**УДК 004.056.5**
**ORCID ID: https://orcid.org/0000-0002-8442-7372**
**DOI https://doi.org/10.32703/2663-6352/2021-2-10-112-119**
***Белуга Юлія Миколаївна,***
*старший викладач кафедри*
*цивільного права і процесу*
*Юридичного факультету*
*Національного авіаційного університету,*
*м. Київ, Україна*

# ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

***Анотація:*** *У статті проаналізовано актуальні проблеми інформаційної безпеки як складової національної безпеки. Зазначені основні причини незадовільної ситуації у сфері інформаційної безпеки. Особлива увага приділяється поняттю інформаційної безпеки та визначенню її місця в системі забезпечення національної безпеки, а також зазначені основні проблеми у сфері правового регулювання відносин інформаційної безпеки. Успішний розвиток і саме існування України як суверенної держави неможливі без забезпечення її національної безпеки. Інформаційна безпека визначається ступенем захисту суспільства і держави, та як наслідок, стабільністю основних сфер життя щодо небезпечних, дестабілізуючих, деструктивних методів, що порушують інтереси країни інформаційних дій як при здійсненні, так і при пошуку.*

***Ключові слова:*** *інформація, безпека, інформаційна безпека, національна безпека, інформаційна сфера.*

***Annotation.*** *In protecting its information interests, each state must take care of its information security. The strengthening of Ukrainian statehood requires the same. Balanced state information policy of Ukraine is formed as an integral part of its socio-economic policy, based on the priority of national interests and threats to national security. From the legal point of view, it is based on the principles of a democratic state governed by the rule of law and is implemented through the development and implementation of relevant national doctrines, strategies, concepts and programs in accordance with applicable law. There is an objective need in Ukraine for state and legal regulation of scientific, technological and information activities that would meet the realities of the modern world and the level of information technology development, international law, but at the same time effectively protect Ukraine's own national interests. Relations related to information security, as the most important for society and the state today, require the fastest legislative regulation.*

*State information policy, as the activity of the system of public authorities and management in the information-psychological sphere, occupies a central place in the system of regulation as socio-political relations in the modern information society. Transparency of state information policy is the basis for ensuring socio-psychological stability and successful economic development of the country. The practice of information*

*and psychological influence is increasingly evolving in the modern world. The terms "information" and "psychological" wars are widely used by politicians and political scientists and are increasingly appearing in the context of information security issues in the country. Radical change of the state's approach to solving this problem should become one of the priorities in ensuring national security.*

***Key words**: information, security, information security, national security, information sphere.*

**Постановка проблеми.** Бурхливий розвиток інформаційних технологій наприкінці ХХ ст. призвів до зростання відносної важливості окремих аспектів суспільного життя. Внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. Організація соціуму почала трансформуватися у напрямку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками, зросла впливовість засобів масової інформації (ЗМІ). Інформатизація та комп'ютеризація докорінно змінюють обличчя суспільства. За таких обставин забезпечення інформаційної безпеки поступово виходить на перший план у проблематиці національної безпеки.

З огляду на сучасні тенденції суспільного розвитку національна безпека України не могла залишитися поза впливом внутрішнього інформаційного фактора. Адже в умовах інформаційного суспільства всі без винятку об'єкти національної безпеки (людина, суспільство, держава) стають чутливими до інформації, яка їх оточує. Таким чином, цілеспрямовано змінюючи інформацію, зафіксовану на певних носіях, керуючи каналами комунікації, впливаючи на технічні засоби обробки інформації, можна змінювати рішення, а відтак, і дії об'єктів національної безпеки [1, с. 23].

Водночас, об'єкти національної безпеки перебувають під впливом зовнішнього інформаційного фактора, що визначається змінами у сфері міжнародних відносин:

- руйнуванням біполярної моделі світу та формуванням поліполярної;
- виходом на міжнародну арену не лише окремих держав та їх об'єднань, а й таких нетрадиційних гравців, як, наприклад, транснаціональні корпорації, міжнародні терористичні рухи тощо;
- загостренням протиборства між традиційними та новими геополітичними центрами;
- інтенсифікацією глобалізаційних процесів, з одного боку, та зростанням тенденцій дезінтеграції, навіть у досить стабільних суспільствах, з іншого;
- перенесенням дій щодо розгортання та вирішення міжнародних конфліктів в інформаційний простір;
- переформатуванням інформаційного суспільства в інформаційно-комунікативне [2, с. 146].

**Аналіз останніх досліджень і публікацій**. Інформаційну безпеку, проблеми захисту національного інформаційного простору досліджували багато науковців. Зокрема, А. Марущак, В. Петрик, В. Ліпкан, Б. Кормич, В. Почепцов та інші фахівці. Проблемні питання забезпечення кібернетичної безпеки

досліджували Р. Лук'янчук, В. Бурячок, А. Бабенко, В. Гавловский, Д. Дубов, В. Номоконов, М. Погорецький, В. Шеломенцев та інші науковці.

**Мета дослідження.** В даному науковому дослідженні автор хоче окреслити сутність та особливості понять інформаційної безпеки, визначити актуальні проблеми в інформаційній сфері як складової національної безпеки України.

**Виклад основного матеріалу.** Одним з найвагоміших факторів у сфері державної безпеки є безпека інформаційного середовища, яка активно впливає на стан економічної, політичної, та інших складових державної безпеки України.

Інформаційна безпека є самостійною складовою національної безпеки, і в цьому проявляється її двохсторонній характер. Це обумовлено:

– прагненням кожної держави реалізувати та захистити власні національні інтереси, що направлені на формування та накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів;

– необхідністю не лише розвивати й посилювати національний інформаційний потенціал, але й захищати від широкого спектра існуючих і потенційних інформаційних загроз;

– існуванням реальної потреби в захисті всіх суб'єктів інформаційних відносин від можливих негативних наслідків упровадження та використання інформаційних технологій; – наявною можливістю інформаційного тиску на Україну, навіть інформаційної агресії з боку розвинутих країн світу з метою одержання односторонніх переваг у політичній, економічній, військовій та інших сферах, а також інформаційного впливу на свідомість і підсвідомість індивідів, на сім'ю, суспільство й державу, що загрожує державній безпеці [3, с. 87].

Національна безпека істотно залежить від забезпечення інформаційної безпеки, й у ході технічного прогресу ця залежність буде зростати. Визначень інформаційної безпеки на сьогодні існує досить багато. Лише в нормативних документах і в науковій літературі їх налічується шістнадцять. Єдиної думки про те, що таке інформаційна безпека немає. І в цьому, на нашу думку, головна проблема стану захисту інформації. Ми постійно говоримо про те, що інформаційна безпека забезпечується на належному рівні, але як ми можемо казати про це напевне, коли ми не маємо єдиних правил про те, що ми захищаємо, як захищаємо і від чого.

Проте, зробивши аналіз літератури можна зазначити, що поняття інформаційної безпеки можна разглядати у декількох аспектах.

Так інформаційна безпека – це:

- стан захищеності інформаційного середовища, який відповідає інтересам держави, який забезпечує формування, використання і можливості розвитку, незалежно від впливу внутрішніх і зовнішніх інформаційних загроз [4, с. 101];

- стан інформаційного середовища суспільства і політичної еліти, що забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства [5, с. 128];

Також з одного боку, інформаційну безпеку можна розглядати як самостійний елемент національної безпеки будь-якої країни, а з іншого –

інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо.

Найдоступнішим є таке визначення: інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [6]. Це визначення є оптимальним та відображає усі аспекти взаємодії суб'єктів інформаційних відносин.

Отже, інформаційна безпека суспільства, держави характеризується ступенем їх захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Загальноприйнятим є таке визначення інформаційної безпеки, як стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері [7, С.18] .

Ще однією проблемою є відсутність дієвих механізмів забезпечення інформаційної безпеки. Так, відповідно до Доктрини інформаційної безпеки України [8] актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

- інформаційне домінування держави-агресора на тимчасово окупованих територіях;

- неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері;

- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [8].

В частині 1 ст. 17 Конституції України зазначається, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Якщо ми кажемо про оборону країни, то захист її суверенітету, територіальної цілісності і недоторканості покладаються на Збройні Сили України.

Забезпечення державної безпеки і захист державного кордону України покладаються на відповідної військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом.

Збройні сили України так само зазначено що вони роблять, які формування мають право на існування, які ні. Але жодним чином не зазначена проблема, яка на сьогоднішній день є реальною загрозою не лише держави, а й нашого майбуття. Це відсутність жодних структур які б забезпечували саме інформаційну безпеку.

Для забезпечення інформаційної безпеки необхідно:

- Захистити інформацію під час її зберігання, оброблення і передавання мережею;
- Знайти і попередити порушення цілісності об'єктів даних;
- Захистити технічні пристрої і приміщення;
- Захистити програмні засоби від під'єднання програмних закладок і вірусів;
- Захистити конфіденційну інформацію від витоку і від вбудованих електронних пристроїв знімання інформації.

Проблемою залишається забезпечення належних темпів розвитку національних інформаційних ресурсів і відповідної інфраструктури. Остаточно не розв'язано в Україні також проблему впровадження сучасних інформаційно-аналітичних технологій державного управління, що негативно позначилося на взаємодії гілок влади, формуванні цілісної вертикалі ефективної виконавчої влади, дієвості політичних та економічних реформ, становленні громадянського суспільства та інших сферах суспільного життя [9].

Інформаційна безпека є однією з суттєвих складових частин національної безпеки країни. Її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії в значній мірі сприяла б забезпеченню досягнення успіху при вирішенні задач у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності.

Те, що відбувається зараз в країні стосовно проблем в інформаційній системі, призводить до необхідності захисту інформації.

Основні завдання інформаційної безпеки – це забезпечення:

- доступності інформації
- цілісності інформації
- конфіденційності інформації
- вірогідності інформації
- невідстежуваності дій користувача

Так, приведення в життя вдалої інформаційної політики, може суттєво вплинути на розв'язання внутрішньо політичних, зовнішньо політичних та військових конфліктів. У сфері інформаційної безпеки знання в будь-якій її формі, виступає з одного боку як об'єкт безпосереднього захисту, а з іншого як фактор забезпечення інтересів людини, суспільства та країни у будь-якій сфері її життєдіяльності на інформаційному рівні і в просторі.

Проблем інформаційної безпеки безліч. У цій сфері необхідно вирішувати питання, пов'язані з визначенням природи різних видів інформаційних небезпек (загроз), механізмів їхнього впливу на об'єкти інформаційної безпеки, можливих

наслідків цих впливів, шляхів і методів їх зменшення. З цієї низки проблем найбільш вивченими є проблеми, пов'язані із захистом інформації. Що ж до питань захисту людини, людських спільнот, суспільства в цілому, то з погляду розробки методології, шляхів, форм і методів забезпечення інформаційної безпеки вони вивчені недостатньо [10, с.121].

Особливо складна на сьогодні проблема завчасного створення засобів, необхідних для інформаційного протиборства, або, якщо користуватися американською термінологією, - «інформаційної війни» [11, с. 46].

У цій сфері розвитку озброєнь розглядаються два типи дій і, відповідно, дві групи засобів. Перша сукупність засобів зв'язку, що пов'язана з «інформаційною війною» як специфічним видом протиборства, можливо не пов'язаного з традиційними військовими діями, в особливій сфері, що називається «інфосферою». При цьому зачіпаються усі компоненти інформаційного потенціалу держав: інформація і її інформаційні носії, центри зосередження інформації; наукові і всі інші кадри — творці та споживачі інформації; технічні засоби збору, переробки, накопичення, збереження і передачі інформації; програмно-математичні засоби; інфраструктура всебічних систем управління; органи управління інформаційними ресурсами держави.

Хоча така війна буде вестись спеціальними структурами, у ній є суттєвий військовий аспект, поскільки можливі наслідки, що знизять бойові можливості збройних сил, а саме: блокування системи управління ракетно-ядерною зброєю та іншими стратегічними системами військового призначення; порушення роботи систем управління військово-транспортними перевезеннями та іншими системами забезпечення військових формувань (матеріалами, енергією, тощо); різке погіршення морально-політичної обстановки у військових формуваннях, серед їх резерву і зниження бойового духу особового складу внаслідок дезінформації, порушення систем забезпечення життєдіяльності, дезорганізації систем управління тощо.

**Висновки.** В даному дослідженні ми розглянули визначення інформаційної безпеки, побачили, що воно є комплексним і багатозначним. Інформаційна безпека є невід'ємною складовою національної безпеки. Саме тому різні органи державної влади мають приділяти особливу увагу ґарантуванню цієї безпеки, особливо в контексті неухильного руху розвинених суспільств до всеохоплюючої інформатизації всіх сфер їх життєдіяльності.

Особливо це стосується правоохоронних органів та органів безпеки, які мають не лише протидіяти інформаційним атакам всередині держави та на міжнародному рівні, в контексті інформаційної війни, а й бути готовими до боротьби з новою категорією злочинів: кіберзлочинами — правопорушеннями в сфері інформаційних технологій.

Отже, пріоритетними завданнями для суб'єктів забезпечення національної безпеки України в умовах глобального інформаційно-комунікативного суспільства є:

- стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоздатного національного інформаційного продукту, зокрема, сучасних засобів і систем захисту інформаційних ресурсів;

- забезпечення безпеки інформаційно-телекомунікаційних систем, які функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури;

- створення національної системи кібербезпеки, що потребує залучення суспільства, бізнесу й держави до активних дій з розбудови інформаційно-телекомунікаційної інфраструктури;

- чітке визначення місця й ролі кожного сектору (держави, бізнесу, громадськості) в процесі розвитку інформаційно-комунікативного суспільства, адже забезпечення інформаційної безпеки вимагає об'єднання зусиль різних державних і недержавних відомств, інститутів громадянського суспільства;

- підвищення рівня свідомості суспільства, зосередження ресурсів для розвитку інформаційно-комунікативного суспільства з метою досягнення національних пріоритетів. Подальші дослідження автора будуть спрямовані на розробку організаційно-правових засад реалізації зазначених завдань. [12, с.174]

Вважаємо, що на сьогоднішній день проблема інформаційної безпеки – одна з найактуальніших. Можна стверджувати, що нині в Україні все більшого забарвлення та гостроти набуває проблема забезпечення інформаційної безпеки. Тому необхідно докласти зусиль у вирішенні питань стратегій і тактики розвитку системи інформаційної безпеки, що надавало б можливість захистити людину, суспільство та державу.

**Література:**


1. Панченко В.М. Поняття інформаційної безпеки в сучасному юридичному дискурсі. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2 (2). С. 22-27.
2. Горошко Е.И. Информационно-коммуникативное общество в тендерном измерении. – Х. : ФЛП Либуркина Л.М., 2009. – 816 с.
3. Леонов А. П. Комп'ютерна злочинність і інформаційна безпека – Мінськ: АРІЛ, 2000.- 552 с.
4. Горова С. В. Особа в інформаційному суспільстві: виклики сьогодення. Монографія. Київ: НБУВ. Київ. 2017. 452 с.
5. Лужецький В.А., Войнович О.П., Дудатьєв А.В. Інформаційна безпека: навчальний посібник. Вінниця: УНІВЕРСУМ-Вінниця, 2009. 240с.
6. Захист інформаційної безпеки як функція держави URL: http://www.mego.info/матеріал/23 (дата звернення: 25.11.2021).
7. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління. *Аспекти публічного правління*. № 9. 2018. С.16-22.
8. Доктрина інформаційної безпеки України: Указ Президента України від 25 лютого 2017 р. № 47. URL: http://www.president.gov.ua/documents/472017-21374(дата звернення: 25.11.2021).
9. Загальні проблеми інформаційної безпеки URL: HTTPS://PIDRU4NIKI.COM/10560412/POLITOLOGIYA/ZAGALNI_PROBLEMI_INFORMATSIYNOYI_BEZPEKI (дата звернення: 25.11.2021).

10. Анісімов А. В. Інформаційна безпека: сутність та проблеми (матеріали круглого столу). URL: http://www.niurr.gov.ua/ukr/publishing/panorama3_ 4/kr_stil_a.htm#1. (дата звернення: 25.11.2021).
11. Роговец В. Информационные войны в современном мире: причины, механизмы, последствия. Персонал. 2000. №5. С.45-51.
12. Скулиш Є.Д. Інформаційна безпека: нові виклики інформаційному суспільству. *Інформація і право*. № 2(5). 2012. С.170-175.