

УДК 351:342

DOI [https://doi.org/10.32689/2523-4625-2024-1\(73\)-6](https://doi.org/10.32689/2523-4625-2024-1(73)-6)

**Валерій КОТЛЯРОВ**

докторант, Національний авіаційний університет, kotva0503@gmail.com

ORCID: 0000-0002-2291-3199

## ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВІТЧИЗНЯНОЇ ТА СВІТОВОЇ СПІЛЬНОТИ

*У статті досліджується стан інформаційної безпеки України в умовах російської військової агресії. Аналізуються можливості реалізації цілей, зазначених у Стратегії інформаційної безпеки України, за умов воєнного стану. Показано, що національні інтереси України вимагають забезпечення сприятливих умов політичного розвитку країни. Так, інтереси особи полягають у реальному забезпеченні політичних прав і свобод громадян, суспільство потребує зміцнення демократії, а інтереси держави виражаються у необхідності ефективного захисту конституційного ладу суверенітету та територіальної цілісності країни, встановлення та підтримання політичної стабільності, включаючи стабільність державної влади та її інститутів. В інформаційній сфері на основі національних інтересів України формуються стратегічні та поточні завдання політики держави щодо забезпечення інформаційної безпеки. Доведено, що ефективна інформаційна діяльність може суттєво поліпшити зусилля держави щодо мирного вирішення кризових ситуацій. І навпаки, ігнорування інформаційних чинників, а часто й навмисне змінені інформація здатні спровокувати найрадикальніші настрої, спалахи ворожості та призвести до катастрофічних наслідків.*

*Аргументовано, що застосування інформаційних технологій військовими відкрило нові можливості щодо забезпечення оборони держави. Володіння інформаційними ресурсами та його захист у військовій сфері стали таким самим неодмінним атрибутом, як озброєння, боєприпаси, транспорт тощо. Виграш України в інформаційному протистоянні під час війни з росією сприятиме досягненню її стратегічних цілей. Обґрунтовано, що у Стратегії інформаційної безпеки України відображено інтереси держави, які виражаються у необхідності ефективного захисту конституційного устрою суверенітету та територіальної цілісності країни, встановлення та підтримання політичної стабільності, включаючи стабільність державної влади та її інститутів. Аналіз ходу реалізації цілей Стратегії показав, що цей процес не зупиняється, незважаючи на всі труднощі воєнного стану.*

**Ключові слова:** інформаційна безпека, Стратегія інформаційної безпеки України, національні інтереси держави, інформаційні технології, інформаційне протистояння.

### Valerii Kotliarov. INFORMATION SECURITY OF THE DOMESTIC AND GLOBAL COMMUNITY

*The article examines the state of information security of Ukraine in the conditions of Russian military aggression. The possibilities of realizing the goals specified in the Information Security Strategy of Ukraine under the conditions of martial law are analysed. It is shown that the national interests of Ukraine require the provision of favourable conditions for the country's political development. Thus, the interests of the individual consist in the real provision of political rights and freedoms of citizens, society needs to strengthen democracy, and the interests of the state are expressed in the need to effectively protect the constitutional system of sovereignty and territorial integrity of the country, establish and maintain political stability, including the stability of state power and its institutions. In the information sphere, on the basis of the national interests of Ukraine, strategic and current tasks of the state policy on ensuring information security are formed. It has been proven that effective information activities can significantly improve the state's efforts to resolve crisis situations peacefully. Conversely, ignoring informational factors, and often deliberately altered information, can provoke the most radical attitudes, outbursts of hostility and lead to catastrophic consequences.*

*It is argued that the use of information technologies by the military has opened up new opportunities for ensuring the defence of the state. Possession of information resources and its protection in the military sphere have become the same indispensable attribute as weapons, ammunition, transport, etc. Ukraine's victory in the information conflict during the war with Russia will contribute to the achievement of its strategic goals. It is substantiated that the Information Security Strategy of Ukraine reflects the interests of the state, which are expressed in the need to effectively protect the constitutional system of sovereignty and territorial integrity of the country, establish and maintain political stability, including the stability of state power and its institutions. The analysis of the implementation of the Strategy's goals showed that this process does not stop, despite all the difficulties of the martial law.*

**Key words:** information security, Information Security Strategy of Ukraine, national interests of the state, information technologies, information struggle.

**Постановка проблеми.** Проблема становлення інформаційного суспільства. Зауважимо, що аналіз низки нормативно-правових актів та планів дій у сфері становлення інформаційного суспільства

забезпечення інформаційної безпеки Європейського Союзу (надалі ЄС), розглядається поряд з іншими проблемами

ЄС, дозволив дійти висновку про значно вужче розуміння поняття «інформаційна безпека» як щодо українського, так і до міжнародного законодавства. Забезпечення інформаційної безпеки було визнано глобальною проблемою сучасності відповідно до Резолюції 54/49 ООН «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» від 1 грудня 1999 року [1]. Представники різних країн наголошували, що використання нових інформаційних технологій і засобів впливу високорозвинених країн на менш технологічні країни світу призвело до зміни глобального і регіонального балансу сили, обумовило нові сфери конфронтації між традиційними і новими центрами глобального протистояння, уможливило досягнення переваг в інформаційних технологіях і засобах маніпулювання суспільною свідомістю для широкомасштабної експансії із застосуванням не обмежених міжнародним правом видів озброєнь [2].

Отже, актуальність таких проблем, як інформаційно-технологічний дисбаланс, інформаційна ізоляція окремих регіонів, країн, а також негативний вплив інформаційних технологій, акцентується не тільки ЮНЕСКО, а й іншими міжнародними організаціями, зокрема ООН.

Проблема теоретико-правових засад забезпечення інформаційної безпеки ЄС у вітчизняній науковій літературі достатньо ґрунтовно не досліджувалась. Вона розглядалася лише через висвітлення окремих її аспектів вітчизняними та зарубіжними фахівцями інформаційного права, національної безпеки, а саме: С.С. Алексєєв, А.В. Баровська, І.Л. Бачило, В.Т. Білоус, В.Д. Гавловський, В.О. Голубєв, С.Ф. Гончар, В.М. Горючий, І.Г. Грабар, Р.В. Гришук, М.В. Гуцалюк, Ю.І. Данько, О.П. Дубас, Р.А. Калюжний, А.М. Колодій, М.Ю. Комаров, В.О. Копилов, В.А. Ліпкан, В.В. Макаренко, Є.А. Макаренко, Н.Р. Нижник, А.В. Ониськова, В.М. Петренко, Н.П. Резнік, А.О. Селіванов, І.Г. Ханін, В.С. Цимбалюк, М.Я. Швець, Ю.С. Шемшученко, О.К. Юдін, В.І. Ярочкін та інші.

**Метою статті** є визначення пріоритетних напрямів удосконалення забезпечення інформаційної безпеки України та світової спільноти.

**Виклад основного матеріалу.** Як свідчать дослідження, безпека інформаційних систем не зводиться до звалювання в одну кучу (сукупність) засобів, способів і методів захисту. Враховуючи суспільну

значимість категорія «інформаційна безпека» у нормативно-правовому аспекті має конституційний статус. У системі юридичних норм України вона знайшла відображення у статті 17 Конституції України.

Інформаційна безпека – невід’ємна частина політичної, економічної, оборонної та інших складових національної безпеки. З метою зменшення ентропії щодо сутності та змісту законодавець визначає орієнтовний перелік об’єктів інформаційної безпеки. Об’єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни.

Інформаційне забезпечення безпеки суспільства, держави та особистості буде міцним та надійним тоді, коли воно спирається на такі ціннісні підстави, як інформаційна цивілізованість, інформаційна культурність. Сучасна історична обстановка свідчить про те, що параметри інформаційної безпеки, стереотипи та звички в цій сфері, що склалися, значною мірою не відповідають завданням забезпечення національної безпеки.

Інформаційне забезпечення безпеки України тісно пов’язане з його включенням до технологічної співпраці у глобальному масштабі. Концепція національної безпеки України має включати і концепцію інформатизації суспільства, оскільки загрози безпеці, викликані відсутністю сучасних засобів інформаційного забезпечення в галузі економіки, екології, охорони здоров’я, соціального забезпечення, у багато разів перевищують допустимі витрати на їхню інформатизацію [3].

Устаткування інформаційними центрами здатне забезпечити миттєву та повну дезорганізацію суспільного життя. Створення єдиної міжнародної інформаційної системи ставить країни-учасниці у залежність від обслуговуючого персоналу інформаційних центрів: інженерів, програмістів, операторів, наділених усіма людськими якостями, зокрема і недоброросвісністю, неделікатністю. Небезпечний момент, пов’язаний з інформацією, – надмірна відкритість нашого суспільства.

Зростаюча небезпека для особистості, суспільства, держави представляє також новий вид соціально-небезпечних злочинів, заснованих на використанні сучасної інформаційної техніки та технології. Основні види цих злочинів включають махінації з електронними грошима; комп’ютерне

хуліганство; розкрадання різноманітної інформації, що зберігається або передається у «безпаперовому» вигляді, незаконне її копіювання тощо [4].

Бурхливий розвиток спеціальних технічних засобів нового покоління, які здатні впливати на психіку, свідомість людей та на інформаційно-технічну інфраструктуру суспільства та армії, досяг такого рівня, що їх характеризують як новий клас зброї – електронну чи інформаційну зброю.

Інформаційна зброя включає різні засоби нападу на комп'ютерні мережі, починаючи з електронного шпигунства до вірусів, здатних руйнувати ключові системи. До нього належать програмні засоби (комп'ютерні віруси, програмні закладки тощо), засоби радіоелектронної боротьби, психотронні генератори тощо.

Застосування та розробка різних видів інформаційної зброї здійснюється все частіше та ширше. Подекуди інформаційний тероризм став елементом державної політики. За даними ЦРУ США не менше 30 країн активно працюють над комп'ютерними програмами, що є інформаційною зброєю.

Причому об'єктами для такої зброї все частіше стають окремі особи, соціальні групи, а не лише маси та державні структури, як це було нещодавно. Інакше кажучи, вибірковість цієї зброї зростає.

Відмінною рисою такої зброї є її дешевизна та складність виявлення. Система «Інтернет», що зв'язала комп'ютерні мережі по всій планеті, змінила правила сучасної зброї. Анонімність, що забезпечується Інтернетом, дозволяє противнику стати невидимим, виявити його дуже складно.

З іншого боку, сучасні військові дії – це не лише вогневе (речовинно-енергетичне), а й інформаційно – технічне протистояння. У військовій справі настає новий, пост'ядерний етап, розгортається нова військово-технічна революція, перехід від зброї масової поразки до високоточної, виборчої контрсилової та інформаційної зброї [5].

Навіть поверховий розгляд проблем інформаційної культури та їхнього впливу на інформаційне забезпечення безпеки безпеку особистості, суспільства та держави дозволяють зробити деякі узагальнення у цьому напрямі.

По-перше, чинник інформаційності та інформатизації став настільки всеосяжним, що потребує тісного практичного поєднання з тим, що вводить його реалізацію у певні межі – правові, гуманітарні, моральні, демократичні. Без цих рамок, характер яких визначається

національно-державними умовами конкретної країни, інформаційність поступово генерує антисоціальні прояви, а отже, стає джерелом соціальної та особистісної небезпеки.

По-друге, надійне інформаційне забезпечення безпеки держави та особистості вже неможливе без урахування та цілеспрямованого культивування зрілої інформаційної культури на всіх рівнях соціальної організації. Культурний «вимір» всього процесу інформатизації та інформаційного забезпечення безпеки означає, що фактор інформатизації тісно поєднується з ціннісно-ментальними підставами, іншими результатами освіти та виховання, які визначають та спрямовують можливості інформатизації у соціально та особистісно-значущі межі реалізації.

По-третє, з погляду інформаційної культури стає відмінним, що інформаційність – якісно нова і ще недостатньо освоєна особистістю і суспільством сфера соціальності та соціалізації, яка об'єктивно діє з усіма наслідками, що з цього випливають. Для суспільства важливо глибоко освоїти цю сферу як джерело соціалізації, дослідити особливості її впливу на особистість та соціальні групи, визначити наслідки цього впливу та постаратися зробити цей вплив керованим та регульованим. У протилежному випадку процес інформатизації набуде (і вже багато в чому набув) власної логіки, в якій інтереси суспільства та особистості, їхня безпека далеко не гарантовані. Проблема дослідження можливостей мережевих засобів масової комунікації особливо актуальна на сьогодні. Це зумовлено тим, що в умовах економічного спаду, політичної нестабільності та загострення протиріч між інтересами різних груп населення без розуміння ролі, значення та функцій сучасних засобів комунікації неможливе ефективне управління соціально-політичними процесами від розумності та виваженості політики у галузі розвитку мережевих комунікацій, а також виробництва інформації та її поширення у глобальному інформаційному просторі значною мірою залежить благополуччя країни та її місце у світовій цивілізації [6].

З іншого боку, зміни, що відбуваються у суспільстві під впливом мережевих засобів масової комунікації, не обмежуються лише певними перевагами та вигодами, що відкриває найширші можливості для ведення інформаційного протистояння у соціально-політичній сфері. Інформаційний тероризм, поширення нелегальних матеріалів, освіта в мережі неформальних молодіжних об'єднань,

деструктивний вплив нових комунікаційних технологій на особистість – це також атрибут існування мережевих засобів масової комунікації.

Сьогодні мережні засоби масової комунікації є новою історичною формою забезпечення взаємодії людей, а Інтернет виступає як основа формування єдиного електронного комунікаційного середовища, соціально-політичний сенс якого полягає у можливості створення системи, що знаходиться над національними культурами, цивілізаціями та державами та здатної якісно змінити світ, хоча розширення соціальних функцій системи масової комунікації у своїй немає. Характер і розвиток цього обнадійливого та водночас небезпечного явища залежить від світових соціальних і політичних процесів, і, у свою чергу, надає на них певний вплив.

Говорячи про інформаційне забезпечення безпеки, пов'язане з функціонуванням мережевих комунікацій і, перш за все, «Інтернет», як нової форми комунікації, доцільно відзначити одночасно як позитивні, так і негативні властивості.

Перше. Електронні мережі забезпечують можливість не лише масової, а й міжособистісної та групової комунікації. В історії засобів комунікації є приклади, коли одна технологія забезпечувала комунікацію всіх трьох рівнів. Достатньо згадати радіо як засіб міжособистісної (діалог по радію), групової (використання певної частоти будь-яким відомством) та масової (традиційні радіостанції) комунікації. Принципова відмінність радіо та «Інтернет» в нашому контексті полягає в тому, що в першому випадку різні рівні комунікації розділені і не змішуються, тоді як у другому випадку користувач мережі може одночасно виступати як суб'єкт і міжособистісної, і групової, і масової комунікації. Крім того, як підкреслюють фахівці, поява та розповсюдження мережі «Інтернет» стимулює в сучасному інформаційному суспільстві нові соціокультурні процеси, головними з яких, як видається, є особливі якості спілкування – відкритість, щирість, можливість уникнення традиційного для засобів масової інформації бажання впливати, впливати, виховувати.

Друге. «Інтернет» з його особливими можливостями зворотного зв'язку з стороною, що сприймає, і навіть стиранням кордонів між розповсюджувачем і одержувачем інформації може докорінно змінити всі мас-медіа процеси. Відкритість, масовість, особистість – усе це не протиріччя, а

синоніми, що характеризують нове якість спілкування людей. Немає кордонів, немає простору, немає цензури, немає обмежень у візуальному самовираженні, повна та абсолютна анонімність, що поєднується з аналогічною відкритістю, можливістю самому вибирати джерело інформації та можливість миттєвого відкликання на те, що відбувається. Нескінченна кількість можливостей пошуку та вибору забезпечує кожному користувачеві Інтернету рівноправне та повноцінне спілкування, при якому досягається взаєморозуміння мотивів та цілей співрозмовників, тобто справжній діалог. У зв'язку з цим можна говорити не лише про соціальну значущість самої мережі «Інтернет», а й соціальну значущість будь-яких варіантів спілкування з прозорістю та щирістю «розмови».

Третє. Нині стає цілком очевидним, що «Інтернет» може виявитися не тільки засобом обміну інформацією, діалогічного спілкування та розваги, а й, як і всі інші ЗМІ, використовуватися як вплив. В даний час кількість його користувачів у нашій країні, як і у всьому світі, зростає дуже швидко. Дедалі більше фірм, підприємств, інститутів, шкіл підключаються до «всесвітньої павутини». Число користувачів «домашнього Інтернету» також постійно зростає (хоча дозволити його можуть далеко не всі – тут домінує матеріальний принцип), охоплюючи чи не найдієздатнішу частину сучасного суспільства.

Сьогодні ми є свідками своєрідної інформаційної війни за свідомість цієї категорії людей, тобто формування світогляду користувачів «Інтернет».

І оскільки деякі з сайтів явно спрямовані на дестабілізацію ситуації в суспільстві, постає питання науково вивіреного проектування інформаційного середовища в мережах «Інтернет». Враховуючи той факт, що Інтернет почав формувати соціокультурне середовище далеко за своїми віртуальними межами, впливати на життя навіть тих людей, які ніколи ним не користувалися, постає питання про інформаційну складову екології сучасної людини у світі комп'ютерних мереж. Доводиться констатувати, що в нашому суспільстві багато чуток, багато суперечливих думок щодо соціально значущої інформації, яку отримують саме з інтернету [7].

Привертають увагу і деякі методи використання мережі «Інтернет» в сучасній політичній боротьбі. Йдеться про оперативне скидання на інтернетівські сайти компромату, як правило, неперевіреного, а часто й хибного,

та про його негайне використання іншими засобами масової інформації, які сповідають принцип вихоплення «гарячих фактів». У мережі «Інтернет», з його специфікою безіменності сайтів та безвідповідальності за достовірність інформації, неможливо встановити не тільки людину, яка запровадила цю інформацію, але навіть місто чи країну, звідки ця інформація надійшла. Безсумнівно, що кількість анонімних сайтів в умовах гострої політичної боротьби зростатиме, безсумнівно й те, що безконтрольне «зливання» компроматів є певною загрозою соціальної стабільності.

У цьому відношенні є доцільним для інститутів політичної системи суспільства ведення оперативного моніторингу появи подібних сайтів, оцінка, прогноз їх можливих соціально-політичних наслідків, а в деяких випадках і створення «противаги» у вигляді інших альтернативних сайтів. Свобода слова, що є одним із основних принципів цієї комп'ютерної мережі, у такому разі анітрохи не порушується.

Четверте. Оскільки специфіка мережі «Інтернет» забезпечує будь-якому її користувачеві можливість стати комунікатором, що має необмежену аудиторію, а самому при цьому залишатися персоною анонімною, що в крайньому випадку користується псевдонімом, природний бурхливий сплеск соціальної активності, що знаходить своє відображення в багатьох ситуаціях. Очікувати, що люди, які отримали доступ до комунікації, не скористаються можливістю висловитися з принципово значимих для себе і для суспільства проблем, не шукатимуть варіанти самоствердження, було б наївно.

Оскільки свобода слова в мережі – річ незаперечна, неважко спрогнозувати, що різні організації та особи продовжуватимуть декларувати тут свої завдання та цілі. У зв'язку з цим виникають природні питання: чи хтось має оцінювати те, що відбувається у віртуальному просторі цієї глобальної мережі, і які мають бути критерії цієї оцінки? Звісно ж, що таку функцію може і має взяти на себе соціальна наука, що орієнтована на позитивні загальнолюдські і цінності. Гласність у наукових підходах змісту та мотиваційної спрямованості сайтів, орієнтованих на дестабілізацію у суспільстві, науковий прогноз можливих соціальних наслідків, використання для такої інформації та друку, і радію, і телебачення, та інтернету – єдиний спосіб проектування здорового соціокультурного середовища [8].

Однак існує й інша сторона цієї проблеми – правова. Останнім часом в інтернеті з'явилася

величезна кількість пропозицій всіляких комерційних фірм про продаж найрізноманітніших баз даних, що містять інформацію, яка є власністю державних структур. Цей факт свідчить про те, що інформаційні ресурси держави не захищені належним чином ні в правовому, ні в технічному плані. У зв'язку з цим має бути уточнено поняття власності на інформаційні ресурси та усі механізми забезпечення відповідних прав власності. Необхідно також забезпечити правовий захист конфіденційної інформації, що не містить відомостей, що становлять державну таємницю.

П'яте. Інтернет створює нову мовну характеристику інформації та організації комунікації, що ведуть до англійської експансії. Сьогодні ми та за населення багатьох інших країн світу, стають свідками потужного і динамічного процесу трансформації соціокультурного простору під впливом зразків американської культури, що все більш активно проникають у наше життя, а також англійських запозичень, безпосередньо пов'язаних з цими новими поняттями. Такі слова, як «комп'ютер», «бізнес», «менеджмент», «маркетинг», «офіс», «консалтинг» тощо, вже міцно увійшли до нашого повсякденного мовлення, до нашого побуту та свідомості.

Тут є свої особливості, але треба виходити, перш за все, з реалій дійсності. На сьогоднішній день у світі склався певний детермінізм: США більшою мірою, ніж інші промислові та технологічно успішні держави, беруть на себе функції центру не тільки в галузі економіки, фінансів та підприємництва, а й у галузі культури, науки, освіти, ЗМІ та інформаційних технологій. Відповідно й у сфері форм мовного втілення культурних і зразків найбільше вплив належить тим самим Сполученим Штатам. Зокрема, найважливіше місце у сучасній культурі глобалізації, зокрема мовної, грає сам «Інтернет». Мова цієї нової культури – англо-американська, оскільки більшість фахівців та користувачів інтернету живуть в англійських країнах [9].

Звідси можна зробити висновок, що сучасна світова культура епохи глобалізації найвищою мірою американо-центрична.

Отже, у міру того, як освоюються і беруться на озброєння американські нововведення у різних сферах життєдіяльності, поступово змінюються і цінності, установки, ментозлітет людей і характер комунікаційних, що народжуються. текстів, а нові англійські терміни, які у них, заповнюють смислові конструкції національних мов – носіїв іншомовних культур.

Таким чином, можна зробити висновок, що мережні засоби масової комунікації та інтернету є технологічною основою інформаційного суспільства, що формується з промислово-розвинених країн світу, у якому значна частина економічного потенціалу утворюється за рахунок інтенсивного розвитку «електронної» економіки, ефективного використання наявних інтелектуальних ресурсів. На цьому тлі не виправдано низьким виглядає існуючий рівень розвитку та використання системи «Інтернет».

Щоб державна політика України у сфері використання та розвитку мережних засобів масової комунікації була успішною, обов'язково необхідно врахувати як соціальне, економічне, політичне і культурне своєрідність нашої країни, а й особливості вітчизняних мережних засобів масової комунікації.

Як позитивний чинник може бути відзначено інтенсивний розвиток україномовного сектору інтернету, особливо після повномасштабного вторгнення Росії на територію України (підсистем інтернету, які використовують українську мову). Завдяки цьому явищу, що частково компенсує передбачувану вторинність України на глобальному інформаційному ринку, інформаційний вплив країн Північної Америки та Європи буде, ймовірно,

певною мірою досить рівно. Дані досліджень свідчать про те, що сайти російською користувалися в українців найбільшою популярністю, але зараз стрімко поширюється в Україні використання україномовних сайтів.

З 16 липня 2022 року набрали чинності частини 2 та 6 статті 27 Закону України «Про забезпечення функціонування української мови як державної», відповідно до яких власники всіх інтернет-ресурсів повинні запровадити україномовні версії вебсайтів [10]. Споживачі мають право на обслуговування їх державною мовою, а підприємці з 16 січня повинні обслуговувати лише українською. До таких підприємців відносяться всі продавці та надавачі послуг, хто безпосередньо обслуговує клієнтів, в тому числі інтернет-магазини та інтернет-каталоги, кафе, ресторани, магазини, гуртки, перукарні, спортклуби тощо.

Загалом перспективи інформаційної безпеки у сфері використання мережних комунікацій та «Інтернет» значною мірою залежать від продуманої державної політики у сфері масових комунікацій. Реалізація принципів ліберальної теорії, що на практиці означає передачу електронних мереж зв'язку на відкуп комерційним структурам, не відповідає існуючим соціально-політичним потребам російської держави та громадян. Тому державна концепція розвитку мережних комуні-

## Використання Інтернет у світі

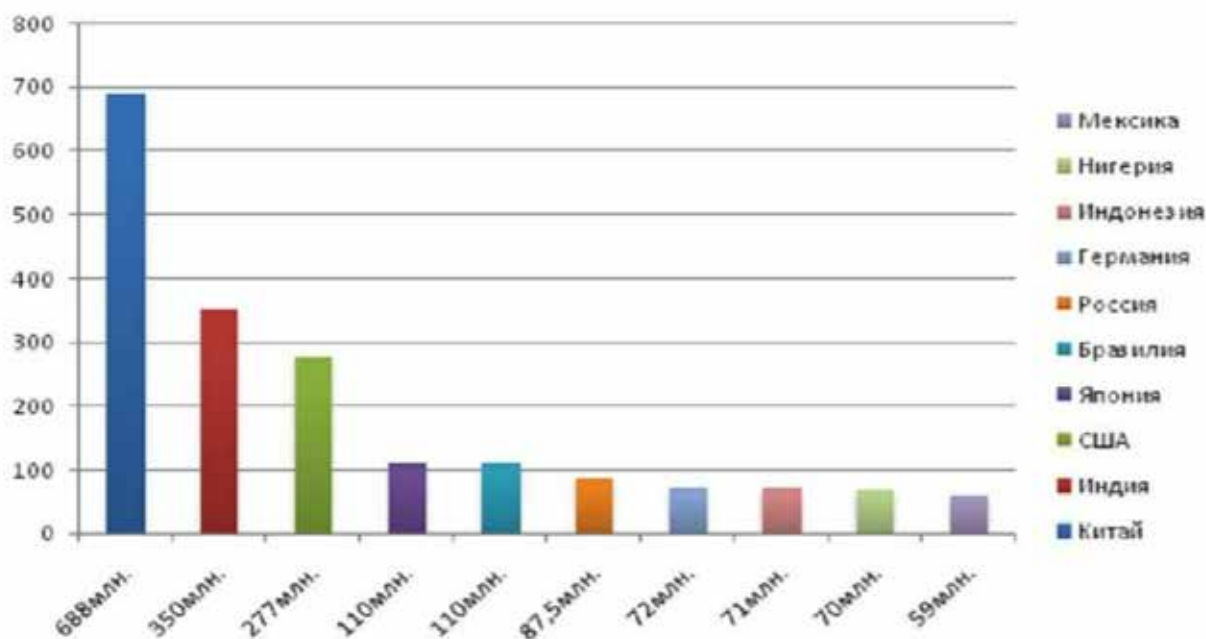


Рис. 1. Використання мережі «інтернет» у світі

Джерело: складено автором на основі власних досліджень.





Рис. 2. Забезпечення функціонування української мови як державної

Джерело: складено на основі [11].

кацій та Інтернету має однаково враховувати як існуючий світовий досвід, і національні особливості розвитку та використання російських комунікаційних систем. Оптимальним є комбінований підхід, що поєднує комерційний шлях розвитку мережевих засобів масової комунікації з їх контролем та підтримкою з боку України.

**Висновки.** Поняття та сутність інформаційної безпеки в умовах інформатизації України як соціального явища пропонується визначити наступним чином. Інформаційна безпека в умовах інформатизації України (формування інформаційного суспільства) – це суспільні відносини щодо створення і підтримання у

належному стані режиму нормального функціонування відповідної автоматизованої (комп'ютеризованої) інформаційної системи, систем телекомунікації; комплекс організаційних, правових та інженерно-технологічних (технічних та програмно-математичних) заходів щодо охорони, захисту, запобігання і подолання природних, техногенних і соціогенних загроз, реалізація яких може порушити чи припинити життєдіяльність конкретної соціо-технічної інформаційної системи.

Більш детально окремі проблеми щодо інформаційної безпеки в авторському розумінні подаються у публікаціях, наведених у списку літератури.

#### Література:

1. Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки : Резолюція ООН від 1 грудня 1999 року. URL: [//www.un.org](http://www.un.org).
2. Resolution adopted by the General Assembly UN [on the report of the First Committee (A/53/576)] «Development in the field of information and telecommunication in the context of information security». Distr. General A/RES/53/70, 4 January, 1999, N.Y.
3. Інформаційні війни. URL: [http://pidruchniki.com/18000102/politologiya/informatsiyni\\_viyuni](http://pidruchniki.com/18000102/politologiya/informatsiyni_viyuni) (дата звернення: 22.09.2022).
4. Комаров М. Ю., Гончар С. Ф., Ониськова А. В. Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об'єктах критичної інфраструктури. Моделювання та інформаційні технології. №82. 2018. С. 40–48.
5. Киричок Р. В., Складанний П. М., Бурячок В. Л., Гулак Г. М., Козачок В. А. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення. Наукові записки Українського науково-дослідного інституту зв'язку. №3. 2016. С. 48–61.
6. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: <https://zakon.rada.gov.ua/laws/show/685/2021n7>.
7. «Перша світова медійна війна». З якою назвою напад росії на Україну увійде в історію і що робити з 9 травня – інтерв'ю з Антоном Дробовичем. URL: <https://nv.ua/ukr/world/geopolitics/viynav-ukrajini-persha-svitova-mediyna-viyna-drobovichnovini-ukrajini-50235840.html>.

8. Онищенко О. С. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища: монографія / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.]; НАН України, Національна бібліотека України ім. В. І. Вернадського. К., 2014.
9. Горовий В. М. Правові перспективи національного розвитку. URL: <http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/st hash.AgJjKJa4.dpuf>.
10. Баровська А. Інституційне забезпечення державної комунікативної політики : досвід країн Європи: аналітична доповідь. URL: [www.niss.gov.ua/articles/1730](http://www.niss.gov.ua/articles/1730).
11. Про забезпечення функціонування української мови як державної. Закон України. Відомості Верховної Ради (ВВР), 2019, № 21, ст.81. URL: <https://zakon.rada.gov.ua/laws/show/2704-19iText> (дата звернення 02.04.2022).
12. Danko Y. I. Reznik N. P. Contemporary challenges for China and Ukraine and perspectives for overcoming these challenges. *Global Trade and Customs Journal*, 2019. 14(6).
13. Reznik N., Hridin O., Chukina I., Krasnorutskyu O., Mykhaylichenko M. Mechanisms and tools of personnel management in institutional economics. *AIP Conference Proceedings*. 2022. 2413, 040012 <https://doi.org/10.1063/5.0089330>.
14. Довгань О. Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації. *Правова інформатика*. 2013. № 4(40). С. 79–88.
15. Ханін І. Г. Формування в міжнародній системі інформаційної безпеки: економічні орієнтири для України. *Ефективна економіка*. 2015. № 4. 10.
16. Грабар І. Г., Гришук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія; за заг. ред. Р. В. Гришука. Житомир: ЖНАЕУ, 2019. 280 с.