Полторан Д.В.
здобувач вищої освіти
Таврійський державний агротехнологічний університет
імені Дмитра Моторного
Науковий керівник: д.т.н., доцент Мірошниченко М.Ю.

ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ ЯК НЕОБХІДНІСТЬ СУЧАСНОГО СУСПІЛЬСТВА

Анотація. *У статті розглядається проблема захисту персональної інформації як одна з потреб сучасного суспільства. Визначено сутність персональних даних та їх значення в умовах розвитку цифрових технологій, проаналізовано основні ризики й загрози, пов'язані з витоком та незаконним використанням інформації. Окреслено міжнародні та національні підходи до правового регулювання у сфері захисту персональних даних, приділено увагу технічним і освітнім аспектам інформаційної безпеки. Особливий акцент зроблено на викликах, що постають перед Україною в умовах цифровізації та воєнного стану. У висновках підкреслено необхідність комплексного підходу, який поєднує правові, технологічні та культурно-освітні механізми захисту.*

Ключові слова: *персональні дані, інформаційна безпека, цифровізація, захист інформації, кіберзагрози, приватність, національна безпека.*

Poltoran D.V. Protection of personal information as a need of modern society. *The article examines the issue of protecting personal information as one of the key needs of modern society. The essence of personal data and its significance in the context of digital technology development are defined; the main risks and threats associated with data leaks and unauthorized use of information are analyzed. International and national approaches to legal regulation in the field of personal data protection are outlined, with attention given to technical and educational aspects of information security. Particular emphasis is placed on the challenges faced by Ukraine in the context of digitalization and martial law. The conclusions highlight the necessity of a comprehensive approach that combines legal, technological, and cultural-educational mechanisms of protection.*

Key words: *personal data, information security, digitalization, data protection, cyber threats, privacy, national security.*

Актуальність дослідження. У XXI столітті цифрові технології стали невід'ємною складовою суспільного розвитку. Інформаційно-комунікаційні системи, соціальні мережі, електронна комерція, дистанційна освіта та державні електронні послуги значно спростили життя людей. Водночас, зазначені переваги створили нові загрози, пов'язані з витоком, незаконним використанням персональної інформації, маніпулювання суспільною думкою тощо.

Сьогодні інформація перетворилася на стратегічний ресурс, а доступ до персональних відомостей – на потужний інструмент впливу. Використання великих масивів даних (Big Data) для маркетингових чи політичних цілей, поширення кіберзлочинності, шкідливих програм, фішингових атак та підроблених акаунтів у соціальних мережах підвищують рівень уразливості особистості. Проблема захисту персональної інформації особливо актуальна в умовах гібридних воєн, коли інформаційні технології використовуються як зброя [2, с. 121].

Україна, що активно розвиває цифрову державу та впроваджує європейські стандарти електронного врядування, стикається з подвійним викликом: необхідністю створення зручних електронних сервісів та одночасним забезпеченням надійного захисту персональних даних громадян. Саме тому дослідження питань інформаційної безпеки є надзвичайно важливим як у науковому, так і у практичному вимірі.

Метою статті є аналіз проблеми захисту персональної інформації в умовах сучасного суспільства, визначення основних загроз та викликів у цій сфері, а також окреслення шляхів удосконалення системи інформаційної безпеки з урахуванням світових і національних тенденцій.

Виклад основного матеріалу. У сучасних умовах поняття персональної інформації набуло більш широкого змісту. До традиційних паспортних даних, адреси проживання чи ідентифікаційних кодів додаються електронні відомості, що створюють так званий «цифровий слід» людини. Це історія пошукових запитів, активність у соціальних мережах, дані про пересування, електронні платежі, навіть уподобання та стиль комунікації. Сукупність такої інформації формує «цифровий портрет» особистості, який у багатьох випадках виявляється цінішим за традиційні анкетні дані [7, с. 344].

Проблема полягає в тому, що персональні дані дедалі частіше стають об'єктом несанкціонованого доступу. Витоки інформації з державних реєстрів, банківських систем, освітніх платформ чи медичних закладів свідчать про те, що навіть найважливіші інституції не завжди здатні забезпечити належний рівень захисту. Кібератаки, фішингові схеми, використання соціальної інженерії демонструють, що зловмисники постійно вдосконалюють інструменти впливу, тоді як користувачі часто нехтують елементарними правилами безпеки, створюючи простір для злочинних дій.

Не менш небезпечною є ситуація, коли самі громадяни свідомо або несвідомо розкривають інформацію про себе у публічному просторі. Сучасна людина звикла ділитися фото, геолокацією, особистими переживаннями у відкритих соціальних мережах, що суттєво підвищує ризики маніпуляцій чи навіть фізичних загроз. Таким чином, проблема захисту даних має не лише технічний чи правовий вимір, але й культурно-освітній, адже від рівня цифрової грамотності населення безпосередньо залежить безпека особистості [5, с. 106].

На міжнародному рівні сформувалися різні моделі правового регулювання захисту персональної інформації. Найбільш відомим є європейський підхід, закріплений у Загальному регламенті із захисту даних (GDPR). Він базується на пріоритеті прав людини та передбачає суворі вимоги до обробки інформації, зокрема необхідність чіткого інформування користувача та отримання його згоди на використання даних. У США більш поширеною є галузева модель регулювання, яка охоплює окремі сфери, наприклад, банківську чи медичну.

Україна у цій сфері робить активні кроки, зокрема через Закон «Про захист персональних даних» та низку підзаконних актів. Водночас на практиці ще зберігаються значні проблеми: недостатній рівень контролю за дотриманням вимог, слабкі механізми відповідальності за порушення, а також відставання від європейських стандартів. З огляду на курс України на інтеграцію до ЄС, гармонізація національного законодавства з положеннями GDPR є важливим завданням.

Окремої уваги заслуговує технічний аспект захисту персональної інформації. Використання багаторівневої автентифікації, шифрування, резервного копіювання, систем антивірусного захисту та сучасних протоколів передачі даних є необхідними складовими інформаційної безпеки. Проте навіть найсучасніші технології залишаються

малоефективними без належного рівня відповідальності користувачів та організацій, які оперують персональними даними [8, с. 26]. Звідси випливає важливість комплексного підходу, що поєднує правові, технічні та освітні заходи.

У перспективі розвиток штучного інтелекту та аналітичних систем дозволить ефективно виявляти аномальну активність та потенційні кіберзагрози у режимі реального часу. Водночас це породжує нові етичні виклики, адже автоматизовані системи також працюють із персональною інформацією і здатні впливати на права людини [6, с. 626]. Отже, майбутнє захисту персональних даних потребує балансу між технологічними можливостями, законодавчими гарантіями та етичними стандартами.

Особливе значення питання захисту персональної інформації набуває в умовах постійної загрози з боку кіберзлочинців. Витік даних у таких обставинах може становити не лише приватну загрозу окремій людині, а й безпосередню небезпеку для національної безпеки, оскільки інформація про місце проживання, переміщення громадян, їхні соціальні зв'язки чи фінансову активність може бути використана для цілеспрямованих атак, диверсій чи кампаній із дезінформації. Інформаційна війна стала одним із ключових інструментів гібридної агресії, а персональні дані нерідко перетворюються на «зброю», що дозволяє маніпулювати суспільною думкою, підривати довіру до державних інституцій і посилювати панічні настрої серед населення [4, с. 301].

У цьому контексті захист державних інформаційних ресурсів, зокрема офіційних реєстрів та баз даних, виступає важливим стратегічним пріоритетом. Доступ до таких ресурсів відкриває можливості для масштабних кібератак, які здатні паралізувати діяльність органів влади, порушити роботу критичної інфраструктури тощо. Як наслідок, безпека державних інформаційних систем повинна реалізуватися через застосування новітніх технологій шифрування, багаторівневу систем автентифікації, постійний моніторинг кіберзагроз і тісну співпрацю з міжнародними партнерами у сфері кібероборони [3, с. 192].

Водночас важливо враховувати людський чинник, адже багато витоків даних відбуваються не лише через технічні вразливості, а й через необережність чи недобросовісність співробітників, які працюють з

інформаційними системами. Тому підвищення рівня цифрової культури та професійної підготовки працівників, а також створення умов для їхньої відповідальності за порушення правил роботи з даними є необхідним завданням на будь-якому підприємстві [1, с. 80]. Ефективна система безпеки даних здатна не лише мінімізувати загрози для окремих громадян, а й посилити здатність підприємства протистояти інформаційним атакам та забезпечити безперервність функціонування критичних сервісів.

Висновки. Захист персональної інформації є однією з важливих потреб сучасного суспільства. Він виступає не лише гарантією приватності окремої людини, але й умовою формування довіри громадян до держави, стабільності економічних процесів та безпеки держави в цілому. Аналіз показує, що головними викликами залишаються стрімкий розвиток технологій, зростання масштабів кіберзлочинності, недостатня цифрова грамотність населення та недосконаліть національного законодавства.

Для подолання цих проблем необхідно забезпечити інтеграцію правових, технічних та освітніх заходів, розвивати міжнародну співпрацю, гармонізувати національні норми із європейськими стандартами та підвищувати рівень культури безпечного користування цифровими технологіями. Лише комплексний підхід дозволить ефективно захистити особу і суспільство від небезпек, які пов’язані з неправомірним використанням персональної інформації.

Література

1. Колмакова В.О., Шаров С.В. Використання МВОК для формування імунітету від інформаційних загроз. *Українські студії в європейському контексті.* 2023. № 6. С. 80–87.
2. Мірошниченко М.Ю. До проблеми захисту інформаційних систем. *Сучасний стан та перспективи розвитку електротехнічних систем: матеріали IV Всеукр. наук.-практ. інтернет-конференції пам’яті В.В. Овчарова* (04-18 листопада 2021 р., м. Мелітополь). 2021. С. 120–122.
3. Мірошниченко М.Ю. Алгоритм захисту персональних даних в соціальних мережах. *Українські студії в європейському контексті*. 2024. № 9. С. 190–195.
4. Назаров Є.М. Захист на рівні додатків: сучасні виклики та технології. *Українські студії в європейському контексті*. 2023. №7. С. 300–307.

5. Пилипчук В.Г. Проблеми захисту приватності, індивідуальних свобод та безпеки людини в інформаційному суспільстві. *Науковий часопис Національного педагогічного університету імені М.П. Драгоманова*. 2017. Серія 18. С. 106–118.
6. Правдюк А.Л. Захист персональних даних в контексті інформаційної безпеки. *Наукові інновації та передові технології*. 2024. № 5(33). С. 625–638.
7. Сергієнко Т.І. Роль інформаційних технологій у житті сучасної людини. *Українські студії в європейському контексті*. 2023. №7. С. 344–349.
8. Sharov S., Rassokha I. Specific features of using Web 2.0 technology in the educational process. *Вісник Черкаського національного університету імені Богдана Хмельницького. Серія: Педагогічні науки*. 2022. № 3. С. 26–33.

Рябець С.І.
кандидат технічних наук,
доцент кафедри інформатики, програмування,
штучного інтелекту та технологічної освіти
Центральноукраїнський державний університет
імені Володимира Винниченка
Кирпа К.О.
майстер виробничого навчання,
ДЗП (ПТ)О «Кропивницький професійний
ліцей сфери послуг і торгівлі»

ТЕХНІЧНІ ЗАСОБИ СТВОРЕННЯ І ДРУКУ ЗОБРАЖЕНЬ В СИСТЕМІ АВТОМАТИЗОВАНОГО ПРОЄКТУВАННЯ: ІСТОРИЧНИЙ ТА ПЕРСПЕКТИВНИЙ АКЦЕНТИ

Анотація. *Периферійне обладнання виступає невід'ємною складовою частиною апаратно-програмного комплексу CAD-систем. Воно виконує функції введення, обробки, виведення та фізичного відтворення проєктних рішень, сприяючи точному позиціюванню геометричних об'єктів, створенню креслень, тривимірному моделюванню, скануванню та друку цифрових моделей. Еволюція таких пристроїв є паралельною до розвитку програмного забезпечення САПР і*