**УДК 338.47:65**
**DOI: 10.31470/2518-7600-2019-8-134-155**

# INFORMATION SECURITY AS A TOOL TO PROTECT THE NATIONAL MEDIA SPACE

# ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ІНСТРУМЕНТ ЗАХИСТУ НАЦІОНАЛЬНОГО МЕДІАПРОСТОРУ

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ИНСТРУМЕНТ ЗАЩИТЫ НАЦИОНАЛЬНОГО МЕДИАПРОСТРАНСТВА

***Олена Ісайкіна*,**
кандидат історичних наук,
доцент кафедри
документознавства
isaykina.od@ukr.net
https://orcid.org/0000-0001-6370-7546
ID: 0000-0001-6370-7546
ДВНЗ «Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди»,
м. Переяслав-Хмельницький,
вул. Сухомлинського, 30,
Київська обл., Україна, 08401

***Olena Isaikina*,**
PhD in Historical sciences,
associate professor of Department of scientific discipline of documentation
isaykina.od@ukr.net
https://orcid.org/0000-0001-6370-7546
ID: 0000-0001-6370-7546
Pereiaslav-Khmelnytskyi Hryhorii Skovoroda State Pedagogical University, 30,
Sukhomlynskoho Str.,
Pereiaslav-Khmelnytskyi,
Kyiv region, Ukraine, 08401

***Алла Зленко*,**
кандидат історичних наук,
доцент кафедри
документознавства
zlenko.am@ukr.net
https://orcid.org/0000-0002-5586-3984
ID: 0000-0002-5586-3984
ДВНЗ «Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди»,
м. Переяслав-Хмельницький,
вул. Сухомлинського, 30,
Київська обл., Україна, 08401

***Alla Zlenko*,**
PhD in Historical sciences,
associate professor of Department of scientific discipline of documentation
zlenko.am@ukr.net
https://orcid.org/0000-0002-5586-3984
ID: 0000-0002-5586-3984
Pereiaslav-Khmelnytskyi Hryhorii Skovoroda State Pedagogical University, 30,
Sukhomlynskoho Str.,
Pereiaslav-Khmelnytskyi,
Kyiv region, Ukraine, 08401


*ISSN (print) 2518-7600 ISSN (online) 2524-1060*
*https://sdc-journal.com*

**ABSTRACT**

*The publication is devoted to the study of information security as a prerequisite for the protection of national information content, since the information factor plays an important role in the creation of the state and the defense of the interests of the state. The globalization of media processes, the spread and popularity of the so-called digital media have led to a significant increase in the influence of mass communication on the formation in society not only of ideas, attitudes, values and the overall picture of the world, but also of the public and individual consciousness in general. Particularly important in this spectrum of public relations are the problems of information security.*

*The article, based on the theoretical analysis of the scientific views of modern researchers, concludes that information security today means several fundamentally different tasks, namely: protection of the country's IT infrastructure (the so-called cyberspace); counteraction to special operations (provocations, diversions) carried out with the help of mass media; counteracting hostile (purposeful and destructive) ideological influence; counteracting the destructive effects carried out by the media (various kinds of «toxic» content, such as the advertising of destructive cults, cruelty, deviant behavior) (IBU, 2014). Each of these tasks is characterized by a different correlation of objective and subjective factors.*

*Information security is a state of protection of the information environment of a society that ensures its formation, use and development in the interests of citizens, organizations, and the state.*

*Information security threats are the downside of using information technology. The sources of such threats and challenges may be international criminal groups of hackers, some IT-trained criminals, foreign government agencies, terrorist groups, non-governmental organizations, political structures and informal extremist groups, transnational corporations and financial-industrial groups, etc.*

*The current legal framework does not cover all the basic elements necessary to effectively counteract information threats in Ukraine. At the same time, given the multifaceted nature and complexity of the identified problem, it is necessary to stipulate the*

*further need for scientific research of mechanisms for ensuring information security in Ukraine.*

***Keywords**: information, information security, media space, social networks, communication media, information society, threats, influences.*

**Постановка проблеми.** Протягом останніх десятиріч в Україні спостерігається поступальний розвиток інформаційної сфери як особливої системи суспільних відносин, що виникають в усіх сферах життя і діяльності суспільства та держави в результаті одержання, використання, поширення та зберігання інформації, насамперед у сфері законодавчого закріплення права особи на інформацію та на вільне поширення її в країні і за кордоном, трансформації моделі взаємовідносин між органами державної влади та засобами масової інформації, створення національних систем і мереж інформації.

Водночас, поряд із очевидними перевагами інноваційного розвитку, Україна, так само як і інші розвинуті країни світу, зазнає зростаючого тиску на власний інформаційний суверенітет та інформаційну безпеку особи, суспільства, держави. Глобальність процесів інформатизації та їх технічні особливості роблять питання забезпечення інформаційної безпеки однією з найважливіших функцій держави.

**Аналіз останніх досліджень і публікацій.** Дослідженням інформаційної сфери займалися та займаються такі вчені, такі як І. Арістова (Арістова, 2005), О. Баранов (Баранов, 2014), Ю. Бурило (Бурило, 2012), В. Горовий (Горовий, 2015), В. Конах (Конах, 2014), М. Сенченко (Сенченко, 2006) та ін.

Дослідження сучасних загроз інформаційній безпеці держави ґрунтується на наукових здобутках відомих дослідників у сфері безпекознавства, політології, соціології, теорії управління тощо, таких як В. Горбулін (Горбулін, 2009), В. Світлична (Світлична, 2013), Р. Хмелевський (Хмелевський, 2016), О. Снитко (Снитко, 2017) та інші науковці, які присвятили свої праці питанням забезпечення національної безпеки. Водночас, оскільки загрози інформаційній безпеці

держави в сучасних умовах є динамічними та постійно змінюються, відповідна проблематика наукових досліджень не втрачає своєї актуальності.

**Метою статті** є всебічне дослідження проблеми гарантування інформаційної безпеки України, захисту національного інформаційного медіапростору з огляду на реальні й потенційні загрози.

**Виклад основного матеріалу дослідження.** Живучи на рубежі століть і тисячоліть, ми стаємо свідками грандіозних змін, результатом яких є поява, обробка і засвоєння небачених раніше обсягів знань. За підрахунками вчених, на перше подвоєння знань було потрібно 1750 років (тобто від початку нашої ери до 1750 року), друге подвоєння сталося вже до 1900 року, а третє до 1950 року. Тобто лише за півстоліття об'єм інформації збільшився у 8-10 разів. Надалі обсяги знань подвоювалися з ще більшою швидкістю: спочатку з різниці в 10 років, потім в 5 років, а з 1991 року - щорічно. Вражає з якою швидкістю подвоюється інформація сьогодні. Ці дані свідчать про початок переходу суспільства в інформаційний період свого розвитку (Найдьонов, 2010).

Вся інформація, що створюється і поширюється в нашій державі, незалежно від змісту, форм, часу й місця становить її інформаційні ресурси. Україна самостійно їх формує на своїй території та вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами. Національні інформаційні ресурси є основою інформаційного суверенітету України, який гарантується інформаційною безпекою.

Виходячи із наукових підходів і законодавчих актів України можна визначити інформацію як документовані або публічно оголошені відомості про події та явища, що відбувають у суспільстві, державі та навколишньому середовищі. Інформацією можна вважати дані, що знайшли свого споживача.

Використання всесвітньої мережі та нових технологій супроводжується такими явищами, як низький рівень культури безпеки, збільшення онлайн користувачів і залежності від цифрової інфраструктури, поширення небажаного контенту,

розвиток кібер-шахрайства, витоки інформації, втрата даних, несанкціонований доступ до інформації.

Швидкий темп життя сучасної людини, збільшення потоків інформації вносять свої корективи і в критерії задоволення потреби людини в інформації. Якщо десять – п'ятнадцять років тому популярними були великі аналітичні матеріали, у тому числі й розгорнуті політематичні інтерв'ю, то сьогодні в пріоритеті короткі повідомлення – новини, невеликі за об'ємом, бліц-інтерв'ю, стислі коментарі. Крім того, у зв'язку зі зростанням кількості засобів масової комунікації (ЗМК), актуальним для пересічних громадян є питання формування єдиної новинної стрічки з різних джерел. Таку можливість надають соціальні мережі.

Сторінки користувачів соцмереж дозволяють одночасно в єдиній стрічці передивлятися добірку повідомлень із сторінок низки мас-медіа, тобто вони виконують функції дайджесту подій. Перевага подібного інформування полягає в тому, що користувач самостійно визначає ЗМК, з яких він бажає отримувати інформацію. До того ж, саме в соціальних мережах є можливість найлегше і найшвидше, без додаткової реєстрації або авторизації, показати власне ставлення до матеріалу за допомогою «лайка» або написання коментарів до того або іншого повідомлення. З іншого боку, редакція ЗМК також має безпосередній контакт із представниками своєї аудиторії, які не лише переглядають новини, але і допомагають їх створювати, – підказують теми для нових матеріалів, інформують про конкретні події тощо (Литвиненко, 2019).

Найбільш популярними пристроями, якими володіють користувачі, сьогодні є комп'ютери, лептопи, планшети та смартфони. Серед засобів комунікації – різноманітні месенджери: Viber, Telegram, Whatsapp, Hangouts. У багатьох є акаунти у Gmail чи Facebook.

Означимо коло ризиків, для власника цих пристроїв та акантів. Окрім того, що пристрої можуть фізично забрати та отримати до них доступ, через зламані акаунти може статися витік інформації, її знищення або розповсюдження компромату.

Загроза смартфона в тому, що користувач постійно залогований через нього в один чи два акаунти. Якщо

зловмисник отримує смартфон і той буде незахищеним – він отримує доступ до цих акаунтів. Через номер телефону можна отримати доступ до Telegram. Тому для персонального захисту інформації важливо, щоб сервіси, які прив'язані до номера телефону, були налаштовані таким чином, щоб зловмисники не змогли взяти їх під контроль.

У першу чергу потрібно звернути увагу, на те, де розташовані сервери компанії, як шифрується комунікація, яка практика в цій компанії щодо розкриття інформації. Наприклад, Facebook Messenger належить Facebook, у ньому наскрізне шифрування за замовчуванням не встановлено. Hangouts належить Google, у ньому шифрування немає зовсім. Тобто, обидві компанії знають про комунікації користувачів. У разі, якщо буде потреба чи запит правоохоронних органів, вони можуть надіслати запит на розкриття даних.

Месенджер *Whatsapp* використовує той тип шифрування, коли він лише фіксує, коли і з ким користувач спілкувався, проте не знає змісту повідомлень (так зване наскрізне шифрування). Міжнародна правозахисна організація Amnesty International назвала WhatsApp найбільш захищеним месенджером.

Сервери месенджера *Telegram* розташовані у п'ятьох різних країнах. Точно відомо про три дата-центри в Лондоні, Сингапурі та Сан-Франциско. Але цей месенджер не шифрує повідомлень і таким чином має дані про зміст листування. І якщо влада країни, в якій розташовані сервери, вирішить їх вилучити, листування можуть відкрити. Хоча така ймовірність дуже низька, оскільки це автоматично зруйнує імідж менеджера.

У месенджера *Viber* є сервери в Ізраїлі, Білорусі, Росії. Також відомо, що шифрування Viber не захищає листування від самої компанії. Тому для чутливої комунікації цей месенджер краще не використовувати. Також не варто надто довіряти *Skype,* що належить Microsoft. У цій програмі не використовується наскрізне шифрування, а організація Amnesty International звертає увагу на те, що Microsoft відкриває дані щодо листування користувачів на запити уряду.

Глобалізація масмедійних поцесів, поширення і набуття

популярності так званих цифрових медіа зумовили значне посилення впливу засобів масової комунікації на формування у людей не тільки уявлень, установок, ціннісних орієнтацій та загальної картини світу, але й суспільної та індивідуальної свідомості в цілому. Кожен конкретний ЗМК може створювати свою версію медіареальності, через яку люди сприймають усе те, що відбувається довкола. Включеність людини в подібну медіареальність відкриває їй унікальний доступ до різних знань, відомостей та інформації, у зв'язку з чим масмедіа отримують здатність детермінувати формування нового розуміння реальності і нових зв'язків людини з цією реальністю.

У той же час, ЗМК можуть не лише відображувати, фіксувати, моделювати дійсність (тобто факти, події, соціальні й інші стосунки), продукуючи інформацію про цю дійсність, але й управляти соціальною реальністю, змінювати її, транслювати, підтримувати, затверджувати суспільні норми й цінності, контролювати якість виконання управлінських рішень, регулювати соціальні та інші стосунки. Вплив масмедіа на хід будь-яких суспільних процесів з розвитком інтернет-технологій продовжує зростати і стає усе більш активним. Це означає, що ЗМК перестають бути лише «сторонніми спостерігачами за подією», вони самі виступають каталізаторами, а інколи й авторами ідеї створення певної події. ЗМК можуть як об'єднувати людей, так і роз'єднувати їх. У таких умовах виникає висока вірогідність порушення основоположних принципів інформаційної безпеки як кожної окремо взятої людини, так і суспільства та держави в цілому відносно права отримувати достовірну, правдиву, неупереджену й всебічну інформаційну картину світу (Литвиненко, 2019).

Поняття «інформаційна безпека» з'явилося наприкінці 80-х років у праці німецького вченого Я.М. Жаркова йдеться про важливий інформаційний компонент у міжнародній безпеці та робиться спроба розглянути проблеми безпеки, які пов'язані з інформаційними загрозами комплексно. А у вітчизняній пресі починаючи з кінця 1991 – початку 1992 року спостерігається тенденція до відкритого дослідження проблеми інформаційної безпеки як окремого питання (Жарков&Бєсєдіна, 2009).

В українському законодавстві термін «інформаційна безпека» закріплено лише у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Інформаційна безпека – стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави (ЗУ, 2007).

На сьогоднішній день під інформаційною безпекою розуміється кілька принципово різних за своєю природою завдань, а саме:

– захист ІТ-інфраструктури країни (так званого кіберпростору);

– протидія спеціальним операціям (провокаціям, диверсіям), здійснюваним за допомогою мас-медіа;

– протидія ворожому (цілеспрямованому і деструктивному) ідеологічному впливу;

– протидія деструктивним впливам, які здійснюються за допомогою мас-медіа (різного роду «токсичний» контент на зразок реклами деструктивних культів, жорстокості, девіантної поведінки) (ІБУ, 2014).

Кожне з цих завдань характеризується різним співвідношенням об'єктивних і суб'єктивних факторів.

Цифрова безпека – це не стільки про інструменти, скільки про практики, звички й ставлення до того, що користувач робить в Інтернеті. Треба виходити з кількох базових тез: абсолютного захисту не існує; цифрова безпека – це питання того, як збільшити ціну атаки проти вас, щоби більшість потенційних супротивників цим не займалися.

У сучасному глобалізованому інформаційному суспільстві, де кіберпростір перетворюється на поле боротьби, вагомими загрозами інформаційній безпеці держави (і України, зокрема) є комп'ютерна злочинність, кібертероризм, кібервійни, які передбачають протистояння національних інтересів у просторі Інтернету, застосування комп'ютерних та інтернет-технологій для нанесення шкоди супротивнику. Найчастіше технології кібервійни, кібертероризму спрямовані на сферу державної безпеки й оборони і становлять реальну загрозу суверенітету держави.

Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій. Джерелами таких загроз та викликів можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері ІТ злочинці, іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо.

В наш час зростає загроза використання проти інтересів України кібернетичних засобів як з середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури як «транзитного майданчику» для приховування атаки на інформаційні ресурси третьої сторони, що може розцінюватись провідними країнами як дії держави з відповідними наслідками політичного, економічного, правового, а можливо, і воєнного характеру (ДПСІ, 2014).

Інформаційна безпека є інтегрованою складовою національної безпеки і її розглядають як пріоритетну функцію держави. Інформаційна безпеки, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій. Рішення комплексної проблеми інформаційної безпеки дасть змогу як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об'єктивної та якісної інформації (Ільницька, 2018).

За останні роки Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн та її інформаційна безпека опинилась під загрозою. Можна констатувати, що:

– український інформаційний простір є незахищеним від зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії;

– у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні. Як наслідок – світова громадськість відчуває брак інформації або отримує її з інших джерел, які часом дезінформують, надають викривлену, спотворену, неповну інформацію. Водночас проти України активно застосовується потужний медіаресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності, заниження міжнародного іміджу держави;

– діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення (Ільницька, 2018).

Гарантування інформаційної безпеки України в умовах дестабілізуючих негативних інформаційно-психологічних впливів потребує консолідації зусиль на усіх рівнях державної влади та громадянського суспільства. Як протидія масштабним негативним інформаційно-психологічним впливам пріоритетними напрямами державної інформаційної політики та важливими кроками з боку владних органів України мають бути:

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;

– законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну

конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету;

– оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, які не є підписантами зазначеної Конвенції;

– створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку;

– розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

– забезпечення повного покриття території України цифровим мовленням;

– розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру;

– побудова дієвої та ефективної системи стратегічних комунікацій;

– розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України;

– боротьба з дезінформацією та деструктивною пропагандою;

– виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та/або використовуються для ведення інформаційної війни проти України;

– недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні (ДІБУ).

У Доктрині інформаційної безпеки України визначено, що до національних інтересів України в інформаційній сфері віднесено такі життєво-важливі інтереси особи, як:

– забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

– забезпечення конституційних прав людини на захист приватного життя;

– захищеність від руйнівних інформаційно-психологічних впливів.

Проте, цей документ являє собою сукупність теоретичних понять про цілі, принципи та правові складові інформаційної безпеки. Відтак, з нього не зрозуміло чітких завдань та відповідальних суб'єктів за інформаційну безпеку, оскільки він є лише основою для розроблення проектів, концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України.

Найбільш небезпечні загрози інформаційній безпеці держави, передусім транскордонні й такі, що мають політичне забарвлення, вже тривалий час вивчаються в рамках проблеми інформаційної війни, під поняттям якої об'єднуються.

Існує багато визначень «інформаційної війни», в яких вона тлумачиться як комплекс заходів і операцій, здійснюваних у конфліктних ситуаціях, коли дані є водночас зброєю, ресурсом і ціллю. Тобто це, війна за знання, пошук відповідей на питання: що, де, коли, чому і наскільки надійними окремо узяте суспільство або армія вважають свої знання про себе і своїх супротивників. Інформаційна війна може вестися як у воєнний, так і в мирний час. «Інформаційна війна є електронним конфліктом, де дані є стратегічним здобутком, який варто захопити чи знищити. І комп'ютери, й інформаційні системи стають привабливим напрямком першого удару» (Михальчук, 2004).

Можна у такий спосіб згрупувати види інформаційної зброї, використовуваної в інформаційній війні:

– засоби пропагандистсько-психологічного впливу (через пресу, телебачення, радіо, Інтернет, інші канали);
– засоби програмно-математичного впливу (комп'ютерні віруси, логічні «бомби», засоби придушення комп'ютерних мереж тощо);
– засоби психологічного впливу(голографічні зображення, синтезатори голосів відомих лідерів);
– психотронна зброя (зомбування, гіпноз).

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, її інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану систему цінностей, поглядів, інтересів і рішень в суспільній і

державній діяльності, спрямовувати їх поведінку і розвиток у бажаному для іншої сторони руслі.

Протягом останніх років значно зросла необхідність в комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору, і це проглядається у нормативних документах зарубіжних країн.

Наприклад, у Молдові діє Стратегія інформаційної безпеки яка містить опис безпекових та правових проблем, цілі, завдання Концепції інформаційного захисту та план її реалізації із чітким розподілом відповідальних суб'єктів. У Данії, на державному рівні розроблено стратегію інформаційної та кібербезпеки, яка комплексно охоплює інформаційну безпеку – від найвищого державного рівня – до безпеки людини в мережі. В Естонії, яка вважається європейським лідером із застосування цифрових технологій в економіці та адмініструванні дбають про інформаційний захист з 1996 року (ІБ, 2019).

Ключовими заходами щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію повинні стати:

– стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

– забезпечення функціонування суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;

– створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;

– підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

– розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

– комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;

– підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;

– удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;

– повне покриття території України цифровим та Інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;

– формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;

– пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз (ДІБУ).

**Висновки.** Інтереси суспільства в інформаційній сфері полягають у забезпеченні реалізації конституційних прав і свобод людини та громадянина з метою зміцнення демократії, створення правової соціальної держави, досягнення і підтримки суспільної злагоди, духовного оновлення України, досягнення і підтримки громадської згоди, підвищення творчої активності населення.

Інтереси держави в інформаційній сфері визначаються створенням умов для гармонійного розвитку української інформаційної інфраструктури, для реалізації конституційних прав і свобод людини та громадянина у сфері отримання інформації, користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності України, встановлення політичної, економічної та соціальної стабільності, в безумовному забезпеченні законності і правопорядку, розвитку рівноправного і взаємовигідного міжнародного співробітництва на основі партнерства .

Як показує аналіз стану інформаційної безпеки України, її рівень, значною мірою, не відповідає потребам особистості, суспільства і держави. Очевидно, що державна інформаційна політика в аспекті інформаційної безпеки багато в чому буде

залежати від розробки виважених наукових моделей і підходів до вирішення зазначеної проблеми.

## ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Арістова І.В. Державна інформаційна політика: Організаційно-правові аспекти // Вісник Національного університету внутрішніх справ. 2005. Вип.31. С. 239-245.

2. Баранов О.А. Правове забезпечення інформаційної сфери: Теорія, методологія і практика. К.: Едельвейс, 2014. 434 с.

3. Бурило Ю.П. Інформаційна сфера як сфера господарювання: Теоретично-правовий аспект // Правова інформатика. 2012. №4 (36). С. 18-28.

4. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. К.: Інтертехнологія, 2009. 164 с.

5. Горовий В.М. Національні інформаційні процеси в умовах глобалізації. К.: Нац. б-ка України ім. В.І. Вернадського, 2015. 332 с.

6. ДІБУ – Доктрина інформаційної безпеки України. URL: http://www.president.gov.ua/documents/472017-21374 (актуальність 21.11.19).

7. ДПСІ – Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні. URL: http://policy-analysis.org/wp-content/uploads/2014/10/Stan_informatyzacii_20132.pdf (актуальність 16.11.19).

8. Жарков Я. М., Бєсєдіна Л.М. Напрямки зовнішнього інформаціно-психолоічного впливу на Україну // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. 2009. № 19. URL: http//www.nbuv.gov.ua / portal / natural/ znpviknu / 2009-19 / vip19-21.pdf (актуальність 09.10.19).

9. ЗУ – Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». URL: http://oblosvita.com/normatyvna_baza (актуальність 13.09.19).

10. ІБ – Інформаційна безпека now: яких елементів не вистачає? URL: https://www.prostir.ua (актуальність 11.09.19).

11. ІБУ – Информационная безопасность Украины: проблемы и пути их решения. URL: http://mediasat.info/ 2014/12/04/ informacionnaja-bezopasnost-ukrainy-problemy-i-puti-ih-reshenija/ (актуальність 12.10.19).

12. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. 2018. URL: http:// ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf (актуальність 12.11.19).

13. Конах В.К. Національний інформаційний простір України: Проблеми формування та державного регулювання. К.: НІСД, 2014. 76 с.

14. Литвиненко О. Інформаційна безпека людини й суспільства у контексті медіа філософії. 2019. URL: file:///C:/Users/user/Downloads/28-43-1-PB.pdf (актуальність 16.09.19).

15. Михальчук В.Ф. Спеціальні інформаційні операції в контексті інформаційних війн. К.: Національний університет «Острозька академія». 2014. 300 с.

16. Найдьонов О.Г. Інформатизація як головна ідея третього тисячоліття // Ученые записки Таврического национального университета им. В.И. Вернадского. Серия «Философия. Культурология. Политология. Социология», 2010. Том 23 (62). № 2. С. 161-165.

17. Світлична В.Ю. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення // Науковотехнічний збірник. Х.: ХНАМГ, 2013. № 109. С. 360-369.

18. Сенченко М.І. Книгодрукування і масс-медіа Канади. К.: Кн. палата України, 2006. 34 с.

19. Снитко О.С. Проекти тотального зомбування в інформаційному просторі України // Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С. 207-215.

20. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності // Сучасний захист інформації. 2016. №4. С. 65-70.

## REFERENCES

1. Aristova, I.V. (2005). Derzhavna informatsiina polityka: Orhanizatsiino-pravovi aspekty [State information policy: Organizational and legal aspects ] // *Visnyk Natsionalnoho universytetu vnutrishnikh sprav* – Bulletin of the National University of the Interior, 31, 239-245 [in Ukrainian].

2. Baranov, O.A. (2014). *Pravove zabezpechennia informatsiinoi sfery: Teoriia, metodolohiia i praktyka* [Legal support of information sphere: Theory, methodology and practice]. K.: Edelveis, 434 [in Ukrainian].

3. Burylo, Yu.P. (2012). Informatsiina sfera yak sfera hospodariuvannia: Teoretychno-pravovyi aspekt [Information sphere as a sphere of management: Theoretical and legal aspect] // *Pravova informatyka* – Legal Informatics, 4 (36), 18-28 [in Ukrainian].

4. Horbulin, V. P. (2009). *Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia* [Information operations and security of society: threats, counteraction, modeling]. K.: Intertekhnolohiia, 164 [in Ukrainian].

5. Horovyi, V.M. (2015). *Natsionalni informatsiini protsesy v umovakh hlobalizatsii* [National information processes in the conditions of globalization]. K.: Nats. b-ka Ukrainy im. V.I. Vernadskoho, 332 [in Ukrainian].

6. DIBU – *Doktryna informatsiinoi bezpeky Ukrainy* [Doctrine of Information Security of Ukraine]. URL: http:// www.president.gov.ua/ documents/472017-21374 [in Ukrainian].

7. DPSI – *Dopovid pro stan informatyzatsii ta rozvytok informatsiinoho suspilstva v Ukraini* [Report on the state of information and development of the information society in Ukraine]. URL: http://policy-analysis.org/wp-content/uploads/ 2014/10/Stan_informatyzacii_20132.pdf [in Ukrainian].

8. Zharkov, Ya. M. & Biesiedina, L.M. (2009). Napriamky zovnishnoho informatsino-psykholoichnoho vplyvu na Ukrainu [Directions of external information-psychological influence on Ukraine] // *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu im. T. Shevchenka* – Collection of scientific works of the Military Institute of Kiev National University T. Shevchenko, 19. URL: http//www.nbuv.gov.ua / portal / natural/ znpviknu / 2009-19 / vip19-21.pdf [in Ukrainian].

9. ZU – *Zakon Ukrainy «Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007-2015 roky»* [Law of Ukraine «On Basic Principles of Information Society Development in Ukraine for 2007-2015»]. URL: http://oblosvita.com /normatyvna_baza [in Ukrainian].

10. IB – *Informatsiina bezpeka now: yakykh elementiv ne vystachaie?* [Information security now: what elements are missing?]. URL: https://www.prostir.ua [in Ukrainian].

11. IBU – *Ynformatsyonnaia bezopasnost Ukraynы: problemы y puty ykh reshenyia* [Information Security of Ukraine: Problems and Ways to Solve it]. URL: http://mediasat.info/ 2014/12/04/ informacionnaja-bezopasnost-ukrainy-problemy-i-puti-ih-reshenija/ [in Ukrainian].

12. Ilnytska, U. (2018). *Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnym informatsiino-psykholohichnym vplyvam* [Information Security of Ukraine: Current Challenges, Threats, and Mechanisms to Counteract Negative Information and Psychological Impacts]. URL: http:// ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf [in Ukrainian].

13. Konakh, V.K. (2014). *Natsionalnyi informatsiinyi prostir Ukrainy: Problemy formuvannia ta derzhavnoho rehuliuvannia* [National Information Space of Ukraine: Problems of Formation and State Regulation]. K.: NISD, 76 [in Ukrainian].

14. Lytvynenko, O. (2019). *Informatsiina bezpeka liudyny y suspilstva u konteksti media filosofii* [Information Security of Man and Society in the Context of Media Philosophy]. URL: file:///C:/Users/user/Downloads/28-43-1-PB.pdf [in Ukrainian].

15. Mykhalchuk, V.F. (2014). *Spetsialni informatsiini operatsii v konteksti informatsiinykh viin* [Special information operations in the context of information wars]. K.: Natsionalnyi universytet «Ostrozka akademiia», 300 [in Ukrainian].

16. Naidonov, O.H. (2010). Informatyzatsiia yak holovna ideia tretoho tysiacholittia [Informatization as the main idea of the third millennium] // *Uchenыe zapysky Tavrycheskoho natsyonalnoho unyversyteta ym. V.Y. Vernadskoho* – Uchenye zapiski Tavricheskogo national university im. YOU. Vernadsky, 23 (62), 2, 161-165 [in Ukrainian].

17. Svitlychna, V.Yu. (2013). Informatsiina bezpeka: bahatohrannist sutnosti, vydy zahroz ta shliakhy zabezpechennia [Information security: multifaceted nature, types of threats and ways of providing] // *Naukovotekhnichnyi zbirnyk* – Scientific and Technical Collection. Kh.: KhNAMH, 109, 360-369 [in Ukrainian].

18. Senchenko, M.I. (2006). *Knyhodrukuvannia i mass-media Kanady* [Bookbinding and Media Canada]. K.: Kn. palata Ukrainy, 34 [in Ukrainian].

19. Snytko, O.S. (2017). Proekty totalnoho zombuvannia v informatsiinomu prostori Ukrainy [Total zombie projects in the information space of Ukraine] // *Informatsiina bezpeka liudyny, suspilstva, derzhavy* – Information security of man, society, state, 1 (21), 207-215 [in Ukrainian].

20. Khmelevskyi, R.M. (2016). Doslidzhennia otsinky zahroz informatsiinii bezpetsi ob'iektiv informatsiinoi diialnosti [Research of threats to information security of objects of information activity] // *Suchasnyi zakhyst informatsii* – Modern information protection, 4, 65-70 [in Ukrainian].

**АНОТАЦІЯ**

*Публікація присвячена дослідженню інформаційної безпеки як передумови захисту вітчизняного інформаційного контенту, оскільки інформаційний фактор відіграє важливу роль у державотворенні та відстоюванні інтересів держави. Глобалізація масмедійних процесів, поширення і набуття популярності так званих цифрових медіа зумовили значне посилення впливу засобів масової комунікації на формування в суспільстві не тільки уявлень, установок, ціннісних орієнтацій та загальної картини світу, але й суспільної та індивідуальної свідомості в цілому. Особливе місце в цьому спектрі суспільних відносин займають проблеми забезпечення інформаційної безпеки.*

*У статті за підсумками теоретичного аналізу наукових поглядів сучасних дослідників, зроблено висновок, що сьогодні під інформаційною безпекою розуміється кілька принципово різних за своєю природою завдань, а саме: захист IT-інфраструктури країни (так званого кіберпростору);*

*протидія спеціальним операціям (провокаціям, диверсіям), здійснюваним за допомогою масмедіа; протидія ворожому (цілеспрямованому і деструктивному) ідеологічному впливу; протидія деструктивним впливам, які здійснюються за допомогою масмедіа (різного роду «токсичний» контент на зразок реклами деструктивних культів, жорстокості, девіантної поведінки) (ІБУ, 2014). Кожне з цих завдань характеризується різним співвідношенням об'єктивних і суб'єктивних факторів.*

*Інформаційна безпека – стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.*

*Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій. Джерелами таких загроз та викликів можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері ІТ злочинці, іноземні державні органи, терористичні угрупування, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо.*

*Сучасна нормативно-правова база не охоплює всі основні елементи, необхідні для ефективної протидії інформаційним загрозам в Україні. У той же час, враховуючи, багатогранність та комплексність означеної проблеми, варто обумовити подальшу необхідність наукових досліджень механізмів забезпечення інформаційної безпеки в Україні.*

***Ключові слова:*** *інформація, інформаційна безпека, медіапростір, соціальні мережі, засоби комунікації, інформаційне суспільство, загрози, впливи.*

## АННОТАЦИЯ

*Публикация посвящена исследованию информационной безопасности как составляющей защиты отечественного информационного контента, поскольку информационный фактор имеет важную роль в создании государства и отстаивании его интересов. Глобализация массмедийных процессов, распространение и приобретение популярности*

*так называемыми цифровыми медиа обусловили значительное усиление влияния средств массовой коммуникации на формирование в обществе не только представлений, установок, ценностных ориентаций и общей картины мира, но и общественного и индивидуального сознания в целом. Особое место в этом спектре общественных отношений занимают проблемы обеспечения информационной безопасности.*

*В статье по итогам теоретического анализа научных взглядов современных исследователей, сделан вывод, что сегодня под информационной безопасностью понимается несколько принципиально различных по своей природе задач, а именно: защита ИТ-инфраструктуры страны (так называемого киберпространства); противодействие специальным операциям (провокациям, диверсиям), осуществляемым с помощью массмедиа; противодействие враждебному (целенаправленному и деструктивному) идеологическому воздействию; противодействие деструктивным воздействиям, которые осуществляются с помощью массмедиа (разного рода «токсический» контент вроде рекламы деструктивных культов, жестокости, девиантного поведения) (ИБУ, 2014). Каждая из этих задач характеризуется различным соотношением объективных и субъективных факторов.*

*Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее его формирование, использование и развитие в интересах граждан, организаций, государства.*

*Угрозы информационной безопасности – это обратная сторона использования информационных технологий. Источниками таких угроз и вызовов могут быть международные преступные группы хакеров, отдельно подготовленные в сфере ИТ преступники, иностранные государственные органы, террористические группировки, негосударственные организации, политические структуры и неформальные объединения экстремистского толка, транснациональные корпорации, финансово-промышленные группы и т. п.*

*Современная нормативно-правовая база не охватывает все основные элементы, необходимые для эффективного противодействия информационным угрозам в Украине. В то же время, учитывая, многогранность и комплексность этой проблемы, стоит оговорить дальнейшую необходимость научных исследований механизмов обеспечения информационной безопасности в Украине.*

***Ключевые слова:*** *информация, информационная безопасность, медиапространство, социальные сети, средства коммуникации, информационное общество, угрозы, воздействия.*