УДК 342.9
DOI https://doi.org/10.32782/pdu.2024.3.7

О. О. Терзі
доктор юридичних наук, доцент,
професор кафедри Національної безпеки, інституту безпеки,
ПрАТ "ВНЗ «Міжрегіональна академія управління персоналом»
https://orcid.org/0000-0003-4120-6526

ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: ДОСВІД УКРАЇНИ ТА ЗАРУБІЖНИХ КРАЇН

У статті проаналізовано принципи забезпечення інформаційної безпеки України, які дозволяють встановити як функціонує система інформаційної безпеки як основа всіх інших аспектів національної безпеки, включаючи норми та правила поведінки громадян, держави та громадських установ.

У сучасних умовах розвитку держави проблеми інформаційної безпеки зумовлені гострою необхідністю її інтеграції в глобалізоване інформаційне суспільство та пошуку ефективних рішень щодо забезпечення функціонування держави в інформаційній сфері. Здебільшого це пов'язано з неефективністю належної політики інформаційної безпеки органів державної влади та необхідністю перегляду доктринальних засад її забезпечення.

Визначено, що інформаційна безпека також є важливою частиною національної безпеки. Окрім того, інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів.

Автор прийшов до висновку, що інформаційна безпека має вирішальне значення в сучасному цифровому світі для захисту від різноманітних таких загроз, кількість яких постійно зростає. Фундаментальні принципи інформаційної безпеки є основою надійної стратегії безпеки, що охоплює найкращі практики, методології та методи захисту важливої інформації. На сьогодні принципи забезпечення інформаційної безпеки не закріплені на законодавчому рівні, проте активно розробляються як рівні законопроєктів, так і на доктринальному рівні. Визначальне значення у даному процесі має аналіз зарубіжного досвіду розвинених країн світу.

Нашій державі варто адаптувати найефективніші практики та інструменти забезпечення інформаційної безпеки, враховуючи свої унікальні характеристики та виклики. Серед ключових напрямів, на які варто звернути увагу для забезпечення надійної інформаційної безпеки держави в сучасних умовах, – інтеграція світових стандартів, створення внутрішньої нормативно-правової бази, посилення взаємодії державних і приватних структур, підвищення інформаційної грамотності населення.

Ключові слова: *національна безпека, інформаційна безпека, принципи інформаційної безпеки, зарубіжний досвід, правове регулювання, забезпечення інформаційної безпеки.*

Постановка проблеми. Питання інформаційної безпеки останнім часом стає все більш актуальним для сучасної України. Це пов'язано з неодноразовими вторгненнями в національний інформаційний простір інших держав та підконтрольних їм суб'єктів, а також з активізацією євроінтеграційних зусиль України та залученням країни до міжнародних безпекових ініціатив і програм за підтримки інших держав.

Стан дослідження. Проведений доктринальний аналіз проблем інформаційної безпеки засвідчив значний інтерес до цієї проблематики. Різноманітні аспекти проблеми забезпечення інформаційної безпеки досліджувались багатьма вченими-юристами, що зумовлено її актуальністю. Вивчення інформаційної безпеки знаходить своє відображення у працях таких науковців, як В. Авер'янов, О. Андрійко, Л. Біла, В. Гаращук, Р. Калюжний, В. Ліп-

кан, А. Марущак, О. Олійник, В. Остроухов тощо. Зарубіжний досвід забезпечення інформаційної безпеки стали предметом наукових розвідок таких вчених, як: І. Бережнюк, О. Береза, М. Дмитренко, Н. Камінська, Б. Кормич, Я. Малик, В. Ліпкан, В. Шемчук та ін.

Мета статті – узагальнення зарубіжного досвіду правового регулювання інформаційної безпеки та обґрунтування концептуальних положень системи принципів в сфері забезпечення інформаційної безпеки України.

Виклад основного матеріалу. Стрімкий розвиток інформаційно-комунікаційних технологій, тотальна комп'ютеризація, створення глобального інформаційного простору зумовлює послаблення інформаційного суверенітету держави. Глобалізація інформаційного простору не може не впливати на стан інформаційної безпеки будь-якої держави. Створення інформаційного суспільства зумовило виникнення багатьох новітніх загроз у важливих сферах життєдіяльності суспільства (банківська, воєнна, критична інфраструктура тощо), тому інформаційну безпеку цілком виправдано розглядають як самостійний елемент національної безпеки [1, с. 284].

Як важлива складова політичної, економічної, оборонної та інших аспектів національної безпеки, інформаційна безпека також є частиною національної безпеки. Окрім того, інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів.

Щодо визначення поняття «інформаційна безпека» на сьогодні відсутній цілісний підхід і єдиної думки щодо її визначення серед дослідників не існує. Інформаційна безпека як поняття розглядається у декількох ракурсах. У найзагальнішому вигляді – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах особи, суспільства, держави. Інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, юридичних заходів, спрямованих на забезпечення сталого розвитку суспільства і держави [2, с. 64].

В. Ліпкан зазначає, що інформаційна безпека України є органічною складовою національної, відтак її розгляд є необхідним для формування базових знань та уявлень про національну безпеку. Нормальна життєдіяльність суспільства визначається рівнем розвитку, якістю функціонування і безпекою інформаційного середовища, а також рівнем і станом нормативноправового забезпечення даних процесів. Інформаційне законодавство спрямоване на закріплення державної інформаційної політики, яка передбачає забезпечення гарантованого рівня національної безпеки в інформаційній сфері, нормального розвитку інформаційних технологій і засобів захисту інформації, виключення монополізму в даній області, запобігання розроблення інформаційно деструктивних технологій впливу на антропогенну популяцію, захист авторських і суміжних прав тощо [3, с. 194].

Визначальне значення у контексті формування інформаційної безпеки держави належить принципи, на яких здійснюється відповідні процеси. Різні держави встановили фундаментальні принципи та інструменти для створення ефективного захисту інформації в межах свого національного простору, що є основою інформаційної безпеки будь-якої країни.

Зупинимось на визначенні поняття «принцип» у правовій доктрині. Словник української мови пропонує наступне тлумачення дефініції «принцип»: 1) основне вихідне положення якої-небудь наукової системи, теорії, ідеологічного напряму та ін.; 2) особливість, покладена в основу створення або здійснення чого-небудь, спосіб створення або здійснення чогось; 3) переконання, норма, правило, яким керується хто-небудь у житті, поведінці [4, с. 1125].

Аналізуючи значення принципів для будь-якої соціальної системи, варто зазначити, що принципи сприяють правильному пізнанню і застосуванню норм права, створюють основу єдиного розуміння нормативно-правових приписів, сприяють усвідомленню права і тим самим

дають можливість однакового тлумачення цих приписів [5, с. 123].

Під принципами права в теорії права традиційно розуміють як категорію відправних ідей існування права, що реалізують вираження найважливіших закономірностей та підвалин цього різновиду держави та права, постає однопорядковим із сутністю права та становить його основні характерні ознаки, відрізняється універсальністю, імперативністю вищого класу та суспільною значимістю, відповідає об'єктивній потребі побудування та зміцнення відповідного ладу в суспільстві [6, с. 27].

Щодо принципів інформаційної безпеки, варто зазначити, що законодавство на сьогоднішній не містить їх переліку. Проте, у проєкті Закону України «Про засади інформаційної безпеки України» визначено основні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, системи суб'єктів забезпечення інформаційної безпеки та засади їх функціонування в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору. Відповідно до ст. 3 вказаного проєкту, основними принципами забезпечення інформаційної безпеки України є [7]:

– верховенство права;

– пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері;

– своєчасність і адекватність заходів захисту життєво важливих національних інтересів України від реальних і потенційних загроз інформаційній безпеці;

– свобода збирання, зберігання, використання та поширення інформації; достовірність, повнота та неупередженість інформації;

– захищеність особи від втручання в її особисте та сімейне життя;

– обмеження доступу до інформації виключно на підставі закону;

– гармонізація особистих, суспільних і державних інтересів, відповідальність всього Українського народу за забезпечення інформаційної безпеки;

– розмежування повноважень, взаємодія та відповідальність державних і недержавних суб'єктів забезпечення інформаційної безпеки;

– пріоритетність розвитку національних інформаційних технологій, ресурсів, продукції та послуг;

– можливість задіяння в інтересах забезпечення інформаційної безпеки України систем і механізмів міжнародної та колективної безпеки;

– гармонізація інформаційного законодавства з нормами міжнародного права і правовими актами Європейського Союзу.

Окрім того, досліджувані принципи можна зустріти у проєкті Закону України «Про Концепцію державної інформаційної політики України», поданий Кабінетом Міністрів України (реєстр. № 7251)» від 11 січня 2011 р. [8]. Вказаний проєкт містить більш розширений перелік принципів забезпечення інформаційної безпеки. Зокрема, окрім вищезазначених також називає принципи: захист інформаційного суверенітету України; свобода думки і слова та вільне вираження своїх поглядів і переконань; захищеність особи від втручання в її особисте та сімейне життя; обмеження доступу до інформації виключно на підставі закону; захист інформаційного суверенітету, державного суверенітету, конституційного ладу і територіальної цілісності України; формування в інформаційному просторі української ідентичності як невід'ємної складової сталого суспільно-політичного дискурсу; формування дуальної системи суспільного та комерційного мовлення; сприяння розвитку в національному інформаційному просторі контенту, який підтримує збереження і захист загальнолюдських цінностей, інтелектуальний, духовний і культурний розвиток Українського народу.

На думку О. Олійник, принципи формування і забезпечення функціонування системи інформаційної безпеки мають бути спрямованими на реалізацію головної мети державної політики та визначатися законом як важливіші складові правових механізмів регулювання відносин у цій системоутворюючій складовій забезпечення національної безпеки. До вказаних принципів автор пропонує віднести: пріоритет прав, свобод і законних інтересів людини і громадянина;

верховенство права, рівність усіх суб'єктів правовідносин перед законом; відповідальність держави перед людиною за свою діяльність; комплексний підхід до вирішення завдань забезпечення інформаційної безпеки; єдність і взаємозв'язок напрямів забезпечення інформаційної безпеки; розмежування сфер відповідальності й повноважень державних органів і органів місцевого самоврядування з питань забезпечення інформаційної безпеки; участь у міжнародних і регіональних системах інформаційної безпеки; оперативність, своєчасність, превентивність і адекватність заходів щодо попередження і захисту від зовнішніх інформаційних загроз та нейтралізації джерел внутрішніх інформаційних загроз [9, с. 75, 77]. Б. Кормич пропонує для визначення принципів забезпечення інформаційної безпеки два комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їх нормативно-правову базу, а саме: це комплекс питань, пов'язаних з інформаційною безпекою людини і суспільства, яка, в першу чергу, вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення; це комплекс питань, пов'язаних з інформаційною безпекою держави, які, навпаки, пов'язані із застосуванням обмежень, заборон, жорсткою регламентацією певних типів відносин в інформаційній сфері і невід'ємним елементом яких є сила державного примусу [10, с. 117].

На сьогодні нормативні документи, які визначають концептуальні засади забезпечення національної безпеки й оборони і, зокрема, інформаційної безпеки (Доктрина інформаційної безпеки, Стратегічний оборонний бюлетень) передбачають, що налагодження співпраці із зарубіжними цивільними і мілітарними структурами, які підтримують обороноздатність і державну безпеку, є вагомими запоруками зміцнення основ національної безпеки, у тому числі і інформаційної [11; 12].

Використовуючи успішні інформаційні досягнення інших держав та країн ЄС, необхідно побудувати першокласну систему захисту інформації, яка б задовольняла як нагальні потреби України, так і сучасні вимоги. Таким чином, дослідження зарубіжних моделей інформаційної безпеки стане додатковою мотивацією вітчизняних фахівців до оптимізації та реформування національної моделі державного управління у відповідній сфері.

Сполучені Штати Америки можна вважати лідером у сфері інформаційної безпеки, оскільки вони не лише вперше в історії запровадили електронне урядування з використанням передових технологій, але також розробили унікальну структуру для захисту національного інформаційного суверенітету та безпека інформаційних ресурсів. Згадувати в першу чергу Сполучені Штати Америки (США), найпотужнішу в політичному, економічному та військовому плані державу, є цілком розумним підходом з огляду на її великий досвід забезпечення інформаційної безпеки.

Основні законодавчі засади забезпечення інформаційної безпеки США було сформовано після другої світової війни. Правову основу адміністрування інформаційної безпеки США становлять закони «Про охорону особистих таємниць» (1974 р.), «Про таємницю» (1974 р.), «Про висвітлення діяльності уряду», «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп`ютерних систем» (1987 р.), «Про комп`ютерне шахрайство та зловживання» (1986 р.). За ініціативи Президента США Р. Рейгана було розроблено та ухвалено Закон «Про свободу інформації», а забезпечення інформаційної безпеки стало пріоритетним завданням політики Державного департаменту.

У 1990-х роках на хвилі активізації і глобалізації інформаційних відносин було введено у дію федеральні закони «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997 р.) [13].

Також у лютому 2003 року адміністрацією Джорджа Буша молодшого була опублікована Національна стратегія досягнення безпеки в кіберпросторі (National Strategy to Secure Cyberspace), в якій викладено п'ять пріоритетів діяльності США із забезпечення інформаційної без-

пеки та основних завдань у рамках цих пріоритетів на середньострокову та довгострокову перспективу [14]. Фактично ці документи можуть вважатися офіційною загальнонаціональною політикою США у сфері інформаційної безпеки, на основі якої будується система діяльності державної влади та структура державних органів, які забезпечують інформаційну безпеку в державі.

Сьогодні США має найпотужніший і всеохоплюючий режим управління інформаційною безпекою. За інформаційну безпеку та захист урядових систем та державної інфраструктури США відповідають ціла низка державних та федеральних структур, зокрема, Федеральне агентство кібербезпеки та інфраструктури (CISA), Рада національної безпеки, Федеральне бюро розслідувань (ФБР), Агентство національної безпеки (АНБ), Міністерство оборони (МО), Комісія з цінних паперів та бірж (SEC) тощо. Всі ці установи та організації у своїх внутрішніх структурах мають власні відділи, які займаються питаннями інформаційної безпеки та запобіганням до інформаційних атак, а також підготовкою до кібератак.

Отже, в США вже сформувалась система забезпечення інформаційної безпеки. Основними компонентами єдиного інформаційного простору Сполучених Штатів Америки є національні інформаційні ресурси, інформаційна інфраструктура (яка охоплює інфраструктуру, необхідну для функціонування інформаційного простору) та інформаційно-телекомунікаційні структури (до яких входять системи ЗМІ, комп'ютерні мережі та інформаційні технології).

Базовим законом у сфері інформаційної безпеки Німеччини є Закон «Про посилення безпеки систем інформаційних технологій» (Закон про безпеку IT) від 25.07.2015. Закон відводить Федеральному відомству з безпеки в сфері інформаційних технологій (BSI) центральну роль в захисті критично важливих інфраструктур у Німеччині.

Як Федеральний орган кібербезпеки, Федеральне відомство інформаційної безпеки (BSI) постійно стежить за загрозами IT-безпеки в Німеччині. BSI зосереджується на кібератаках на урядові та громадські установи, компанії та приватних осіб, а також на заходах із запобігання та боротьби з цими ситуаціями. BSI охоплює превентивну кібербезпеку для німецьких комп'ютерних і комунікаційних законів, критичної інфраструктури, як-от енергетика, охорона здоров'я, продовольство, IT та телекомунікації, а також фінанси.

У червні 2023 року була прийнята Стратегія національної безпеки Федерального уряду. У цьому звіті розглядаються поточні та поточні кіберзагрози та оцінюється стан IT-безпеки в контексті агресивної війни Росії проти України. Використовуючи конкретні приклади в різних секторах, звіт простежує шлях і типові методи, які використовують зловмисники, і в той же час показує, як користувачі можуть захистити себе [15].

Система інформаційної безпеки Франції є складником національної безпеки, відповідно, основні її принципи закладені у Білих книгах оборони та національної безпеки.

Перша Біла книга з національної оборони була опублікована у 1972 році, у ній викладені принципи оборонної політики Франції та основи стратегії ядерного стримування. Опублікована у 1994 році друга Біла книга була присвячена закінченню «холодної війни» і перенаправленню збройних сил на військові операції за межами національної території, що призвело до професіоналізації збройних сил [16]. У 2008 році прийнята третя Біла книга під впливом процесів глобалізації та боротьби з тероризмом та розроблення нової концепції стратегії національної безпеки. Четверта Біла книга опублікована в 2013 році під головуванням Франсуа Олланда. П'ятий документ під трохи іншою назвою («Стратегічний оборонний огляд та національна безпека» (далі – Оборонний огляд)) опубліковано в кінці 2017 року під головуванням Еммануїла Макрона. В Оборонному огляді значна увага приділяється інформаційним загрозам та заходам протидії ним.

У 2015 році Франція прийняла національну стратегію кібербезпеки. Ця стратегія спрямована на супровід цифрового переходу французького суспільства та

вирішення нових проблем, пов'язаних із зміною використання цифрових технологій і пов'язаними з ними загрозами. Вона зосереджена на п'яти цілях: гарантування національного суверенітету, забезпечення жорсткої відповіді на кіберзлочинність, інформування громадськості, цифрова безпека як конкурентна перевага для французьких компаній, посилення позиції Франції на міжнародній арені.

Висновки. Інформаційна безпека має вирішальне значення в сучасному цифровому світі для захисту від різноманітних таких загроз, кількість яких постійно зростає. Фундаментальні принципи інформаційної безпеки є основою надійної стратегії безпеки, що охоплює найкращі практики, методології та методи захисту важливої інформації. На сьогодні принципи забезпечення інформаційної безпеки не закріплені на законодавчому рівні, проте активно розробляються як рівні законопроєктів, так і на доктринальному рівні. Визначальне значення у даному процесі має аналіз зарубіжного досвіду розвинених країн світу.

Вивчення міжнародного досвіду дозволяє прийти до висновку, що Україні варто адаптувати найефективніші практики та інструменти забезпечення інформаційної безпеки, враховуючи свої унікальні характеристики та виклики. Серед ключових напрямів, на які варто звернути увагу для забезпечення надійної інформаційної безпеки держави в сучасних умовах, – інтеграція світових стандартів, створення внутрішньої нормативно-правової бази, посилення взаємодії державних і приватних структур, підвищення інформаційної грамотності населення.

Інформаційну безпеку можна гарантувати лише завдяки міжнародній співпраці, оскільки комунікаційні мережі мають глобальний характер. У зв'язку з цим необхідно посилити відносини України з іншими державами та міжурядовими організаціями щодо забезпечення правової безпеки інформації.

Список використаної літератури:

1. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н.Каразіна. Серія "ПРАВО".* 2020. № 29. С. 281-288.
2. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.
3. Ліпкан В.А. Національна безпека України: Навч. посіб. 2-ге вид. К., 2009.
4. Великий тлумачний словник сучасної української мови : 250000 / уклад. та голов. ред. В. Т. Бусел. Київ; Ірпінь: Перун, 2005. VIII, 1728 с.
5. Шмаленя С. В. Особливості застосування аналогії права при вирішенні юридичних справ: дис. … канд. юрид. наук : 12.00.01. Запоріжжя, 2008. 238 с.
6. Колодій А.М. Принципи права України : монографія. Київ : Юрінком Інтер, 1998. 208 с.
7. Проект Закону України «Про засади інформаційної безпеки України», внесений народними депутатами України: І. М. Стойком (реєстр. N 390), О. І. Кузьмуком (реєстр. N 041), Ю. М. Сиротюком (реєстр. N 214) URL: https://ips.ligazakon.net/document/JG3TH00A?an=31
8. Проєкт Закону України «Про Концепцію державної інформаційної політики України» від 13.10.2010 № 7251 URL: https://ips.ligazakon.net/document/JF5LF00A
9. Олійник О.В. принципи забезпечення інформаційної безпеки України. *Юридичний вісник.* 4 (41). 2016. С.71 – 78.
10. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посіб. К.: Кондор, 2008. 382 с.
11. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/217. Офіційний вісник Президента України. 2017. № 5. стор. 15
12. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України»: Указ Президента України від 06.06.2016 р. № 240/216. URL: https://www.president.gov.ua/documents/2402016-20137/
13. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. Інтернет-сайт Центру досліджень соціальних комунікацій НБУВ URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavcheregulyuvannya-

ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350
14. The National Strategy to Secure Cyberspace URL: https://georgewbush-whitehouse.archives.gov/pcipb/
15. The State of IT Security in Germany in 2023 URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf?__blob=publicationFile&v=9
16. Шемчук В.В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Порівняльно-аналітичне право*. 2019. № 2. С. 188 – 191.

Terzi O. Principles of ensuring information security of the state: the experience of Ukraine and foreign countries

The article analyzes the principles of ensuring information security of Ukraine, which allow establishing how the information security system functions as the basis of all other aspects of national security, including norms and rules of behavior of citizens, the state and public institutions.

In the modern conditions of state development, the problems of information security are determined by the urgent need for its integration into the globalized information society and the search for effective solutions to ensure the functioning of the state in the information sphere. This is mostly due to the ineffectiveness of the appropriate information security policy of state authorities and the need to review the doctrinal foundations of its provision.

It was determined that information security is also an important part of national security. In addition, information security is an integral component of the general problem of information provision of people, the state and society. It is focused on the protection of significant or already mentioned subjects of information resources, legitimate interests.

The author concluded that information security is crucial in today's digital world to protect against a variety of such threats, the number of which is constantly increasing. The fundamental principles of information security are the foundation of a sound security strategy, covering best practices, methodologies and methods for protecting critical information. Today, the principles of ensuring information security are not fixed at the legislative level, but they are actively being developed both at the level of draft laws and at the doctrinal level. The analysis of the foreign experience of the developed countries of the world is of decisive importance in this process.

Our state should adapt the most effective practices and tools for ensuring information security, taking into account its unique characteristics and challenges. Among the key areas that should be paid attention to in order to ensure reliable information security of the state in modern conditions are the integration of world standards, the creation of an internal regulatory and legal framework, strengthening the interaction of state and private structures, and improving the information literacy of the population.

Key words: *national security, information security, principles of information security, foreign experience, legal regulation, ensuring information security.*