УДК 321.7
DOI https://doi.org/10.24144/2307-3322.2022.76.2.39

# ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СТАН

**Кононенко В.П.,**
*доктор юридичних наук, доцент кафедри міжнародних відносин, міжнародної інформації та безпеки Харківського національного університету імені В. Н. Каразіна*
*https://orcid.org/0000-0002-6461-7072*

**Здоровко С.С.,**
*викладач кафедри міжнародних відносин, міжнародної інформації та безпеки Харківського національного університету імені В. Н. Каразіна*
*zdorovko@karazin.ua*

**Корольова А.Є.,**
*студентка кафедри міжнародних відносин, міжнародної інформації та безпеки Харківського національного університету імені В. Н. Каразіна,*
*alexandra.pushchayenko@gmail.com*

**Кононенко В.П., Здоровко С.С., Корольова А.Є. Інформаційна безпека як стан.**

Статтю присвячено вивченню проблеми національної та міжнародної інформаційної безпеки, яка є частиною загальної міжнародної безпеки та, на відповідному рівні, галуззю національної безпеки. Новітні загрози призвели до того, що зазначеним питанням почали опікуватись і регіональні міжнародні організації, і військово-політичні, такі, як ЄС та НАТО.

Інформаційний суверенітет держави – це її верховенство в інформаційній сфері на власній території та можливість безперешкодно та незалежно надавати об'єктивну інформацію про особливості внутрішньої та зовнішньої політики та події всередині держави назовні. При цьому верховенство держави в інформаційній сфері означає правове регулювання інформаційної діяльності, спрямоване на забезпечення конкуренції, безпеки та захисту економічних і соціальних інтересів держави, суспільства, прав та законних інтересів, життя і здоров'я людини шляхом законодавчого встановлення і контролю ліцензійних чи інших умов такої діяльності. Впровадження умов для інформаційної діяльності повинне забезпечувати дотримання принципів свободи вираження поглядів і переконань, свободи поширення, обміну та отримання інформації, права на інформацію, відкритості та доступності інформації, достовірності і повноти інформації, захищеності особи від втручання в її особисте та сімейне життя.

Інформаційну безпеку треба розуміти як стан, при якому за допомогою національних та міжнародних ресурсів забезпечується захист від інформаційного впливу на свідомість особи та суспільства, унеможливлюється інформаційний вплив на прийняття рішень державними інститутами, а також недоторканість приватних і державних цифрових баз даних, можливість їх швидкого відновлення у випадку протиправного посягання і забезпечення покарання зловмисників.

На міжнародному рівні стан інформаційної безпеки передбачає захист від інформаційного впливу на свідомість суспільства та прийняття рішень державами та міжнародними організаціями, а також недоторканість приватних, державних та міжнародних цифрових баз даних, можливість їх швидкого відновлення у випадку протиправного посягання і забезпечення покарання суб'єктів таких посягань.

**Ключові слова:** інформаційний суверенітет, інформаційна безпека НАТО, гібридна війна

**Kononenko V., Zdorovko S., Korol'eva A. Information security as a special state.**

The article is devoted to the study of the problem of national and international information security. It is part of general international security and, at the corresponding level, a branch of national security. The

latest threats led to the fact that regional international organizations, such as the EU and military-political organizations - NATO, began to take care of the mentioned issue.

Information sovereignty is the supremacy of the state in the information sphere on its own territory. As well as the opportunity to freely and independently provide objective information about the peculiarities of internal and external policy and events within the state to the outside world.

The supremacy of the state in the information sphere means the regulation of information activities aimed at ensuring the security and protection of the economic and social interests of the state, society, rights and legitimate interests, human life and health. This is done through the legislative establishment and control of licensing or other conditions of such activity. The implementation of conditions for information activity must ensure compliance with the principles of freedom of expression of views and beliefs, freedom of distribution, exchange and receipt of information, right to information, openness and availability of information, reliability and completeness of information, protection of a person from interference in his personal and family life.

Ensuring information security in the state directly affects the economic, military and political spheres of its life. Legal uncertainty at the global level and the lack of unified positions forces state governments to form digital security policies at the national level.

The informational component is a part of modern hybrid wars – both as a cover and as a means of direct influence on the enemy.

Information security should be understood as a state in which, with the help of national and international resources, protection against informational influence on the consciousness of individuals and society is ensured, and informational influence on decision-making by state institutions is prevented. As well as the inviolability of private and state digital databases, the possibility of their quick recovery in the event of illegal encroachment and ensuring the punishment of perpetrators is guaranteed.

At the international level, the state of information security involves protection against informational influence on public consciousness and decision-making by states and international organizations. As well as the inviolability of private, state and international digital databases, the possibility of their quick recovery in case of illegal encroachment and ensuring the punishment of the subjects of illegal encroachments.

**Keywords:** information sovereignty, NATO information security, hybrid warfare.

**Постановка проблеми**. Останнім часом значно зростає інтенсивність споживання інформації в усіх галузях життя – науково-технічній, соціальній, економічній тощо. Процеси збору, накопичення, переробки та розповсюдження інформації стають звичайним процесом в діяльності медицини, освіти, управління, оборони. Тим часом інформація має і дестабілізуючий потенціал через її майже необмежені можливості впливу на людину і суспільство [1, с. 6].

І цей вплив не завжди є мирним, у зв'язку з чим з'явилися такі поняття, як «кібербезпека» та «інформаційна безпека». Особливої актуальності проблема інформаційної безпеки набуває в умовах трансформації системи міжнародних відносин, зростання ролі засобів збройного насильства у реалізації геополітичних стратегій і забезпеченні національних інтересів держав [2, с. 13-14]. Складність формулювання поняття «інформаційна безпека» полягає в тому, що сам предмет, безпека якого визначається, не окреслений як за внутрішньою структурою, так і за внутрішніми властивостями.

**Стан опрацювання проблематики.** Загальні питання безпеки висвітлювали в своїх працях В. Антипенко, О. Бєглий, І. Лукашук, А. Назаренко, Л. Тимченко та ін. Міжнародно-правові проблеми забезпечення глобальної безпеки на сучасному етапі вивчала Н. Ємельянова. Про інформаційний суверенітет також пише і О. Вайцеховська.

Проблемам правового регулювання інформаційної безпеки присвятила монографічне дослідження А. Нашинець-Наумова.

Довгань О., Доронін І. надали аналіз кіберзагроз національним інтересам України та розробили правові аспекти кіберзахисту.

Визначення даної категорії розробляли В. Лук'янова, А. Лаутар, П. Біленчук, Д. Дубов, М. Ожеван, К. Ісмайлов.

Питання інформаційної війни вивчали західні науковці K. Wesolowski, C. Perez, A. Nair, F. Paziuk, B. Lewis, G. Wilde, J. Sherman.

**Метою статті** є дослідження особливостей забезпечення інформаційної безпеки на національному та міжнародному рівні, визначення понять «інформаційний суверенітет держави», «національна інформаційна безпека», «міжнародна інформаційна безпека».

**Виклад основного матеріалу**. З огляду на значний розвиток інформаційно-комунікаційних технологій, загальну діджіталізацію, з'явились принципово нові категорії – інформаційне суспільство, кіберпростір. Саме створення інформаційного суспільства призвело до виникнення багатьох загроз у важливих сферах життя суспільства, тому інформаційну безпеку є підстави вважати окремим елементом національної безпеки [3, с. 284]. Кожна держава або група держав виробляє власну стратегію поведінки та внутрішню і зовнішню політику інформаційної безпеки, що відповідають сучасним умовам розвитку комунікацій. Так, Європі характерні пошуки балансу між державним інтересом та захистом прав людини і бізнесу від надмірного втручання [4, с. 20-21]. Державна інформаційна політика повинна бути збалансованою і формуватися як об'єктивна складова її національної безпеки, а також бути частиною загальної політики, виходячи з головних національних інтересів. Вона має ґрунтуватися на правових демократичних засадах і впроваджуватись шляхом розробки та реалізації відповідних національних доктрин, стратегій та програм згідно із нормами національного та міжнародного права [5, с. 68].

В. Лук'янова та А. Лаутар пишуть, що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. Під інформаційним середовищем розуміють сферу діяльності учасників інформаційних відносин, пов'язану зі створенням, зміною і споживанням інформації. Дане середовище умовно поділяється на три основні предметні частини: створення і розповсюдження первинної та вторинної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації та дві забезпечувальні предметні частини: створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення, а також забезпечення недоторканості інформації (інформаційної безпеки) [6, с. 97].

П. Біленчук щодо визначення даної категорії має абсолютно співпадаючу думку – він так само говорить про стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах особи, суспільства, держави. Дана категорія включає в себе сукупність організаційних, соціально-економічних, правових механізмів, що працюють на забезпечення сталого розвитку суспільства і держави [7, с. 64].

Безпека в інформаційній сфері, на думку П. Біленчука, передбачає забезпечення інформаційного суверенітету; удосконалення державного регулювання даного питання шляхом створення фінансових і правових умов для вироблення і застосування сучасних технологій, доступу до публічної інформації, розвитку державної інформаційної інфраструктури при запобіганні свавільному втручанню органів влади у функціонування ЗМІ; забезпечення захисту національного інфопростору та недопущення монополії держави в інформаційній сфері [7, с. 54-55]. Про інформаційний суверенітет також пише і О. Вайцеховська [8, с. 243].

Нормативна дефініція «інформаційний суверенітет держави» була надана в Законі України «Про Національну програму інформатизації» від 1998 р., згідно з яким – це здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави.

Але зазначений Закон втратив чинність на підставі Закону України «Про Національну програму інформатизації» від 01.12.2022 р., в якому дана категорія вже не згадується.

Ми вважаємо, що інформаційний суверенітет – це верховенство держави в інформаційній сфері на власній території та можливість безперешкодно та незалежно надавати об'єктивну інформацію про особливості внутрішньої та зовнішньої політики та події всередині держави назовні.

При цьому верховенство держави в інформаційній сфері означає регулювання інформаційної діяльності, спрямоване на забезпечення безпеки та захисту економічних і соціальних інтересів держави, суспільства, прав та законних інтересів, життя і здоров'я людини шляхом законодавчого встановлення і контролю ліцензійних чи інших умов такої діяльності. Впровадження умов для інформаційної діяльності повинне забезпечувати дотримання принципів свободи вираження поглядів і переконань, свободи поширення, обміну та отримання інформації, права на інформацію, відкритості та доступності інформації, достовірності і повноти інформації, захищеності особи від втручання в її особисте та сімейне життя.

Забезпечення безпеки процесів обміну інформацією має велике значення як для окремої країни, так і міжнародного співтовариства взагалі, тому потрібно розглядати інформаційну безпеку не тільки в конкретно-прикладних аспектах, а як сталий і безпечний стан всієї соціальної системи.

Це гарантує ефективне функціонування та розвиток як інформаційної сфери, так і соціуму [9, с. 3-4].

Важливу участь у безпекових заходах щодо інформаційної сфери традиційно приймає ООН. Її діяльність у даному напрямку стосується розробки міжнародно-правової бази та розробки положень з метою протидії незаконному застосуванню науково-технологічного прогресу в своїх цілях терористичними угрупованнями та організованою злочинністю. Питання інформаційної безпеки в контексті формування сталого глобального інформаційного суспільства є актуальною і для роботи низки спеціалізованих установ ООН [10, с. 4].

В сучасному світі, в якому дедалі більшу роль у житті держави, її економіці та системі безпеки, відіграють кіберпростір та сучасні інформаційні технології, не можна обійти увагою ті загрози, які пов'язані з застосуванням цих високих технологій [11, с. 332]. Проблеми міжнародної інформаційної безпеки упродовж 1998-2015 рр. періодично дискусувались на Генеральній Асамблеї ООН. Розроблялись нові міжнародні документи на основі резолюцій «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» та «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки», в яких містилися положення щодо застосування новітніх технологій у цивільній і у воєнній сферах, про роботу з сучасними досягненнями науки і техніки у модернізації сучасних озброєнь, про важливість протидії деструктивним інформаційним впливам [12, с. 103]. Міжнародна інформаційна безпека визначається ООН як стан міжнародних відносин, що виключає порушення світової стабільності і створення загрози безпеці держав і світової спільноти в інформаційному просторі [13, с. 61]. Враховуючи поширення інформаційних правопорушень, Генеральна Асамблея ООН у 2019 р. ухвалила резолюцію  під назвою «Заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки», в якій фіксується необхідність створення безпечного, відкритого, доступного, стабільного, і мирного інформаційно – комунікаційного середовища, встановлення відповідальних відносин між державами, розширення можливостей урядів щодо співпраці і просування сучасних технологій, що сприятимуть зменшенню можливості активізації конфліктів. Крім того, під егідою ООН створено Групу високого рівня з питань загроз, викликів і змін, а також розглядається можливість створення єдиного координатора ООН по боротьбі з тероризмом, комісії із світобудівництва.

На рівні Європи до останнього часу проблема інформаційної безпеки вирішувалась лише частково – у сфері протидії кіберправопорушенням. Так, у 2001 р. Радою Європи була прийнята Конвенція про кіберзлочинність (ратифікована Україною 7 вересня 2005 р., що відносила до сфери кіберправопорушень такі дії. 1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ до мереж; незаконне отримання цифрових даних; втручання в комп'ютерні дані; втручання у комп'ютерну систему; зловживання пристроями. 2. Правопорушення, пов'язані з комп'ютерами: підробка та шахрайство, пов'язані з використанням комп'ютерів. 3. Правопорушення, пов'язані з наповненням інфорації: наприклад, дитяча порнографія. 4. Пов'язані з порушенням авторських та суміжних прав. Правова невизначеність на світовому рівні та відсутність єдиних позицій змушує уряди держав формувати політику цифрової безпеки на національному рівні. Більшість держав світу створюють численні правоохоронні служби та військові підрозділи, призначені для протидії цифровим загрозам [14, с. 3-4]. Так само і в Європейському Союзі у 2004 р. було створено Європейське агентство з мережевої та інформаційної безпеки. У 2012 р. це Агентство оприлюднило огляд «Національні стратегії кібербезпеки. Практичний посібник з розвитку та виконання», в якому зазначено, що в національних стратегіях не існує загальноприйнятого та однозначного визначення категорії «кібербезпека» [15, с. 16]. Д. Дубов, М. Ожеван ототожнюють кібербезпеку з інформаційною безпекою [14, с. 4].

З урахуванням тієї обставини, що ефективність забезпечення інформаційної безпеки в європейському цифровому просторі також залежить від плідної співпраці держав та міжнародних органів у 2013 р. в структурі Європола (Європейського поліцейського офісу) був утворений Європейський центр боротьби з кіберзлочинністю. Розуміючи важливість забезпечення цифрової безпеки як складової системи безпеки національної, більшість держав світу почали здійснювати внутрішньодержавні заходи з інформаційної безпеки. Зокрема, ці дії пов'язані з розробкою і вдосконаленням національного правового поля в даній галузі і створенням спеціалізованих органів, що контролюють безпеку в кіберпросторі [3, с. 285]. Що особливо є важливим з урахуванням того, що інформаційна складова є частиною сучасних гібридних війн – як у якості прикриття, так і засобом безпосереднього пливу на супротивника.

Як приклад можна навести твердження НАТО, що Росія досягла своїх цілей у Криму в 2014 р. завдяки поєднанню таких різних факторів, як: російський спецназ, місцеві озброєнні угрупування, економічний вплив, інформаційна війна та дезінформація, експлуатація соціально-політичної поляризації [16]. Так, на думку В. Горбуліна, успіх у гібридній війні є наслідком використання комплексу факторів: стратегії і тактики, інформаційного впливу і своєчасної фізичної реалізації створеної за допомогою підготовчих дій сприятливої ситуації. Так, анексія території АР Крим багато в чому була вдалою завдяки тривалій інформаційної та політичної підготовки, а також ідеально вибраному моменту для її реалізації. Це, зокрема: ослаблення центральної влади та часткове «безвладдя» на тлі зміни влади; зростання суперечностей (а швидше – актуалізація вже наявних) між Центром і регіонами; незадовільний психологічний і матеріально-технічний стан українських безпекових структур; антагонізм між різними силовими структурами; особливо активна інформаційно-пропагандистська робота [див.: 17].

Тому забезпечення інформаційної безпеки у державі безпосередньо впливає на економічну, військову та політичну сфери її життєдіяльності [18, с. 93]. Найбільш ефективними прийомами інформаційних атак є: дезінформація, залякування, схематизм, глузування, вклинювання, фальшування. З метою введення противника або цільові групи, що визначені як мішень для атаки, застосовується дезінформація – надання хибної інформації.

І сьогодні дезінформація стала справжнім викликом для усього демократичного світу. Вона підриває довіру до державних та правових інституцій, провокує та загострює конфлікти в суспільстві та є перешкодою розвитку правової системи та держави загалом [19, с. 38]. Але протистояти таким масованим інформаційним атакам самотужки майже не можливо. Тому великого значення для протидії інформаційній агресії набуває діяльність міжнародних організацій, за якими стоїть потенціал держав – учасниць. Серед міжнародних організацій, основною метою яких є саме безпека, НАТО найбільш ефективно змінила політику щодо інформаційної безпеки. Організація заснувала центри у державах-членах як багатонаціональні інститути для розробки доктрини цифрової безпеки, вдосконалення міждержавної взаємодії, впровадження теоретичних напрацювань у практиці протидії цифровим загрозам, обміну досвідом захисту інформації між країнами-членами та країнами-партнерами. Зараз ентр кібербезпеки НАТО функціонує в Естонії, він не входить до структури збройних сил НАТО, його фінансування забезпечується державами-спонсорами та державами-членами НАТО [20, с. 353-358].

Важливу роль у зміцненні кібербезпеки, безпеки інформаційно-комунікаційних технологій відіграє ОБСЄ, працюючи над зниженням ризиків виникнення конфліктів між державами в результаті використання інформаційних технологій. Ключовою проблемою в цьому відношенні є практична реалізація відповідних директив ООН групами урядових експертів на регіональному рівні. Для розробки сумісного підходу ОБСЄ до проблем кібербезпеки та визначення завдань ОБСЄ, у Відні 9-10 травня 2011 р. було проведено конференцію «Загальний підхід до кібербезпеки: визначення майбутньої ролі ОБСЄ». У 2013 р. ОБСЄ прийняла інноваційні рекомендації про заходи щодо зміцнення довіри у сфері кібербезпеки, спрямовані на підвищення прозорості та забезпечення безпеки в регіоні, які передбачали взаємодію з приватними компаніями і провайдерами найважливішої інфраструктури, а також спільні підходи до управління кібербезпекою [21].

На думку К. Ісмайлова, термін «інформаційна безпека» на даний момент часу не є коректним по своїй суті. Замість нього він пропонує вживати термін «інформаційна захищеність» і використовувати для нього таке визначення: інформаційна захищеність – це захист конфіденційності, цілісності та доступності інформації [22, с. 32-33].

На нашу думку, захист конфіденційності, цілісності та доступності інформації є засобами забезпечення інформаційної безпеки.

**Висновки:** національну інформаційну безпеку треба розуміти як стан, при якому за допомогою національних та міжнародних ресурсів забезпечується захист від інформаційного впливу на свідомість особи та суспільства, унеможливлюється інформаційний вплив на прийняття рішень державними інститутами, а також недоторканість приватних і державних цифрових баз даних, можливість їх швидкого відновлення у випадку протиправного посягання і забезпечення покарання зловмисників.

І, відповідно, на міжнародному рівні стан інформаційної безпеки передбачає захист від інформаційного впливу на свідомість суспільства та прийняття рішень державами та міжнародними організаціями, а також недоторканість приватних, державних та міжнародних цифрових баз даних,

можливість їх швидкого відновлення у випадку протиправного посягання і забезпечення покарання суб'єктів таких посягань.

**Список використаних джерел:**


1. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: «Гельветика», 2017. 168 с.
2. Лук'яненко В.В. Соціально-правове забезпечення інформаційної безпеки України. V Міжнародна наукова конференція Харківського національного університету Повітряних Сил імені Івана Кожедуба «Сучасна війна: гуманітарний аспект»: збірник матеріалів, 25-26 травня 2021 р. Х.: Факт, 2021. С. 13–18.
3. 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.
4. Парахонський Б.О. Зовнішня політика України в умовах кризи міжнародного безпекового середовища: аналіт. доп. К.: НІСД, 2015. 100 с.
5. Бондар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.
6. Лук'янова В.В., Лаутар А.Ю. Інформаційна безпека в умовах розвитку інформаційної системи. Вісник Хмельницького національного університету. 2013. № 2. Т. 3. С. 97–101.
7. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків. 2018. 289 с.
8. Вайцеховська О.Р. Міжнародний фінансовий правопорядок: теоретичні засади та актуальні проблеми в умовах глобалізації. Дис. … докт. юрид. наук. Харків. 2020. 472 с.
9. Манжуева, О.М. Феномен информационной безопасности: сущность и особенности: автореф. дис. … д-ра филос. наук. Улан-Удэ. 2015. 25 с.
10. Фролова О.М. Роль ООН в системі міжнародної інформаційної безпеки. Електронне видання Інституту міжнародних відносин. 2018, № 18. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140 (дата звернення: 30.03.2023).
11. Тимченко Л.Д., Кононенко В.П. Міжнародне право: підручник. Київ: Знання, 2012. 631 с.
12. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. Політичне життя. № 1. 2020. С. 102–109.
13. Болгов Р.В. Деятельность ООН в области информации и международные аспекты информационной безопасности России. Сравнительная политика. 2019. № 1. С. 59–69.
14. Дубов Д.В., Ожеван М.А. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців: аналітична доповідь. НІСД. 2012. 28 с.
15. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки: монографія. К. 2017. Видавничий дім «АртЕк». 107 с.
16. Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-theantidote/index.html (дата звернення: 30.03.2023).
17. Горбулін В.П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Видавництво: НІСД. 2014. С. 5–12.
18. Тригубенко М.В. Сучасні виклики у сфері інформаційної безпеки в державному управлінні. Актуальність та особливості наукових досліджень в умовах воєнного стану: збірник тез Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки - 2022 в Україні (м. Київ, 24 травня 2022 р.). Київ: ДНДІ МВС України, 2022. С. 93–96.
19. Самчинська О.А. Правова культура громадян як складова системи протидії дезінформації. Правове регулювання суспільних відносин в умовах воєнного стану та післявоєнної відбудови з метою забезпечення сталого розвитку: матеріали XI Міжнародної наук.-практ. конф. (м. Київ, 9 грудня 2022 р.). Упоряд: Бевз С.І., Бирса Н.О., Серебрякова Ю.О. Київ: КПІ ім. Ігоря Сікорського. 2022. С. 35–38.
20. Кононенко В.П, Новікова Л.В., Копицька П.О. Політика міжнародних організацій з питань інформаційної безпеки. Науковий вісник Ужгородського національного університету. Серія Право. 2021. № 65. Т. 1. С. 353–358.

21. Organization for Security and Co-operation in Europe – OSCE. URL: https://www.osce.org/whatis-theosce (дата звернення: 30.03.2023).
22. Ісмайлов К.Ю. Поняття «кібезбезпека та «інформаційна безпека». Типологія безпеки. Міжнародна науково-практична конференція «Актуальні проблеми автоматизації та управління». Луцьк. 2016. С. 32-33.