УДК 004.056.5(477)
DOI https://doi.org/10.32782/TNU-2663-6468/2024.4/06

Новицький В.А.
Класичний приватний університет

ГЕНЕЗА ПОНЯТТЯ «ІНФОРМАЦІЙНА БЕЗПЕКА»: ПОХОДЖЕННЯ ТА СТАНОВЛЕННЯ

Ця стаття розглядає походження поняття інформаційної безпеки як невід'ємної складової національної безпеки. Автор аналізує історичні тлумачення цього поняття, наводить різні погляди вітчизняних науковців на цю тему. Особлива увага приділяється актуальності інформаційної безпеки, особливо в умовах повномасштабної війни з РФ. Метою дослідження є аналіз теоретичних розробок щодо еволюції поняття інформаційної безпеки шляхом визначення її сутності як основного та невід'ємного напрямку національної безпеки. Зазначається, що чинне законодавство України не містить розгорнутого визначення цього поняття, але нормативні акти, що стосуються питань інформаційної безпеки, розглядають її в контексті загального поняття національної безпеки. Інформаційна безпека є не лише окремою складовою національної безпеки, але й невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки, оскільки всі види відносин між суб'єктами інформаційного суспільства базуються на споживанні та обміні інформацією. Доведено, що інформаційну безпеку України доцільно розглядати як стан, умови дії реальних та потенційних загроз, який забезпечує самозбереження, сталий і прогресивний розвиток інформаційної сфери, включаючи захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб'єктів, а також досягнення відповідних національних цілей та реалізацію національних інтересів в інформаційній сфері. Пропонується розглядати інформаційну безпеку як постійний процес діяльності компетентних органів, спрямований на попередження, протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються і здатні контролюватися тривалий час.

Ключові слова: *інформація, інформаційна безпека, державна інформаційна політика, загрози інформаційній безпеці, національна безпека, стратегія національної безпеки.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій у промислово розвинених країнах призвів до появи стратегій «інформаційної війни», основною метою яких є одержання або перетворення інформації у своїх інтересах. У сучасному контексті очевидно, що інформаційні технології відіграють надважливу роль не тільки в забезпеченні національної безпеки, а й у розвитку особистості, суспільства і держави. З розвитком технологій і засобів передачі даних змінилися і методи захисту інформації. На сучасному етапі розвитку суспільства ефективна інформаційна безпека здатна вирішити практично всі види важливих проблем національної безпеки. Інформаційна безпека є важливим компонентом системи національної безпеки, і від успішного розв'язання проблем у цій галузі залежить глобальна безпека.

Аналіз останніх наукових досліджень і публікацій. Через складність і багатогранність питань інформаційної безпеки їх вивченням займаються представники різних галузей криміналістики. Основи розуміння природи інформаційної безпеки можна знайти в працях Сунь-цзи, Нікколо Макіавеллі, Гроція Гуго де Гроота, Томаса Гоббса, Еммануїла Канта, Анрі Бергсона та інших. У розвитку сучасної науки проблему досліджували в працях О. Баранова, В. Глуховського, О. Даниляна, О. Зобана, М. Панова, В. Шатуна та інших.

Постановка завдання. Мета – проаналізувати теоретичні розробки в царині еволюції концепції інформаційної безпеки, виявляючи сутність інформаційної безпеки як фундаментального та невід'ємного напряму національної безпеки.

Виклад основного матеріалу. Коли мова заходить про національну інформаційну безпеку, неможливо ігнорувати «духовного батька» інформаційної війни, китайського військового стратега і філософа Сунь-Цзи (313–239 рр. до н. е.). Сунь Цзи написав першу фундаментальну працю в цій царині – «Мистецтво війни», у якій, зокрема, стверджує, що якщо передові правителі та мудрі полководці перемагають своїх ворогів щоразу, коли вступають у бій, то це відбувається завдяки попередній інформації. Так звана

попередня інформація не може бути отримана від духів або Бога, за аналогією з минулими подіями або шляхом розрахунків. Вона повинна виходити від людини, яка добре знайома з ситуацією противника. Концепція Сунь-цзи ґрунтується на теорії нападу на супротивника, якого заманили у вигідну позицію, позбавили мужності, ослабили та виснажили [8, с. 90].

Якісно новий етап у поелементному формуванні наукових і філософських концепцій безпеки пов'язаний з епохою Відродження. У центрі уваги головних мислителів цього періоду була людина, її духовне життя (інформаційна сфера) і звільнення від гніту та соціальної несправедливості. Розуміючи умови для безпечного і гармонійного розвитку особистості, гуманісти порушували питання про усунення найбільшого зла в житті людини – війни. Безсумнівно, ідея вічного миру народилася тому, що війна ставала загрозою для народів Європи.

У XVI столітті італійський мислитель Нікколо Макіавеллі сформулював інформаційно-психологічну концепцію державної влади, в якій виклав основні принципи ведення інформаційної війни в політичній сфері. Ба більше, історія рясніє прикладами потужних інформаційно-пропагандистських кампаній – класичних варіантів глобальних масових інформаційних операцій, що зіграли смертельну роль.

На початку XVII століття було зроблено спроби врегулювати відносини між державами. Одним з основоположників теорій природного права і міжнародної юриспруденції був голландський мислитель Гроцій Гуго де Гроот. Договори між державами, що підкоряються природному праву, мають мати пріоритет над авторитетом папи римського, несправедливі війни, що порушують права всіх людей, мають бути заборонені, а сторони, що воюють, зобов'язані утримуватися від знищення майна супротивника та вчинення злочинів щодо мирного населення.

Наукові уявлення про національну безпеку загалом у сучасному розумінні та її інформаційні аспекти, а також напрями її розв'язання містяться у працях Томаса Гоббса та Еммануїла Канта. Найхарактернішими в цьому контексті є погляди Гоббса і Канта на природу досліджуваної проблеми. Кант і Гоббс дійшли висновку, що з огляду на беззаконну природу і право кожного на все необхідно створити громадянську систему, яка гарантувала б особисту безпеку.

Ідея безпеки в епоху раннього Просвітництва знайшла відображення у філософських і політичних працях Джона Локка. В епоху Просвітництва Ф. Вольтер і Дідро розвивали філософське питання безпеки через релігійно-етичне розуміння проблеми миру, а в період німецької класичної філософії Й. Фіхте і Й. Гердер розглядали ідею безпеки з різних точок зору через обґрунтування державного суверенітету. Французький філософ Анрі Бергсон пов'язував інформаційну безпеку з розумінням закритих і відкритих суспільств, стверджуючи, що насильство і війна є неминучим наслідком закритих суспільств, а отже, сумною необхідністю нашого часу. Він вважав, що єдиний шлях до подолання насильства, несправедливості й роз'єднаності та досягнення безпечного стану людського існування лежить через поширення «духу простоти», проголошеного християнськими містиками, принципу аскетизму та відмови від «штучних бажань», спричинених розвитком «тіла», а не «душі» людства, що переважав в останні століття [8, с. 93].

Дослідники в галузі інформаційної безпеки приділяють особливу увагу концепції «інформаційної війни». Уперше цей термін був використаний Томасом Роною, науковим консультантом Міністерства оборони США, у його доповіді 1976 року «Системи зброї та інформаційна війна», підготовленій для компанії Boeing. У цьому документі Т. Рона стверджував, що інформаційна інфраструктура, ключовий компонент економіки США, стає вразливою мішенню як у воєнний, так і в мирний час. Термін «інформаційна війна» став офіційно використовуватися міністром оборони США в директиві з інформаційної війни від 21 грудня 1992 року. Таким чином, американські військові вперше застосували новітні інформаційні технології у війні в Перській затоці (1991), а після війни, також уперше у світі, ключові військові діячі США офіційно сформулювали стратегічні принципи інформаційної війни. Сьогодні перед Україною стоять нові та надзвичайно складні виклики. Перед обличчям гібридної війни, розв'язаної Російською Федерацією, і різних аспектів великомасштабної війни наша країна заявляє, що захищатиме фундаментальні національні цінності, як-от національна незалежність, територіальна цілісність, суверенітет, свобода, права людини, верховенство права, процвітання, мир і безпека, і забезпечуватиме ефективне функціонування сектору безпеки й оборони в умовах обмежених ресурсів та часу, очевидно, що країна зіштовхнулася з критичною необхідністю. У сучасній Україні ключ до успішної протидії масштабній зовнішній агресії та сталого розвитку інформацій-

ного суспільства полягає не лише в підвищенні технічних можливостей інформаційного обміну, а й у глибокому усвідомленні всіма суб'єктами інформаційної діяльності необхідності вжиття всіх заходів із захисту інформаційних ресурсів та забезпечення національної інформаційної безпеки [6, с. 46]. Проте це неможливо без чіткого розуміння природи інформаційної безпеки.

Сьогодні існує безліч теорій щодо визначення інформаційної безпеки, але єдиної думки про її сутність поки що не досягнуто. Згідно з класифікацією В. Липкана, існує кілька підходів до визначення сутності феномена інформаційної безпеки, згідно з якими інформаційна безпека – це стан захищеності інформаційного простору, процес протидії загрозам і небезпекам, що гарантує інформаційну безпеку України, інформаційного середовища та інформації; стан захищеності національних інтересів держави в цій сфері; безпека законодавчо встановлених правил під час здійснення державних інформаційних процесів, ключових функцій держави; стан безпеки інформаційного середовища та інформації; безпека законодавчо встановлених правил під час здійснення державних інформаційних процесів [6, с. 25–30].

О. О. Данилян, О. Зобан і М. Панов визначають це поняття як захищеність об'єкта від загроз і негативних впливів, пов'язаних з інформацією [6, с. 165].

На думку В. Гурковського, інформаційна безпека – це суспільні відносини, пов'язані із захистом життєво важливих інтересів особи, громадян, суспільства і держави від реальних і потенційних загроз в інформаційному просторі, збереженням і примноженням духовних і матеріальних цінностей державотворчої держави, існуванням, самозбереженням і прогресивним Це необхідна умова розвитку країни [4, с. 74].

О. Баранов також використовує категорію національного інтересу і визначає інформаційну безпеку як стан захищеності національних інтересів України в інформаційному середовищі, коли шкоди особі, суспільству та державі завдають неповна, несвоєчасна або недостовірна інформація, несанкціоноване розповсюдження або використання, а також несприятливі або негативні наслідки функціонування інформаційних технологій. Визначається як стан справ, за якого не допускається (або мінімізується) заподіяння шкоди особистості, суспільству і державі [2, с. 60–62]. В. Шатун та О. Градун визначають інформаційну безпеку як стан захищеності національних інтересів України в інформаційній сфері від загроз особі, суспільству і державі, спричинених неповнотою та несвоєчасністю інформації, несанкціонованим поширенням і використанням інформації, негативним впливом інформації та негативними наслідками функціонування інформаційних технологій. Нижче наводиться стислий виклад визначення [9, с. 175].

В. Шатун та О. Градун розглядають інформаційну безпеку як процес управління загрозами та небезпекою з боку державних і недержавних організацій та осіб з метою забезпечення інформаційного суверенітету України [6, с. 75]. І. Бондар пропонує визначити інформаційну безпеку як функцію системи засобів забезпечення безпеки інформаційних систем. Інформаційна система – це сукупність (державних, а також індивідуальних і корпоративних) інформаційних ресурсів, інформаційних технологій і програмно-технічних засобів, що здійснюють обробку інформації в людино-машинному або автоматичному режимі. Побудова і функціонування цієї системи інформаційних ресурсів спрямоване на забезпечення прав людини, соціальних і державних інтересів в інформаційній сфері [3, с. 72].

Слід зазначити, що чинне законодавство України не дає детального трактування визначення інформаційної безпеки, яке б відповідало даному поняттю. За сучасних умов наявність достовірної інформації про стан і динаміку економічних, політичних, соціальних та інших процесів у суспільстві є визначальною для спроможності влади та суспільства загалом розробляти й реалізовувати ефективні рішення в геополітичній, військово-стратегічній, науковій, освітній, культурній, історичній та екологічній сферах та за умов інтелектуалізації й інформатизації інформація і телекомунікації є факторами, що забезпечують безпеку суспільства. Таким чином, що активніше розвиватиметься інформаційна сфера як системоутворювальний чинник суспільства, то більше політична, економічна, оборонна та інші складові національної безпеки залежатимуть від інформаційної безпеки, і ця залежність ще більше зростатиме в майбутньому, у міру розвитку технологій [1, с. 45].

Розглядаючи історичні аспекти розвитку інформаційних відносин, можна виділити такі основні етапи становлення інформаційної безпеки [7]:

Перший етап – до початку XIX століття. У той час використовувалися стихійні засоби інформації та комунікації. У той час основним завданням інформаційної безпеки був захист інформації про події, факти, майно, місця та інші дані, що мають життєво важливе значення для окремих осіб або

суспільства, до якого вони належать. У широкому сенсі слова заходи із захисту інформації були спрямовані на запобігання фізичному перехопленню повідомлень, особливо під час воєнних дій. Водночас важливо було захистити й особисті дані, включно з інформацією, що стосується торговельних угод, виробництва або винаходу нових товарів та інновацій у промисловому виробництві.

Другий етап – з 1816 по 1935 рік. Цей етап пов'язаний із початком використання технічних засобів телекомунікацій і бездротового зв'язку. Після переходу інформації з фізичного носія в електромагнітне поле виникла необхідність захисту інформації принципово новим способом. Таким чином, у міру розвитку технологій передавання інформації стали розвиватися і методи її захисту. На цьому етапі необхідно було забезпечити конфіденційність і завадостійкість радіозв'язку шляхом завадостійкого кодування повідомлень і подальшого декодування прийнятого сигналу.

Третій етап – з 1935 по 1946 рік. Цей період пов'язаний із появою радіолокаційних і підводних акустичних засобів. Основним методом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, спрямованих на посилення захисту від впливу активних маскувальних і пасивних імітаційних електронних перешкод на приймальне радіолокаційне обладнання. На тому етапі інформаційна безпека особливо бурхливо розвивалася під час Другої світової війни. Це було пов'язано з тим, що успіх тієї чи іншої операції і виживання її сил безпосередньо залежали від реалізації політики інформаційної безпеки. В економічному плані інформаційна безпека на той час була спрямована насамперед на забезпечення інформаційної безпеки нових технологій військового призначення, але не варто забувати і про технології, розроблені в мирних країнах і призначені для всіх сторін конфлікту, умови яких не давали змоги виробляти і розвивати їх у своїх країнах.

Четвертий етап – середина XX століття. З винаходом і комерціалізацією електронного калькулятора (комп'ютера) виникла нова проблема: забезпечення захисту інформації, представленої в електронному вигляді. На тому етапі питання інформаційної безпеки розв'язували здебільшого способами та засобами обмеження фізичного доступу до об'єктів отримання, оброблення та передавання інформації. Адже на той час отримати інформацію в електронному вигляді можна було тільки отримавши фізичний доступ до обладнання, а захисту під час передачі інформації підлягали її фізичні носії і ті самі радіо-, електричні та електромагнітні сигнали.

П'ятий етап – 1960-ті – 1970-ті роки. З появою і розвитком локальних інформаційно-комунікаційних мереж завдання інформаційної безпеки змінилися незначно і зводилися до фізичного захисту елементів локальної мережі. Водночас з'явилися нові завдання, як-от необхідність управління та експлуатації доступу до мережевих ресурсів, які на той момент не були схильні до зовнішнього впливу. Інформаційно-комунікаційні системи промислових підприємств також потребували захисту інформації, що циркулює в них, оскільки будь-яка втрата або пошкодження даних могли призвести до збоїв і, зрештою, до втрати виробництва.

Шостий етап – до середини 1980-х років. Цей етап пов'язаний з використанням ультрамобільних комунікаційних пристроїв, що виконують широкий спектр завдань. Загрози інформаційній безпеці стали серйознішими. Необхідно було розробити нові стандарти безпеки для забезпечення захисту інформації в інформаційно-комунікаційних системах з бездротовими мережами передачі даних. Крім того, з'явилася ціла спільнота людей – хакерів, мета яких – завдати шкоди інформаційній безпеці окремих користувачів, компаній, організацій і навіть цілих країн. Інформація стала найважливішим ресурсом держави, а забезпечення її безпеки – найважливішим і невід'ємним елементом національної безпеки. У міжнародній правовій системі навіть з'явився новий напрям – інформаційне право. Те саме відбулося і в економічній сфері, де компанії почали формулювати власні політики безпеки та визначати способи їх реалізації.

Сьомий етап – з 1985 р. Бурхливий розвиток глобальних інформаційно-комунікаційних систем і поширення космічного зв'язку вимагають нових високотехнологічних засобів захисту інформації. Всебічна автоматизація виробничих процесів на підприємствах також вимагає розширення заходів інформаційної безпеки та постійного оновлення політик безпеки. Як зазначає професорка Г. Аніловська, на сучасному етапі бурхливий розвиток інформаційних технологій та їхнє повсюдне впровадження в облікові процеси призвело до розвитку таких облікових систем, що взаємодіятимуть з іншими системами, а також до проблем конфіденційності самих облікових систем. Ба більше, ці проблеми існують на технологічному, програмному та інформаційному рівнях. Розв'язати ці проблеми можна шляхом розроблення та впровадження єдиних, загальних та обов'язкових пра-

вил створення та використання бухгалтерських інформаційних систем [10].

З розвитком нових інформаційних технологій поняття інформаційної безпеки значно розширилося. Сьогодні захист процесів, інформації та діяльності в кіберпросторі передбачає не тільки втрату інформації. Іншими словами, втрата інформації супроводжується безліччю інших складних проблем. Сьогодні комплекс заходів щодо забезпечення інформаційної безпеки має враховувати, крім іншого, антивірусний захист, захист від хакерських атак і підробки даних. Наприклад, зараження комп'ютерним вірусом може призвести не тільки до видалення або крадіжки даних, а й вплинути на роботу і продуктивність співробітників і навіть призвести до зупинки виробництва.

Тому інформаційна безпека є не лише самостійним компонентом національної безпеки, а й невіддільною частиною політичної, економічної, оборонної та інших складових національної безпеки. І. Бондар пропонує розглядати національну безпеку як складову частину чотирьох компонентів: індивідуального, громадського (соціального), комерційного (ділового).

Інформаційна безпека – явище, унікальне для сучасного суспільства, і її виникнення має глобальне значення для всього людства.

Інформаційна безпека – це справді складне явище. Існує низка умов, що ускладнюють визначення цього поняття. Перелічимо найважливіші з них:

Інформаційна безпека – об'єктивне явище, зумовлене об'єктивними умовами суспільного розвитку. Виникнення інформаційної безпеки відбувається на тлі процесу інформатизації суспільства, який поки що перебуває на початковій стадії і тому потребує подальшого ретельного вивчення. Крім того, особливості інформаційної безпеки в Україні здебільшого пов'язані з реформуванням самої системи національної безпеки. Унаслідок перелічених вище чинників виникають труднощі з наданням достатньо повного визначення досліджуваного поняття. Ми вважаємо, що складність у визначенні поняття «інформаційна безпека» пов'язана ще й із тим, що феномен інформаційної безпеки вивчають із різних аспектів – технічного, юридичного, психологічного та соціального. Науковці, які розглядають це явище з погляду своїх наукових дисциплін, наповнюють термін «інформаційна безпека» власним змістом, що ще раз підкреслює його складність, ускладнюючи створення єдиного визначення.

На наш погляд, під час формулювання визначення практично всі дослідники були одностайні у своєму прагненні уточнити значення терміна «інформаційна безпека» не тільки термінологічно, а й методологічно. Виходячи з того, що сутність безпеки системи полягає у здатності зберігати свою цілісність і розвиватися, реалізуючи ці можливості в реальних умовах, зокрема несприятливих (конфлікт, ризик, невизначеність тощо), ми стверджували, що система безпеки (у нашому разі інформаційної безпеки) є адаптацією вищезазначеного. Ми дійшли основного методологічного висновку, що метою є реалізація можливостей. Тому інформаційну безпеку слід розглядати як безпеку об'єкта в інформаційному середовищі та безпеку інформаційної сфери.

Інакше кажучи, інформаційна безпека досягається не тільки засобами, методами і заходами, що захищають інформаційне середовище і оберігають суб'єкт (об'єкт) від деструктивних впливів, а й формуванням здатності суб'єкта (об'єкта) протистояти деструктивним інформаційним впливам. Таким чином, забезпечення інформаційної безпеки – це створення оптимальних умов для функціонування інформаційної інфраструктури, головним елементом якої є не комп'ютер, а людина, що може поступово розвиватися і діяти відповідно до своїх цінностей і цілей. Ми хотіли б підкреслити, що ця ідея є центральною для нашого дослідження.

На наш погляд, основний зміст виявленої системної формації інформаційної безпеки визначає інформаційну безпеку як цілісне явище. Підсумовуючи наші висновки, ми вивели визначення інформаційної безпеки.

Інформаційна безпека – це сталий стан інформаційної сфери, що гарантує її цілісність і захищеність її об'єктів за наявності внутрішніх і зовнішніх негативних впливів, заснований на цінностях, потребах (життєвих інтересах) людей і усвідомленні ними цілей розвитку.

Це визначення в стислому вигляді відображає суть поняття «інформаційна безпека». Аксіологічний, епістемологічний та онтологічний аспекти розкривають філософський зміст розглядуваного визначення. Онтологічний аспект інформаційної безпеки відображає контекст управління ризиками, метою якого є забезпечення цілісності суб'єкта та стабільності інформаційного середовища. Антропологічний аспект поняття розкриває безпеку суб'єкта інформаційної взаємодії. Аксіологічні елементи поняття «інформаційна безпека» відображають цінності та цілі, що визначають інформаційні потреби людини.

По суті, інформаційна безпека – це комплексне явище об'єктивного розвитку сучасної цивілізації, спрямоване на сприяння гармонійному розвитку інформаційного суспільства. Для забезпечення інформаційної безпеки насамперед необхідно вивчити негативні наслідки, що виникають у процесі застосування інформаційних технологій, і дослідити причини їх прояву.

Не вдаючись у детальний аналіз сучасних підходів до розуміння природи національної інформаційної безпеки, не входитимемо в рамки наявних концептуальних підходів до трактування інформаційної безпеки, тобто статичних (безпека як стан захищеності інформаційного середовища та інформації, системи забезпечення тощо).

З погляду цього підходу, інформаційна безпека України, в контексті протидії реальним і потенційним загрозам, визначається як самозбереження, сталий і прогресивний розвиток безпеки інформаційної сфери, зокрема інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їхніх суб'єктів, а також відповідну безпеку слід розглядати як стан, за якого забезпечується досягнення національних цілей і реалізація національних інтересів в інформаційній сфері. При цьому забезпечення національної інформаційної безпеки слід розглядати як безперервний процес діяльності компетентних органів, спрямований на запобігання та боротьбу із загрозами інформаційній сфері, застосування випереджувальних заходів інформаційного впливу та сукупність умов для цієї діяльності, що можуть бути реалізовані та керовані в довгостроковій перспективі.

Висновки. Збройне вторгнення Росії в Україну, анексія та окупація частини української території призвели до воєнно-політичних труднощів і загроз для інформаційного простору. Поряд зі стратегічною важливістю інформаційного простору для сталого розвитку сучасного суспільства, це визначає пріоритетність інформаційної безпеки в системі національної безпеки України. Тому вкрай важливо правильно зрозуміти зміст категорії «інформаційна безпека», що неможливо без її наукового визначення. Проаналізувавши різні підходи до визначення категорії «інформаційна безпека», що дають змогу всебічно та системно осмислити дане явище, можна сказати, що інформаційна безпека – це юрисдикція, спрямована на запобігання та протидію загрозам в інформаційній сфері шляхом використання позитивних засобів інформаційного впливу. Її пропонується розглядати як постійний процес діяльності органів влади та сукупність умов, за яких ця діяльність може здійснюватися і контролюватися в часі.

Інформаційна безпека як ключова складова національної безпеки охоплює такі пріоритетні напрями Захист інформаційного простору та безпека культурного генофонду людства в умовах глобалізації, тобто окрім правових, організаційних і технічних засобів і методів, важливо ще раз підкреслити, що соціокультурний вимір є важливою складовою процесу забезпечення безпеки інформаційного середовища.

Список літератури:

1. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних *інформаційних технологій. Науковий вісник НЛТУ України*. 2008, вип. 18.9. С. 270.

2. Баранов О. П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. *Вісник Національної академії державного управління при Президентові України*. 2014. No 3. С. 60–65.

3. Бондар І. Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014. No 1. С. 68–75.

4. Гурковський В. І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства. *Правова інформатика*. 2010. No 2(26). С. 72–77.

5. Данильян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України : структура та напрямки реалізації: навчальний посібник. Х. : Фоліо, 2002. 285 с.

6. Ліпкан В.А., Харченко Л.С., Логінов О.В. Інформаційна безпека України : Глосарій. К. : Текст, 2004. 136 с.

7. Присяжнюк М. М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка*. Військово-спеціальні науки. 2013. Вип. 30. С. 42–46.

8. Ткачук Т. Ю., Довгань О. Д. Система інформаційної безпеки України : онтологічні виміри. *Інформація і право*. 2018. No 1 (24). С. 89–104.

9. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»*. 2016. Т. 267. Вип. 255. С. 174–180.

10. NIST Interagency or Internal Report 7298 : Glossary of Key Information Security Terms : Richard L. Kissel, editor, Computer Security Division, Information Technology Laboratory. Revision 2. Gaithersburg, MD, USA : National Institute of Standards and Technology, 2013. 222 p.

Novytskyi V.A. GENESIS OF THE CONCEPT "INFORMATION SECURITY": ORIGIN AND ESTABLISHMENT

This article considers the origin of the concept of information security as an integral component of national security. The author analyzes the historical interpretations of this concept and cites different views of domestic scientists on this topic. Particular attention is paid to the relevance of information security, especially in the conditions of a full-scale war with the Russian Federation. The purpose of the study is the analysis of theoretical developments regarding the evolution of the concept of information security by determining its essence as the main and integral direction of national security. It is noted that the current legislation of Ukraine does not contain a detailed definition of this concept. Still, normative acts related to information security consider it in the context of the general concept of national security. Information security is not only a separate component of national security but also an integral part of political, economic, defense, and other components of national security, since all types of relations between subjects of the information society are based on the consumption and exchange of information. It has been proven that the information security of Ukraine should be considered as a state, conditions of action of real and potential threats, which ensures self-preservation, stable and progressive development of the information sphere, including the security of information infrastructure, information space, information resources, information processes, and their subjects, as well as achievement of relevant national goals and realization of national interests in the information sphere. It is proposed to consider information security as a permanent process of activities of competent authorities, aimed at prevention, countering threats in the information sphere, the use of active measures of information influence, as well as a set of conditions of such activity, which are implemented and can be controlled for a long time.

Key words: *information, informational security, state information policy, threats to information security, National security, national security strategy.*