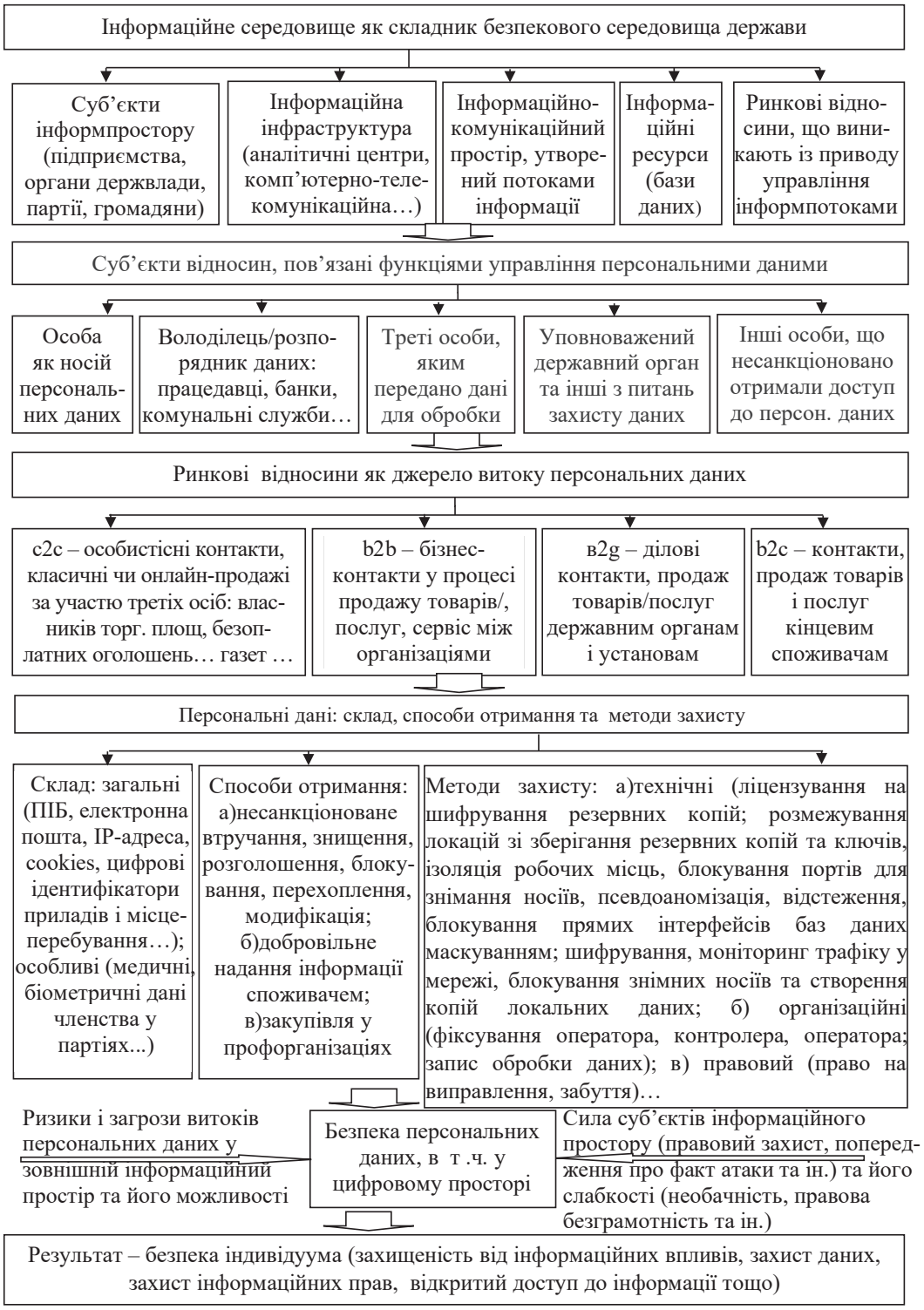


**Рис. 1. Концептуальна схема ідентифікації безпеки персональних даних**

*Джерело: власна розробка*

функціями управління персональними даними; ринкові відносини як джерело витоку персональних даних; ідентифікація складників захисту персональних даних, у зв'язку з чим до розгляду взято проблему безпеки персональних даних, яка піддається впливу ризиків і загроз зовнішнього інформаційного простору, а завдяки поєднанню загроз, вразливостей та наслідків їх прояву уможливлює проведення оцінки ідентифікованих ризиків; результат роботи системи із забезпечення безпеки персональних даних.

Спрощення комунікацій та процесів проведення трансакцій стимулює кінцевих споживачів активно долучатися до користування мережею Інтернет та ставати постійними споживачами Інтернет-послуг у світі.

Розвинуті ринки Північної Америки та Європи, галузь телекомунікацій яких знаходиться на стадії зрілості життєвого циклу, характеризуються найвищими показниками проникнення Інтернету у суспільне життя, за ними слідують інші регіони світу, що знаходяться на стадії розвитку, про що свідчить Індекс поширення Інтернету (табл. 1).

Зокрема, найбільший Індекс поширення Інтернету виявлено в Європі та Північній Америці – відповідно 87,7% та 89,4% (за даними першого півріччя 2019 р.), де були здійснені основні кібератаки та які пов'язані з найбільшою кількістю інцидентів щодо витоку персональних даних. Це засвідчує, що розвиток економіки та цифровізація усіх сфер суспільного життя поряд із визнаними позитивними зрушеннями відкриває можливості для поширення кіберзлочинності, у тому числі щодо витоку баз персональних даних громадян. До прикладу, у 2019 р. головними тенденціями у сфері поширення кібезлочинності стали [15]:

• розширені комплекти фішингу, сайтам яких притаманний короткий термін перебування у мережі (до п'яти годин), що знижує рівень довіри (65%) до усіх URL-адрес;

• атаки віддаленого доступу, націлені на смартфони, камери з Інтернет-протоколом (IP), комп'ютери чи пристрої мережевого зберігання (NAS), які завдяки відкритим портам мають змогу пересилати дані у зовнішні мережі чи Інтернет;

• атаки на мобільні додатки, налаштовані у смартфонах споживачів. Значний обсяг даних у смартфоні та двофакторна аутентифікація на ньому розглядаються як потенційне джерело витоків інформації у разі його втрати. Співвідношення рівня кібербезпеки та цифрового розвитку низки країн у цілях компаративного аналізу наведено в табл. 2.

Як видно з табл. 2, Індекс національної кібербезпеки перевищує рівень цифрового розвитку у Франції, Польщі, Грузії та Україні на 4,06, 3,54, 5,28 та 5,54 пункти відповідно, що свідчить про випереджальні темпи розвитку галузі інформаційної безпеки відносно *процесів цифровізації* економіки у цих країнах. Щодо України та Грузії, то слід зазначити, що основним чинником формування такого співвідношення є вимушена захисна політика цих країн у відповідь на тривалу гібридну неоголошену агресію з боку РФ, у тому числі у кіберпросторі. Натомість у Німеччині, США та РФ рівень цифрового розвитку є вищим за Індекс національної кібербезпеки на 1,43, 3,11 та 2,55 пункти відповідно, що засвідчує тенденцію про те, що темпи розвитку цифровізації економіки є вищими за систему заходів щодо запобігання реалізації кіберзлочинності у цих країнах. Індекс національної кібербезпеки та рівень цифрового розвитку в Україні є нижчими за всі аналізовані країни, у т.ч. РФ. Статистику поширення Інтернету та використання соціальних мереж наведено в табл. 3.

Як свідчить табл. 3, поширення Інтернету у Німеччині є найбільшим – 96%, Україна знаходиться на другому місці – 93,4%, за нею слідують Франція, РФ, Польща, Грузія та США – 92,3%, 80,9%, 78,2%, 68,1% та 77,2% відповідно. Натомість серед споживачів, які користуються Інтернетом, найбільше відвідують Facebook у США (82,4%) та Грузії (79%), близько половини відвідувачів припадає на Францію (54,6%) та Польщу (47,1%), близько третини – на Німеччину (39,2%).

Таблиця 1

**Індекс поширення Інтернету за регіонами світу, перше півріччя 2019 р.**

| Країна/ регіон | Кількість населення, млн осіб | Користувачі Інтернету, млн осіб | Індекс поширення Інтернету, % | Темп зростання користувачів Інтернету (2019/2000 рр.), % |
|---|---|---|---|---|
| Північна Америка | 366,50 | 327,57 | 89,4 | 203 |
| Європа | 829,17 | 727,56 | 87,7 | 592 |
| Латинська Америка/ Карибський регіон | 658,35 | 453,70 | 68,9 | 2,411 |
| Австралія/ Океанія | 41,84 | 28,64 | 68,4 | 276 |
| Середня Азія | 258,36 | 175,50 | 67,9 | 5243 |
| Азія | 4241,98 | 2300,47 | 54,2 | 1,913 |
| Африка | 1320,04 | 522,81 | 39,6 | 11481 |
| Світ | 7716,22 | 4536,25 | 58,8 | 1,157 |

*Джерело: складено за [11]*

Таблиця 2

**Розвиток галузі кібербезпеки та цифрового розвитку деяких країн**

| Ранг | Країна | Індекс національної кібербезпеки | Рівень цифрового розвитку | Відхилення |
|---|---|---|---|---|
| 6 | Франція | 83,12 | 79,06 | 4,06 |
| 10 | Німеччина | 80,52 | 81,95 | -1,43 |
| 13 | США | 79,22 | 82,33 | -3,11 |
| 21 | Польща | 70,13 | 66,59 | 3,54 |
| 23 | Грузія | 64,94 | 59,66 | 5,28 |
| 25 | Росія | 64,94 | 67,49 | -2,55 |
| 28 | Україна | 63,64 | 58,10 | 5,54 |

*Джерело: вибрано з [11; 13]*

Таблиця 3

**Статистика поширення Інтернету та використання Facebook у досліджуваних країнах, 2019 р.**

| Країна | Поширення Інтернету, % | Користувачі Інтернету, тис осіб | Facebook, тис ос.іб | Поширення Facebook серед користувачів Інтернету, % |
|---|---|---|---|---|
| Німеччина | 96,0 | 79127,6 | 31000 | 39,2 |
| Україна | 93,4 | 40912,4 | 9500 | 23,2 |
| Франція | 92,3 | 60421,7 | 33000 | 54,6 |
| РФ | 80,9 | 116353,9 | 13100 | 11,3 |
| Польща | 78,2 | 29757,1 | 14000 | 47,1 |
| США | 77,2 | 783909,3 | 645661,2 | 82,4 |
| Грузія | 68,1 | 2658,3 | 2100 | 79,0 |

*Джерело: сформовано на основі [11]*

Найменший показник поширення Facebook серед користувачів України та РФ (23,2% та 11,3% відповідно).

У 2015 р. IT компанія Gartner заявила, що всі дані сьогодні є великими. Ці дані можуть спростити маніпуляції з особистостями як споживачами товарів, так і з громадянами України як об'єктами інформаційного впливу. З одного боку, комплекс інформації спрощує вплив на політичні погляди та переконання особи, з іншого – робить надлегким продаж йому пропонованих товарів. Проте обсяг зібраної інформації про споживача та механізми подальшої її обробки залишаються для останнього поза контролем. Наприклад, розширення додатків Google, надсилаючи лише запит на обробку даних, мають змогу отримувати скріншоти робочого столу, записи аудіо з мікрофону та збирати дані з локальної файлової системи, що є прямим порушенням прав споживача на конфіденційність [12].

Важливим для аналізу проблематики персональних даних є аналіз Індексу захисту інтелектуальної власності, який опосередковано вказує на рівень захисту персональних даних (табл. 4).

У 2019 р., за даними ЄС, Україна, РФ, Індія, Індонезія, Туреччина віднесені до країн другого пріоритету з числа третіх країн, які порушують права інтелектуальної власності та завдають шкоди економічним інтересам ЄС. До основних положень в Україні віднесено проблеми щодо законодавчого захисту інтелектуального права, механізмів реєстрації торговельних марок, транзиту контрафактної та піратської продукції на ринки ЄС. В Україні аналіз Індексу захисту прав інтелектуальної власності, проведений у 2014–2019 рр., указав на спадну тенденцію даного показника (з 5,65 до 4,578 бали) на противагу іншим досліджуваним країнам (РФ, Польщі, Німеччині, США, Франції), які демонструють позитивну тенденцію щодо значень індексу. РФ, яка у 2014–2017 рр. демонструвала нижчий за Україну рейтинг, у 2018–2019 рр. випередила Україну з діапазоном значень Індексу (5,216–5,391 бали). Польща демонструє вищі за РФ показники Індексу: у 2014–2019 рр. вони становлять 5,967–6,121 бали. Трійка лідерів – Франція, Німеччина та США зі значеннями індексів у 2019 рр. 7,929, 8,292 та 8,78 бали відповідно. Структурний аналіз Індексу (2019 р.) аналізованих країн указав, що Україна серед них займає найнижчу позицію в галузі захисту інтелектуальної власності, що опосередковано вказує на комплементарний розвиток проблем захисту персональних даних у ній. Індекс захисту прав інтелектуальної власності вказує також на стан піратства в Інтернеті в Україні. Так, на сайтах із піратським контентом, наприклад, можна знайти бази даних із персональною інформацією українських громадян: військових, держслужбовців тощо. У контексті зазначеного важливою є боротьба з кіберзлочинністю у частині досягнення безпеки персональних даних, тенденції розвитку якої ілюструють дані табл. 5.

Проведений компаративний аналіз статистичних даних у досліджуваних країнах (співвідношень темпів поширення цифровізації та політики кіберзахисту, користування найбільшою соціальною мережею Facebook та захисту прав інтелектуальної власності), які за своїм змістом ідентифікують динаміку розвитку середовища формування та обробки баз персональних даних, виявив недостатню державну підтримку у частині забезпечення кібернетичної безпеки. У контексті зазначеного перспективним напрямом залучення держави до питань забезпечення кібернетичної безпеки має стати формування Державної програми забезпечення безпеки персональних даних, у складі якої, серед

Таблиця 4

**Динаміка Індексу «Захист прав інтелектуальної власності», бали**

| Індекс | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|
| США | 8,333 | 8,436 | 8,632 | 8,715 | 8,7 | 8,78 |
| Німеччина | 8,133 | 8,094 | 8,23 | 8,376 | 8,343 | 8,292 |
| Франція | 7,8 | 7,802 | 7,897 | 8,092 | 7,824 | 7,929 |
| Польща | 5,967 | 5,826 | 5,94 | 6,114 | 6,088 | 6,121 |
| Росія | 4,767 | 4,841 | 4,841 | 4,943 | 5,216 | 5,391 |
| Україна | 5,65 | 4,07 | 4,32 | 4,419 | 4,436 | 4,578 |

*Джерело: сформовано на основі [14]*

Таблиця 5

**Показники ідентифікації сектору персональних даних в Україні**

| Рік | Обліковані кіберзлочини, од. (y) | Домашні абоненти мережі Інтернет, тис ($x_1$) | Економічно активне населення, тис осіб ($x_2$) | Наявний дохід у розрахунку на одну особу, грн ($x_3$) |
|---|---|---|---|---|
| 2005 | 39 | 266,775 | 20481,7 | 6332 |
| 2006 | 100 | 430,65 | 20545,9 | 7771 |
| 2007 | 145 | 997,2 | 20606,2 | 10126,0 |
| 2008 | 156 | 1532,2 | 20675,7 | 13716,3 |
| 2009 | 217 | 2214,6 | 20321,6 | 14372,8 |
| 2010 | 190 | 3661,2 | 20220,7 | 18485,6 |
| 2011 | 131 | 3821,4 | 20247,9 | 21637,9 |
| 2012 | 138 | 4671,7 | 20393,5 | 25206,4 |
| 2013 | 595 | 5478,3 | 20478,2 | 26719,4 |
| 2014 | 443 | 5432,6 | 19035,2 | 26782,1 |
| 2015 | 598 | 5625,1 | 17396,0 | 31803,1 |
| 2016 | 865 | 15493,1 | 17303,6 | 37079,9 |
| 2017 | 2573 | 20619,0 | 17193,2 | 47269,7 |
| 2018 | 2688 | 23354,2 | 17296,2 | 58442 |
| 2019 | 4263 | 25683,8 | 17323,7 | 67208,3 |
| 2019/ 2005 | 109,31 | 96,28 | 0,85 | 10,61 |

*Джерело: складено за [2, с. 65; 3, с. 71; 4, с. 8; 7-9]*

іншого, мають міститися положення щодо принципів, цілей розвитку та політики супроводу; організаційного забезпечення, навичок, компетенцій та кваліфікації персоналу, навчання та розвитку; програмного забезпечення тощо.

Аналіз проблематики дослідження на прикладі України дав змогу виявити специфіку формування внутрішньої політики безпеки персональних даних та основні чинники впливу на неї, серед яких слід відзначити такі, як:

• специфіка діяльності володільця/розпорядника персональних даних. Володільцем даних є юридичні чи фізичні особи, які формують бази даних, розпорядником є особи, які обробляють дані від імені володільця;

• мета обробки даних, їх обсяг, структура (наприклад, у разі звернення користувачів до серверів здійснюється обробка даних під час заповнення реєстраційних форм, у процесі користування сервісами, файлів cookie, ір-адрес, параметрів та налаштувань Інтернет-браузерів (User-agen); категорії даних (соціальних верств: громадян похилого віку, інвалідів, хворих та ін.);

• інформаційно-комунікаційні технології, задіяні у процесі обробки персональних даних; ступінь їх захищеності;

• акредитовані категорії та чисельність осіб із доступом до персональних даних; політика навчання у галузі гарантування безпеки даних;

• форми ведення реєстру з обробки персональних даних (паперова, електронна або змішана);

• ризики, які можуть виникнути під час обробки даних: інформаційні, технічні, персонофіковані тощо;

• відповідальність на всіх етапах обробки персональних даних.

Аналіз практики застосування згоди на обробку персональних даних засвідчив виникнення таких проблем їх супроводу [4-6; 10].

1. Положення щодо надання згоди на обробку даних (яка може бути отримана способами: у письмовому, електронному чи усному вигляді; з оповіщенням за замовчуванням особи) передбачають лише повну згоду особи без узгодження терміну дії згоди, часто є непропорційними меті обробки даних, не заперечують передачу даних на аутсорсинг, сприяють утворенню чисельних каналів формування баз даних та неможливості відслідковування осередків їх виникнення.

2. Час, кількість даних, які збираються, та витрати на їх обробку часто є невиправданими та не посилюють захист персональних даних.

3. Відсутність критеріїв пропорційності між змістом згоди на обробку даних та метою їх обробки, недостатній рівень ідентифікації напрямів подальшого використання даних, не визначено відповідальність, стандарти доведення вини та методика визначення завданої шкоди у разі витоку незаконного використання інформації.

Із метою оцінювання впливу показників, які ідентифікують сектор персональних даних в Україні, до розгляду було вибрано: обліковані кіберзлочини (представлено як залежну ознаку y, од.), що являє собою ідентифікатор безпеки персональних даних громадян та впливу на нього таких показників, як домашні абоненти мережі Інтернет (представлено як незалежну ознаку $x_1$, тис), економічно активне населення (ознака $x_2$, тис осіб) та наявний дохід у розрахунку на одну особу (ознака $x_3$, грн) (табл. 5).

Незалежні ознаки були перевірені на мультиколінеарність, тобто відсутність лінійної залежності між собою за $\chi^2$ – критерієм, який визначається так:

$$\chi_p^2 = -(n-1-\frac{2m+5}{6}) * \ln(\det R), \qquad (1)$$

де n – кількість вибіркових значень, m – кількість незалежних змінних, det R – визначник матриці R.

$\chi^2_р$ = 50,637. Кореляційну матрицю С з визначником det R = 0,0016, наведено в табл. 6.

Таблиця 6

**Кореляційна матриця**

| | | | |
|---|---|---|---|
| С= | 1,000 | -0,860 | 0,968 |
| | -0,860 | 1,000 | -0,858 |
| | 0,968 | -0,858 | 1,000 |

Знаходимо табличне значення $\chi^2_{кр}$ за ймовірністю 0,95, обсягом вибірки n = 15 та ступенем вільності k =3: $\chi^2_{кр}$ = 7,26. Оскільки розраховане значення більше за табличне ($\chi^2_р > \chi^2_{кр}$), тобто 50,637>7,26, то з ймовірністю 0,95 можна стверджувати, що між трьома незалежними змінними існує мультиколінеарність. Зменшуючи кількість чинників впливу до двох ($x_1$, $x_2$) на залежну ознаку у, $\chi^2_р$ = 16,737 за $\chi^2_{кр}$ = 3,8 (за ступеня вільності к = 1, р = 0,95, m = 2), тобто ознаки $x_1$ та $x_2$ є взаємозалежні. Водночас за виведення з розгляду ознаки $x_3$ застосована функція LINEST, що дало змогу отримати такі параметри для оцінювання рівняння регресії (табл. 7).

Таблиця 7

**Результати застосування функції LINEST**

| | | |
|---|---|---|
| 0,169 | 0,161 | -3675,606 |
| 0,148 | 0,026 | 3043,905 |
| 0,902 | 428,052 | - |
| 54,959 | 12 | - |
| 20140085,16 | 2198743,777 | - |

Згідно з табл. 7, коефіцієнт детермінації становить 0,902, що засвідчує тісний зв'язок між факторними та результуючою ознаками. Критерій Фішера, що становить F = 54,96 >$F_{кр}$ ($F_{кр}$ = 3,26, $к_1$ = m-1 = 1; $к_2$ = n-m-1 = 12), вказує на адекватність моделі та свідчить про зв'язок між змінними для всієї генеральної сукупності даних. Здійснимо перевірку отриманих коефіцієнтів моделі на статистичну значимість для оцінювання показника облікованих кіберзлочинів, од. (у). Значення t-статистики для ступеня к = 11 рівне t = 2,179 (ймовірність р = 0,95). Оцінки стандартної помилки для коефіцієнтів рівні: $S_0$ = 3043,905; $S_1$ = 0,026; $S_2$ = 0,148. Відповідно, за формулою: $t_i = a_i/S_i$, де i = 1,3; $a_i$ – коефіцієнти багатофакторної моделі, $t_0$ = –1,208; $t_1$ = 6,298; $t_2$ =1,141, За модулем усі параметри t-статистики менші за табличне значення (крім $t_1$). Приймаємо рішення про подальше дослідження залежності y= f ($x_1$).

Оцінювання впливу між змінними у та $x_1$ дало змогу встановити таке: рівняння регресії виду: $y = 4E\text{-}10x^3 – 9E\text{-}06x^2 + 0{,}1041x + 16{,}509$; $R^2 = 0{,}9741$ – зв'язок щільний між факторною та результуючою ознаками; F = 488,9305>$F_{кр}$ ($F_{кр}$ = 4,67, $к_1$ = m = 1; $к_2$ = n-m-1 = 13) – модель адекватна, існує тісний зв'язок між змінними для всієї генеральної сукупності даних, що дає змогу використати модель для прогнозування показника облікованих кіберзлочинів. $У_{прогн.}$ = 6461,056 (за заданого значення $x_1$ = 30928,36).

Слід зауважити, що в подальшому слід зосередитися на пошуку більшої кількості незалежних факторних ознак впливу на результуючу ознаку У для підвищення точності розрахунків.

**Висновки.** Україна як держава з низьким рівнем захисту персональних даних не спроможна повною мірою здійснити ефективну інформаційну захищеність громадян від витоків конфіденційної інформації, яка циркулює в суспільному інформаційному просторі. За умов слабо інституційованих засад формування політики збору персональних даних обсяги збирання конфіденційної інформації не відповідають меті дослідження і часто перевищують мінімально необхідний обсяг збирання інформації про особу, норма про яку має бути превентивно встановлена за замовчуванням.

За умов низької поінформованості споживачів про наслідки витоку конфіденційної інформації у відкритий доступ та ігнорування відповідальності, покладеної на володільців баз персональних даних, витоки інформації несуть загрози не тільки окремим особистостям чи окремим сегментам споживачів, а й національній безпеці України.

Нівелювання чи мінімізація ризиків витоку персональних даних можливі завдяки вдосконаленню нормативно-правового та організаційного забезпечення та приведення його у відповідність до міжнародних стандартів ISO, зокрема GDPR, у т.ч. в контексті формування дієвої системи контролю та суб'єктами інформаційного простору в частині управління інформаційними ресурсами на всіх стадіях їх обробки. Чинником, що ускладнює процес уніфікування захисту персональної інформації про фізичних осіб є необхідність збирання близько 40 видів документів, аби працювати відповідно до положень GDPR.

На рівні громадськості необхідним є посилення культурно-просвітницької діяльності та підвищення поінформованості споживачів щодо правил комунікацій у частині формування безпеки поведінки та відповідального поводження у соціальних мережах, правил захисту персональних даних. Для громадян серед превентивних заходів із формування безпеки даних доцільно запропонувати здійснювати реєстрацію номерів на власне ім'я, відокремлення фінансового номеру від номера для щоденного користування, підключення на пошті та в додатках, де є така опція, двофакторної аутентифікації, вимог у оператора мереж заміни SIM-карти за вимогою паспорту, активації заборони на віддалену заміну карти.

На рівні організацій-споживачів підвищення безпеки персональних даних повинно стосуватися програмно-технічних та організаційно-економічних методів убезпечення циркулювання інформації з акцентом на превентивні заходи виявлення/нівелювання/захисту інформації від витоків.

На рівні держави формування політики забезпечення кібернетичної безпеки в частині форм убезпечення персональних даних має стосуватися розроблення відповідних нормативно-правових актів щодо

формування державно-приватного партнерства у цій галузі, міжгалузевого партнерства на базі їх компаративного розвитку, стратегічного партнерства неурядових організацій та впровадження форм міжнародного співробітництва з НАТО та ЄС, методів: запровадження ефективної системи стандартизації та сертифікації, методичних засад незалежного аудиту, поглиблення участі держави у формування безпечного національного кіберпростору, що мають стати предметом подальших досліджень авторів.

**Список літератури:**

1. Гнатюк С.Л. Кібербезпека в умовах розгортання Четвертої промислової революції (Industry 4.0): виклики та можливості для України. *НІСД.* URL : https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi (дата звернення: 03.01.2020).

2. Звіт про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, за 2018 рік. Київ, 2019. 72 с. URL : https://nkrzi.gov.ua/images/upload/142/8484/Zvit_za_2018_29032019_new.pdf (дата звернення: 03.01.2020).

3. Звіт про роботу НКРЗІ за 2016 рік. Київ, 2017. 102 с. URL : https://nkrzi.gov.ua/images/upload/142/6852/Zvit_NCCIR_2016.pdf. (дата звернення: 03.01.2020).

4. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України.* 2018. № 2(19). С. 155–166. URL : http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y (дата звернення: 03.01.2020).

5. Матяш О.І. Забезпечення безпеки інформації в Німеччині. *Актуальні проблеми управління інформаційною безпекою держави* : збір. матер. наук.-практ. конф., м. Київ, 22 березня 2011 р. Київ. : Наук.-вид. відділ НА СБ України, 2011. Ч. 1. С. 238–240.

6. Проблеми захисту персональних даних. URL : http://kmp.ua/uk/analytics/infoletters/personal-data-protection-issues-according-to-laws-of-ukraine/ (дата звернення: 6.08.2019).

7. Проникнення Інтернету в Україні зупинилося на рівні близько 65%. *РБК-Україна.* URL : https://www.rbc.ua/ukr/news/proniknovenie-interneta-ukraine-ostanovilos-1542366021.html (дата звернення: 02.02.2020).

8. Річний звіт про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, за 2013 рік. Київ, 2014. 82 с. URL : https://nkrzi.gov.ua/images/upload/142/4422/-1d8e4b19ebef49ac3f56eceb2579fa27.pdf (дата звернення: 03.01.2020).

9. Сайт Державної служби статистики України. URL : http://ukrstat.gov.ua (дата звернення: 03.01.2020).

10. *Шадська У.* ТОП-10 питань у сфері захисту персональних даних. URL : https://www.prostir.ua/?library=top-10-pytan-u-sferi-zahystu-personalnyh-danyh (дата звернення: 03.01.2020).

11. Internet World Stats. URL : internetworldstats.com (дата звернення: 03.02.2020).

12. Стець О. Google заборонив додаткам збирати персональні дані користувачів. URL : https://www.poglyad.tv/google-zaboronyv-dodatkam-zbyraty-personalni-dani-korystuvachiv/ (дата звернення: 03.01.2020).

13. NCSI. URL : https://ncsi.ega.ee/ncsi-index/ (дата звернення: 03.01.2020).

14. Reports. International Property Rights Index 2019. URL : https://internationalpropertyrightsindex.org/compare/country?id (дата звернення: 03.01.2020).

15. Von Gravrock, Ein. Here are the biggest cybercrime trends of 2019. URL : https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/ (дата звернення: 03.01.2020).

**References:**

1. Hnatiuk S. L. (2019) Kiberbezpeka v umovakh rozghortannia chetvertoi promyslovoi revoliutsii (industry 4.0): vyklyky ta mozhlyvosti dlia Ukrainy. [Cyber Security in the Deployment of the Fourth Industrial Revolution (Industry 4.0): Challenges and Opportunities for Ukraine]. NISD. Available at: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi (accessed 03.01.2020).

2. Zvit pro robotu Natsionalnoi komisii, shcho zdiisniuie derzhavne rehuliuvannia u sferi zviazku ta informatyzatsii za 2018 rik (2019) [Report on the work of the National Commission for State Regulation in the Field of Communication and Informatization for 2018]. Kyiv. Available at: https://nkrzi.gov.ua/images/upload/142/8484/ Zvit_za_2018_29032019_new.pdf. (accessed 03.01.2020).

3. Zvit pro robotu NKRZI za 2016 rik (2017) [Report on the work of the NCCIR for 2016]. Kyiv. Available at: https://nkrzi.gov.ua/images/upload/142/6852/Zvit_NCCIR_2016.pdf. (accessed 03.01.2020).

4. Kravtsova M. O. (2018) Suchasnyi stan i napriamy protydii kiberzlochynnosti v Ukraini [The current state and trends of combating cybercrime in Ukraine]. *Visnyk Kryminolohichnoi Asotsiatsii Ukrainy* (electronic journal), 2018, no. 2(19), pp. 155-166. Available at: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y. (accessed 03.01.2020).

5. Matiash O. I. (2011) Zabezpechennia bezpeky informatsii v Nimechchyni [Information security in Germany]. Proceedings of the *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy (Ukraine, Kyiv, March22, 2011),* Ukraine: Nauk.-vyd. viddil NA SB Ukrainy, pp. 238–240.

6. Problemy zakhystu personalnykh danykh [Problems of protection of personal data]. Available at: http://kmp.ua/uk/analytics/infoletters/personal-data-protection-issues-according-to-laws-of-ukraine/ (accessed 06.08.2019).

7. Pronyknennia Internetu v Ukraini zupynylosia na rivni blyzko 65%. [Internet penetration in Ukraine has stopped at around 65%]. Available at: https://www.rbc.ua/ukr/news/proniknovenie-interneta-ukraine-ostanovilos-1542366021.html (accessed 02.02.2020.)

8. Richnyi zvit. Pro robotu Natsionalnoi komisii, shcho zdiisniuie derzhavne rehuliuvannia u sferi zviazku ta informatyzatsii za 2013 rik [Annual report. About the work of the National Commission for the State Regulation of Communications and Informatization for 2013]. Kyiv. Available at: https://nkrzi.gov.ua/images/upload/142/4422/1d8e4b19ebef49ac3f56eceb2579fa27.pdf. (accessed 03.01.2020).

9. Sait Derzhavnoi sluzhby statystyky Ukrainy [State Statistics Service website]. Available at: http://ukrstat.gov.ua. (accessed 03.01.2020).

10. Shadska U. (2019) TOP-10 pytan u sferi zakhystu personalnykh danykh [Top 10 issues in the area of personal data protection]. Available at: https://www.prostir.ua/?library=top-10-pytan-u-sferi-zahystu-personalnyh-danyh (accessed 03.01.2020).

11. Internet World Stats. Available at: internetworldstats.com (accessed 03.02.2020).

12. Stets O. (2019) Google zaboronyv dodatkam zbyraty personalni dani korystuvachiv [Google has prohibited applications from collecting user personal information]. Available at: https://www.poglyad.tv/google-zaboronyv-dodatkam-zbyraty-personalni-dani-korystuvachiv/ (accessed 03.01.2020).

13. NCSI. Available at: https://ncsi.ega.ee/ncsi-index/ (accessed 03.01.2020).

14. Reports. International Property Rights Index 2019. Available at: https://internationalpropertyrightsindex.org/compare/country?id (accessed 03.01.2020).

15. Von Gravrock, Ein. Here are the biggest cybercrime trends of 2019. Available at: https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/ (accessed 03.01.2020).