ISSN 3041-1238 № 6 (6) 2024

DOI: https://doi.org/10.26642/sas-2024-6(6)-76-82 | УПРАВЛІННЯ НАЦІОНАЛЬНОЮ
УДК 351.746.1:007.004.056.5 БЕЗПЕКОЮ

Фасій Богдан
кандидат юридичних наук, доцент
Національний університет «Одеська юридична академія»
https://orcid.org/0000-0002-8715-930X

Національна безпека та захист персональних даних в епоху цифрових технологій

Анотація. У статті здійснено комплексний аналіз взаємозв'язку між захистом персональних даних і національною безпекою в умовах цифрової трансформації. Розвиток інформаційних технологій створює нові виклики, які вимагають перегляду традиційних підходів до забезпечення безпеки держави та захисту прав людини. Особлива увага приділяється питанням зарубіжного досвіду захисту персональних даних та визначенню причин недосконалого рівня захисту в Україні. Важливим аспектом є дослідження загроз, що виникають у цифровому середовищі, таких як кібершпигунство, кібератаки та масовий контроль над особистими даними, які можуть загрожувати правам людини. У статті також розглянуто юридичні, технічні та організаційні механізми захисту даних, зокрема впровадження шифрування, багатофакторної автентифікації та використання штучного інтелекту для підвищення рівня безпеки.

Провідними методами дослідження є діалектичний та системний методи, які дозволяють всебічно аналізувати взаємозв'язок між захистом персональних даних і національною безпекою в умовах цифрової трансформації. Діалектичний метод сприяє дослідженню розвитку правових норм і технологічних процесів у контексті постійно змінюваних викликів кіберпростору, зокрема через протиставлення загроз і заходів безпеки. Системний метод надає можливість оцінювати правові, технічні та організаційні питання захисту персональних даних як частини єдиного механізму національної безпеки, враховуючи правові норми, державну політику та технологічні рішення.

Теоретична цінність статті полягає в поглибленому аналізі взаємозв'язку між захистом персональних даних і національною безпекою в умовах цифрових технологій, а також у визначенні основних загроз і правових підходів для їх подолання. Практична цінність полягає у наданні конкретних пропозицій щодо впровадження сучасних технічних рішень для підвищення рівня захисту від кіберзагроз.

Ключові слова: персональні дані; національна безпека; кібербезпека; штучний інтелект; цифрові технології.

Актуальність теми. У сучасному світі національна безпека та захист персональних даних стали надзвичайно важливими аспектами суспільного життя. З розвитком цифрових технологій виникають нові виклики, які вимагають перегляду традиційних підходів щодо забезпечення безпеки держави. Кібератаки, витоки інформації та використання даних без згоди осіб стають звичайним явищем і загрожують як національним інтересам, так і правам громадян. У зв'язку з цим, розуміння співвідношення національної безпеки і захистом персональних даних є критично важливим для формування ефективних політик.

Цифровізація економічних відносин, зростання популярності соціальних мереж і використання великих даних створюють нові можливості, але одночасно й ризики для захисту приватності. Персональні дані, які раніше вважалися приватними, тепер можуть бути легко доступними для державних структур та приватних компаній. Це зумовлює необхідність вжити заходів для забезпечення безпеки даних, адже недотримання прав осіб у цій сфері може призвести до серйозних наслідків, таких як зловживання, маніпуляції та шахрайство.

Міжнародні норми та стандарти у сфері захисту персональних даних постійно змінюються, що створює додаткові виклики для державних органів. Для прикладу, законодавство ЄС, таке як GDPR, встановлює високі вимоги до обробки персональних даних, які повинні враховуватися національними урядами. Україна, яка прагне інтеграції до європейських структур, повинна адаптувати своє законодавство та практики відповідно до міжнародних стандартів, щоб забезпечити захист прав громадян.

Крім того, національна безпека в епоху цифрових технологій вимагає міжвідомчої співпраці та створення комплексних стратегій, які б поєднували в собі елементи правозахисної діяльності та забезпечення безпеки. Це означає, що державні органи повинні співпрацювати з приватним сектором, науковими установами та громадським суспільством задля розробки нових підходів для захисту даних. Залучення всіх зацікавлених сторін є необхідним для створення ефективної системи захисту, що враховує різноманітність загроз [1, с. 396].

Аналіз останніх досліджень та публікацій, на які спирається автор. Питання національної безпеки є предметом наукових досліджень таких науковців, як Р.Арзуманяна, І.Дороніна, [1], Є.Магди, М.Мальського, В.Мартинюка, В.Предборського, І.Руснака та інших. Окремі питання інформаційної безпеки висвітлені у дослідженнях А.Голобуцького, Г.Головко, С.Домбровської, О.Зозулі, В.Косевцова, Ю.Машкарова, О.Полтаракова, В.Садкового, В.Стрельцова та інших. На важливості захисту персональних даних у своїх наукових дослідженнях наголошували М.Бем, М.Блохін, О.Дяковський, І.Городиський, М.Кравчук та інші. При цьому питання співвідношення національної безпеки та захисту персональних даних залишаються малодослідженими та в умовах постійних кібератак потребують ґрунтовних наукових досліджень.

Метою статті є комплексний аналіз взаємозв'язку між національною безпекою та захистом персональних даних в умовах розвитку цифрових технологій.

Викладення основного матеріалу. У сучасному світі поняття «національної безпек» зазнає значних змін завдяки розвитку інформаційних технологій. По-перше, з поширенням інтернету та цифрових платформ національна безпека стикається з такими загрозами, як кібератаки, кібертероризм і кібершпигунство. Ці загрози можуть бути спрямовані на критичну інфраструктуру, державні установи або приватні компанії, порушуючи систему функціонування важливих об'єктів, що гарантують безпеку та стабільність держави. По-друге, цифрові технології дали змогу застосовувати інструменти гібридної війни, такі як дезінформація, пропаганда та маніпуляція громадською думкою через соціальні мережі. Це своєю чергою може загрожувати політичній стабільності, підривати довіру до державних інститутів, а також спричиняти масові соціальні конфлікти. По-третє, у цифрову епоху персональні дані стають важливим елементом національної безпеки. Збір, обробка та збереження таких даних можуть бути використані для контролю над суспільством, забезпечення правопорядку або, навпаки, для зловживань і порушення прав людини. Недостатній захист персональних даних може призвести до масових витоків інформації, що загрожує безпеці як окремих осіб, так і держави.

Тому варто зазначити, що концепція безпеки трансформується в умовах глобалізації та передбачає інтеграцію національних економік та суспільств, а також зростаючу залежність держав від цифрових систем та платформ. У зв'язку з цим, національна безпека більше не обмежується лише традиційними аспектами, такими як військова сила або територіальна цілісність; вона містить в собі захист інформаційних ресурсів, кіберінфраструктури та прав громадян. Тому на сьогоднішній день необхідно впроваджувати нові підходи до формування політики безпеки, які б враховували складність і багатогранність загроз, що виникають у цифрову епоху.

Кіберпростір як нова сфера конфліктів є специфічним середовищем, де держави, неурядові організації та приватні особи можуть активно взаємодіяти. Такий простір стає ареною не лише економічних та соціальних, але й політичних конфліктів. Сучасні держави стикаються з викликами, пов'язаними з кібератаками, які можуть мати руйнівні наслідки для критично важливих інфраструктур [2, с. 53]. Тому управління кібербезпекою набуває важливого значення у формуванні стратегій національної безпеки, оскільки неадекватна реакція на кібератаки може підривати довіру до держави та загрожувати її стабільності.

Кібертероризм і кібершпигунство у цифрову епоху стали серйозною загрозою національній безпеці, оскільки зловмисники, використовуючи технології з будь-якого місця та в будь-який час, можуть здійснювати атаки на державні структури та приватні підприємства [3, с. 51]. Це може призвести до крадіжки конфіденційної інформації, фінансових втрат та загрози фізичній безпеці громадян. У такій ситуації важливо розуміти, що традиційних методів забезпечення безпеки вже недостатньо, і необхідно впроваджувати нові механізми реагування, які б містили технологічні інновації та міжнародне співробітництво.

Однією із підступних загроз в умовах сьогодення є розповсюдження дезінформації, яка часто використовується як інструмент гібридних війн. Використання соціальних мереж та онлайн-платформ для маніпуляції громадською думкою може серйозно підривати довіру до державних інститутів і викликати соціальні заворушення. Дезінформація також може бути націлена на дестабілізацію політичної ситуації в країнах, що робить її ефективним інструментом для реалізації зовнішньополітичних амбіцій. Тому боротьба з дезінформацією вимагає комплексного підходу, що містить не лише технологічні рішення, але й освітні програми для населення.

Правові питання національної безпеки в умовах цифрових технологій створюють окрему проблему. Так законодавство, що регулює захист персональних даних, часто не встигає за швидким розвитком технологій та зростанням загроз. Сьогодні в Україні існують певні прогалини в законодавстві щодо захисту даних з урахуванням потреби у забезпеченні національної безпеки.

Захист персональних даних відіграє важливу роль у системі національної безпеки, оскільки інформація про особу є одним з найцінніших ресурсів в умовах цифровізації. Персональні дані, як визначається в законодавстві, охоплюють будь-яку інформацію, що може бути використана для ідентифікації особи, сюди належать дані про ім'я, адресу, номери телефонів, а також інформація про

фінансовий стан, здоров'я та інші чутливі відомості [4]. Важливість персональних даних зростає в умовах швидкого розвитку інформаційних технологій, оскільки вони стають основою для прийняття рішень у різних сферах, від бізнесу до державного управління. Підходи до захисту персональних даних формують базу для забезпечення довіри суспільства до державних і приватних інститутів, а також сприяють стабільності національної безпеки.

Сучасні правові межі захисту персональних даних, такі як Загальний регламент захисту даних (GDPR) [5] в Європейському Союзі та Закон України «Про захист персональних даних» [4], визначають стандарти і вимоги щодо обробки, зберігання та передачі персональних даних. Ці нормативні акти покликані не лише захистити права особи, а й підвищити рівень безпеки даних, що є критично важливим для запобігання їх несанкціонованого використання. Законодавчі ініціативи створюють правову основу для формування політик на національному рівні, забезпечуючи відповідальність за порушення норм захисту персональних даних.

Світу відомі випадки витоку персональних даних великих компаній, що завдало значних збитків майнового та немайнового характеру. Так у 2017 році через вразливість вебдодатка Apache Struts компанія Equifax допустила витік даних 148 мільйонів американців, що містять номери соціального страхування, дати народження та адреси. У 2018 році внаслідок компрометації бази бронювання Starwood у Marriott було розкрито дані майже 383 мільйонів клієнтів, зокрема паспортні дані та платіжну інформацію. У 2014 році хакери, використавши облікові записи співробітників, отримали доступ до даних 145 мільйонів користувачів eBay, в тому числі імена, адреси та зашифровані паролі. У 2016 році витік з Adult Friend Finder стосувався 412 мільйонів облікових записів, що спричинило хвилю шантажу та атак [6].

В період дії воєнного стану Україна також відчула наслідки кібератак на державні організації та підприємства. Так 14 квітня 2022 року внаслідок хакерської атаки було тимчасово зупинено роботу низки урядових сайтів, в тому числі порталу Дія. На сайті МЗС хакери трьома мовами (українською, російською та польською) повідомили про викрадення персональних даних українців і погрожували оприлюднити їх. Проте СБУ заявила, що витоку даних не сталось; атака була здійснена через злам October CMS [7]. 15 лютого 2022 року відбулась потужна DDoS-атака, яка протягом приблизно п'яти годин унеможливлювала роботу 15 банківських сайтів, державних вебресурсів у домені gov.ua, а також сайтів Міністерства оборони, Збройних сил та Міністерства з питань реінтеграції тимчасово окупованих територій. За даними Ради національної безпеки США, зазначена атака була організована Головним розвідувальним управлінням рф. Згодом 23 лютого напередодні повномасштабного вторгнення Росії в Україну було здійснено нову хвилю атак на державні та банківські ресурси, крім того на зламаних сайтах компанія ESET ідентифікувала шкідливе програмне забезпечення HermeticWiper, створене ще 28 грудня 2021 року [8]. 28 серпня 2023 року Держспецзв'язку повідомила про нову хакерську атаку на органи юстиції та нотаріату України, пов'язану з розповсюдженням шкідливих листів із AsyncRAT. Листи містять архіви, відкриття яких надає хакерам віддалений доступ до пристроїв. CERT-UA відстежує цю активність із початку 2023 року та підозрює зв'язок із угрупованням «чорних нотаріусів» UAC-0007 [9]. Аналіз випадків витоку інформації шляхом кібератак дає можливість підкреслити нагальну потребу у підвищенні технічного, правового та організаційного захисту персональних даних.

На нашу думку, захист персональних даних є багатосторонньою проблемою, що має охоплювати кілька підходів, серед яких правовий, технічний та організаційний. Правовий підхід спрямований на створення регуляторних меж, які забезпечують законність збору, обробки та зберігання даних. Такий підхід формує правові основи для захисту конфіденційності та визначає обмеження щодо доступу до персональної інформації. Для вдосконалення системи захисту персональних даних з точки зору правової позиції доречним є гармонізувати національне законодавство з положеннями GDPR, зокрема уточнити вимоги щодо обробки даних і запровадити механізми транскордонного захисту. Також доцільно розробити міжнародний договір, який би регулював обмін даними між країнами, особливо в умовах зростаючих кіберзагроз, і запровадити адміністративну та кримінальну відповідальність за недбалість у захисті персональних даних.

Технічний підхід зосереджений на впровадженні інструментів кібербезпеки, які мінімізують ризики зловживання або витоку персональних даних. Шифрування даних, багатофакторна автентифікація, використання міжмережевих екранів та інших технологічних рішень є ключовими механізмами захисту, що допомагають зберегти дані від несанкціонованого доступу.

Окрім того, організаційний підхід містить внутрішні політики та процедури управління даними в компаніях, моніторинг та регулярні аудити, а також навчання співробітників для підвищення рівня обізнаності з питань кібербезпеки. На організаційному рівні для вдосконалення системи захисту персональних даних слід створити національні кіберцентри, які здійснюватимуть моніторинг кіберзагроз, прогнозуватимуть відповідні загрози і реагуватимуть на них в реальному часі, а також необхідно забезпечити постійне навчання працівників щодо роботи із персональними даними разом із проведенням

симуляційних кібернавчань. Крім того, варто запровадити обов'язкові аудити захисту персональних даних у приватних і державних установах та обмінюватись досвідом на міжнародному рівні.

Персональні дані є стратегічним ресурсом у цифрову епоху, оскільки вони використовуються в різних аспектах життя, від комерційної діяльності до державного управління. Обробка великих обсягів даних дозволяє аналізувати поведінку користувачів, прогнозувати їхні потреби та приймати обґрунтовані рішення. Однак разом із цим виникають ризики, пов'язані з використанням та зловживанням такими даними. Визначення меж використання особистої інформації є необхідним для забезпечення прав людини та запобігання зловживанням, які можуть підривати довіру до державних установ та приватного сектору [10].

Межі використання особистої інформації визначаються як національними, так і міжнародними нормами для захисту права на приватність, серед яких:

1) законність і прозорість;
2) цільове обмеження;
3) мінімізація даних;
4) термін зберігання;
5) захист від незаконного доступу;
6) права суб'єкта даних.

Цифрові технології також створюють численні загрози для персональних даних, зокрема в умовах активного використання великих даних. Злами, витоки інформації та кіберзлочини стали звичними явищами, які ставлять під загрозу конфіденційність даних. Наприклад, випадки витоку інформації з великих компаній та державних установ демонструють, що недостатні заходи безпеки можуть призвести до серйозних наслідків як для окремих осіб, так і для держави в цілому. Окрім того, впровадження штучного інтелекту для обробки персональних даних відкриває нові горизонти для їх аналізу, але водночас постає питання про етичність і правомірність таких дій. Отже, важливо знайти баланс між сучасними технологіями та безпекою, щоб захистити права осіб у цифрову епоху.

Механізми захисту персональних даних мають базуватися на комплексному підході, який поєднує державні політики, міжнародні стандарти та технологічні засоби. Державні політики повинні відповідати найкращим практикам, прийнятим у міжнародному співтоваристві, і передбачати постійний моніторинг ситуації в сфері захисту даних. Технологічні рішення, такі як шифрування інформації, багатофакторна автентифікація та інші засоби, здатні значно підвищити рівень захисту персональних даних від зловмисних дій [11, с. 20].

У сучасному світі спостерігається зростаючий конфлікт інтересів між забезпеченням національної безпеки і захистом прав людини, зокрема прав на конфіденційність. Держави, які стикаються з численними загрозами, часто вживають заходів для контролю за персональними даними своїх громадян. Вони стосуються моніторингу, спостереження і масового збору інформації, які можуть бути виправдані з точки зору безпеки. Однак таке втручання в приватне життя може призвести до серйозних порушень прав людини, що ставить під питання законність і етичність таких дій.

Спостереження і масовий збір даних, що використовуються для забезпечення національної безпеки, можуть становити серйозну загрозу для прав людини. Технологічні досягнення, такі як розширене використання камер спостереження, системи розпізнавання обличчя й аналізу великих даних, дозволяють державам здійснювати широкий контроль за своїми громадянами. Проте такі практики можуть призвести до зловживань, а також до формування культури спостереження, де приватність особи стає лише ілюзією. Важливо забезпечити, щоб будь-які заходи безпеки, які впроваджуються державою, не порушували основних прав людини і принципів конфіденційності.

Для захисту прав людини в умовах підвищеного контролю з боку держави необхідно запроваджувати юридичні механізми, які б враховували принципи пропорційності й необхідності. Принцип пропорційності вимагає, щоб обмеження прав людини були адекватними, обґрунтованими та відповідали суті загрози. Необхідність таких обмежень повинна бути ретельно обґрунтована, а їхня реалізація не повинна перевищувати те, що необхідно для досягнення мети [12, с. 228].

У сучасному світі питання захисту персональних даних в умовах загроз національній безпеці стає все більш актуальним. Технічні рішення відіграють ключову роль у забезпеченні безпеки даних. Впровадження нових стандартів кібербезпеки має стати основою для створення ефективної системи захисту інформації. До неї належать сучасні технології, такі як блокчейн і шифрування, що забезпечують надійний захист даних від несанкціонованого доступу. Крім того, використання штучного інтелекту може суттєво підвищити рівень захисту, адже він здатний знаходити аномалії в трафіку, що свідчить про кібератаки, та автоматизувати процеси реагування на них.

Зарубіжні країни активно використовують низку сучасних методів захисту персональних даних, які варто перейняти Україні для покращення власної системи захисту в умовах цифровізації, серед них:

- *шифрування даних* є одним із найефективніших технічних методів захисту, який широко застосовується в ЄС, США та Японії. Шифрування гарантує, що дані, навіть у випадку витоку, будуть недоступними для зловмисників [13];

- *багатофакторна автентифікація (MFA*) використовується у США та Європі для захисту доступу до чутливих даних. Процес підтвердження особи здійснюється через декілька методів (пароль, SMS-код, біометрія), що значно ускладнює несанкціонований доступ до даних;

- *регулярні кібербезпекові аудити та сертифікації,* які активно застосовують Країни ЄС для підтвердження надійності інформаційних систем. Це дозволяє виявляти слабкі місця в системах захисту і своєчасно їх усувати;

- *машинне навчання та штучний інтелект для моніторингу безпеки*, які вже активно використовуються великими компаніями, такими як Google і Microsoft для виявлення потенційних загроз і аномальних дій, які можуть свідчити про злам чи інші кіберінциденти.

Навіть спираючись на позитивний ефект від перейняття міжнародного досвіду, Україна все ще не може запровадити високоефективні механізми захисту персональних даних через низку причин. Однією з основних причин є недосконаліть законодавства. В Україні діє Закон «Про захист персональних даних», проте його положення не повністю відповідають міжнародним стандартам, зокрема GDPR. Це призводить до правової невизначеності, оскільки немає чітких правил щодо застосування новітніх технологій захисту. Крім того, впровадження таких методів вимагає значних фінансових ресурсів, а бюджетні обмеження та низький рівень інвестицій у кібербезпеку уповільнюють модернізацію. Багато державних установ і підприємств не можуть дозволити собі дорогі технології захисту, такі як багатофакторна автентифікація чи штучний інтелект для моніторингу загроз. Ще одним суттєвим бар'єром є кадровий дефіцит і низький рівень кіберграмотності. В Україні не вистачає кваліфікованих фахівців у сфері кібербезпеки, що ускладнює як впровадження, так і підтримку сучасних технологій захисту даних. Недостатня кількість знань і навичок серед державних службовців і працівників бізнесу також сприяє нехтуванню базовими принципами захисту даних. Складна політична та економічна ситуація, зокрема воєнний конфлікт, ще більше загострює проблему. В умовах війни ресурси спрямовуються на безпекові потреби, тоді як питання захисту даних часто стають другорядними.

Зважаючи на природу та специфіку цифрового середовища, на нашу думку, доречним є вдосконалення механізмів міжнародної співпраці у сфері кібербезпеки та захисту персональних даних. Для покращення міжнародної співпраці у сфері кібербезпеки та захисту персональних даних доцільно запровадити кілька вдосконалених механізмів. Зокрема, створення глобальної платформи для оперативного обміну інформацією дозволить забезпечити в реальному часі обмін даними про кіберзагрози, нові вразливості та механізми реагування між державами, міжнародними організаціями та приватним сектором. Розробка уніфікованих стандартів кібербезпеки, що охоплюють шифрування, управління ризиками та захист персональних даних, сприятиме гармонізації підходів у різних країнах. Запровадження механізму міжнародної сертифікації кіберпродуктів створить умови для функціонування спільного ринку програмного забезпечення та апаратних засобів, які відповідатимуть міжнародним стандартам. Посилення партнерства між державами і приватним секторами дозволить об'єднати зусилля у захисті критичної інфраструктури, обміні інноваціями та координації у запобіганні кіберзагрозам. Своєю чергою створення міжнародного кібертрибуналу забезпечить розгляд транснаціональних кіберзлочинів і сприятиме формуванню єдиної практики застосування міжнародного права в цій сфері. Крім того, на нашу думку, важливим елементом є розвиток кібердипломатії через запровадження дипломатичних механізмів задля уникнення ескалації конфліктів у кіберпросторі разом із домовленостями про «червоні лінії». Реалізація цих заходів дозволить посилити глобальну кібербезпеку, підвищити рівень захисту персональних даних і забезпечити довіру між суб'єктами міжнародної співпраці. Міжнародна співпраця у сфері кібербезпеки та захисту персональних даних охоплює взаємодію міжнародних організацій (ООН, ITU, Рада Європи), національних урядових органів, приватного сектору, наукових установ та громадських організацій. Важливу роль відіграють технологічні компанії та CERT-центри, які аналізують загрози й розробляють інструменти захисту, а також міжнародні ініціативи. Така співпраця створює багаторівневу систему координації, спрямовану на вирішення глобальних викликів у сфері інформаційної безпеки.

Висновки та перспективи подальших досліджень. Дослідження питань захисту персональних даних в умовах забезпечення національної безпеки демонструє, що ці два аспекти не тільки тісно взаємопов'язані, але й потребують комплексного підходу для ефективного вирішення сучасних викликів. Інформаційна безпека забезпечує захист конфіденційності, цілісності та доступності даних, що є основою для охорони персональної інформації. Захист персональних даних є складовою інформаційної безпеки, оскільки їх викрадення чи несанкціоноване використання може спричинити серйозні ризики для приватності й безпеки особи. Ефективна система інформаційної безпеки мінімізує загрози кіберзлочинів, захищаючи персональні дані в цифровому середовищі.

З розвитком цифрових технологій, що супроводжуються зростанням загроз для кібербезпеки, з'являються нові ризики для приватності та безпеки особистої інформації. Ефективний захист персональних даних вимагає впровадження сучасних технологічних рішень, таких як штучний інтелект і новітні стандарти кібербезпеки, які можуть забезпечити автоматизацію і підвищити рівень виявлення загроз.

Проте технологічні рішення не можуть повність вирішити питання захисту персональних даних без відповідного юридичного регулювання. Вдосконалення національного законодавства у сфері захисту персональних даних є критично важливим для формування правової основи, яка б підтримувала технологічні заходи і забезпечувала права громадян. Зокрема, необхідно ввести чіткі норми, які б визначили механізми обробки, зберігання і передачі персональних даних, а також відповідальності за їх порушення.

Міжнародна співпраця у сфері кібербезпеки та захисту персональних даних також є невід'ємною складовою успішної стратегії. На нашу думку, спільні ініціативи, обмін досвідом і знаннями між державами можуть значно підвищити рівень захисту даних. Крім цього, взаємодія на міжнародному рівні дозволяє не лише вдосконалити технічні та юридичні аспекти, але й сприяє формуванню глобальної культури безпеки. Саме комплексний підхід забезпечить розвиток демократичного суспільства в цифрову епоху.

Список використаної літератури:

1. *Доронін І.М.* Національна безпека України в інформаційну епоху : теоретико-правове дослідження / *І.М. Доронін*. Дис. на здобуття наук. ступ. д-ра юр. наук; спеціальність 12.00.01 – теорія та історія держави і права; історія політичних і правових учень (081 – Право). – К., 2020. – 539 с. [Електронний ресурс]. – Режим доступу : https://ippi.org.ua/sites/default/files/disertaciya_doronin_0.pdf.
2. *Дубов Д.В.* Кіберпростір як новий вимір геополітичного суперництва : монографія / *Д.В. Дубов*. – Київ : НІСД, 2014. – 328 с.
3. *Діордіца І.В.* Поняття та зміст кібершпигунства / *І.В. Діордіца* // Наукові праці Національного університету «Одеська юридична академія». – Одеса : Гельветика, 2020. – Т. 26. – С. 49-55.
4. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2297-17#Text.
5. Загальний регламент про захист даних / GDPR [Електронний ресурс]. – Режим доступу : https://gdpr-text.com/uk/.
6. Страшні історії кіберсвіту: 5 найбільших витоків даних десятиліття/ ESET [Електронний ресурс]. – Режим доступу : https://www.eset.com/ua/about/newsroom/blog/data-protection/strashnyye-istorii-kibermira-5-krupneyshikh-utechek-dannykh-desyatiletiya/?srsltid=AfmBOooUEY9ppkhBTC_VWwk7cAuSenP8OIDTVHf707i4HMavF0oYdkFg.
7. Витоку даних не було: СБУ розслідує масштабну атаку хакерів на сайти уряду / Українська правда [Електронний ресурс]. – Режим доступу : https://www.pravda.com.ua/news/2022/01/14/7320365/.
8. HermeticWiper : New data-wiping malware hits Ukraine / Welivesecurity [Electronic resource]. – Access mode: https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/.
9. Нова хакерська атака на Україну: постраждали органи юстиції та нотаріусів / UANews [Електронний ресурс]. – Режим доступу : https://ua.news/ua/technologies/novaya-hakerskaya-ataka-na-ukrainu-postradali-organy-yustitsii-i-notariusov#google_vignette.
10. Щодо захисту персональних даних в умовах воєнного стану / Омбудсман України [Електронний ресурс]. – Режим доступу : https://ombudsman.gov.ua/storage/app/media/Воєнний%20стан/Захист%20персональних%20даних/Захист%20персональних%20даних%20в%20умовах%20воєнного%20стану.pdf.
11. *Бєлов М.В.* Виклики та загрози захисту персональних даних у роботі за штучним інтелектом / *М.В. Бєлов, Д.М. Бєлом* // Науковий вісник Ужгородського Національного Університету. Серія : Право. – 2023. – Вип. 79 (2). – С.17-22.
12. *Манжула А.А.* Права людини і національної безпеки як об'єкт правового захисту у контексті діяльності служби безпеки України / *А.А.Манжула, О.А.Сокуренко* // Юридичний науковий електронний журнал. – 2024. – № 6. – С. 227-229 [Електронний ресурс]. – Режим доступу : http://www.lsej.org.ua/6_2024/57.pdf.
13. Шифрування : типи і алгоритми. Що це, чим відрізняються і де використовуються? / HostPro [Електронний ресурс]. – Режим доступу : https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.

References:

1. Doronin, I.M. (2020), «Natsionalna bezpeka Ukrainy v informatsiinu epokhu: teoretyko-pravove doslidzhennia», Dys. na zdobuttia nauk. stup. d-ra yur. nauk., Kyiv, 539 p., [Online], available at: https://ippi.org.ua/sites/default/files/disertaciya_doronin_0.pdf
2. Dubov, D.V. (2014), *Kiberprostir yak novyy vymir heopolitychnoho supernytstva: monohrafiia*, NISD, Kyiv, 328 p.

3. Diorditsa, I.V. (2020), «Ponyattya ta zmist kibershpyhunstva», *Naukovi pratsi Natsionalnoho universytetu «Odeska yurydychna akademiia»*, Helvetyka, Odesa, Vol. 26, pp. 49-55.
4. Verkhovna Rada Ukrainy (2010), *Pro zakhyst personalnykh danykh*, Zakon Ukrayiny vid 01.06.2010 r. No. 2297-VI, [Online], available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text
5. *GDPR*, «Zahalnyi rehlament pro zakhyst danykh», [Online], available at: https://gdpr-text.com/uk/.
6. *ESET*, «Strashni istorii kibersvitu: 5 naibilshykh vytokiv danykh desiatylittia», [Online], available at: https://www.eset.com/ua/about/newsroom/blog/data-protection/strashnyye-istorii-kibermira-5-krupneyshikh-utechek-dannykh-desyatiletiya/?srsltid=AfmBOooUEY9ppkhBTC_VWwk7cAuSenP8OIDTVHf707i4HMavF0oYdkFg
7. *Ukrainska pravda*, «Vytoku danykh ne bulo: SBU rozsliduie masshtabnu ataku khakeriv na saity uriadu», [Online], available at: https://www.pravda.com.ua/news/2022/01/14/7320365/
8. *Welivesecurity*, «HermeticWiper: New data-wiping malware hits Ukraine», [Online], available at: https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/
9. *UANews*, «Nova khakerska ataka na Ukrainu: postrazhdaly orhany yustytsii ta notariusiv», [Online], available at: https://ua.news/ua/technologies/novaya-hakerskaya-ataka-na-ukrainu-postradali-organy-yustitsii-i-notariusov#google_vignette
10. *Ombudsman*, «Shchodo zakhystu personalnykh danykh v umovakh voiennoho stanu», [Online], available at: https://ombudsman.gov.ua/storage/app/media/Voyennyy%20stan/Zakhyst%20personal′nykh%20danykh/Zakhyst%20personal′nykh%20danykh%20v%20umovakh%20voyennoho%20stanu.pdf.
11. Byelov, M.V. and Byelom, D.M. (2023), «Vyklyky ta zahrozy zakhystu personal′nykh danykh u roboti za shtuchnym intelektom», *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu.* Seriia *Pravo*, No. 79 (2), pp.17–22.
12. Manzhula, A.A. and Sokurenko, O.A. (2024), «Prava liudyny i natsionalnoi bezpeky yak obiekt pravovoho zakhystu u konteksti diialnosti sluzhby bezpeky Ukrainy», *Yurydychnyi naukovyi elektronnyi zhurnal*, No. 6, pp. 227–229, [Online], available at: http://www.lsej.org.ua/6_2024/57.pdf
13. *HostPro*, «Shyfruvannia : typy i alhorytmy. Shcho tse, chym vidrizniaiutsia i de vykorystovuiutsia?», [Online], available at: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/

Fasii B.

National security and personal data protection in the era of digital technologies

Abstract. The article provides a comprehensive analysis of the interrelationship between personal data protection and national security in the context of digital transformation. The development of information technologies creates new challenges that require a reconsideration of traditional approaches to ensuring state security and protecting human rights. Particular attention is given to the issues of foreign experience in personal data protection and the reasons behind the insufficient level of protection in Ukraine. An important aspect is the study of threats emerging in the digital environment, such as cyber espionage, cyberattacks, and mass surveillance of personal data, which may jeopardize human rights. The article also explores legal, technical, and organizational mechanisms for data protection, including the implementation of encryption, multi-factor authentication, and the use of artificial intelligence to enhance security.

The leading research methods employed are dialectical and systematic, allowing for a comprehensive analysis of the relationship between personal data protection and national security in the context of digital transformation. The dialectical method facilitates the study of the evolution of legal norms and technological processes in the face of the constantly changing challenges of cyberspace, particularly through the juxtaposition of threats and security measures. The systematic method enables the evaluation of legal, technical, and organizational aspects of personal data protection as part of an integrated national security mechanism, including legal standards, state policies, and technological solutions.

The theoretical significance of the article lies in the in-depth analysis of the interconnection between personal data protection and national security in the digital age, as well as in identifying key threats and legal approaches to addressing them. The practical significance is in providing specific proposals for the implementation of modern technical solutions to enhance protection against cyber threats.

Keywords: personal data; national security; cybersecurity; artificial intelligence; digital technologies.

Стаття надійшла до редакції 06.11.2024.