УДК: 35:316.77:341.1/8
DOI: https://doi.org/10.32689/2617-2224-2019-18-3-144-158

Голованова Наталя Вікторівна,
аспірант 4 курсу кафедри політології та філософії, Харківський регіональний інститут Національної академії державного управління при Президентові України, 61000, м. Харків, просп. Московський, 75, тел.: +38 097 946 90 79, +38 099 146 60 19, e-mail: natalya041162@gmail.com
ORCID: 0000-0002-6729-2226

Голованова Наталья Викторовна,
аспирант 4 курса кафедры политологии и философии, Харьковский региональный институт Национальной академии государственного управления при Президенте Украины, 61000, г. Харьков, просп. Московский, 75, тел.: +38 097 946 90 79, +38 099 146 60 19 e-mail: natalya041162@gmail.com
ORCID: 0000-0002-6729-2226

Holovanova Natalia Viktorivna,
Ph.D. student of the 4th year of the Department of Political Science and Philosophy, Kharkiv Regional Institute of the National Academy of Public Administration under the President of Ukraine, 61000, Kharkiv, avenue Moscow, 75, tel.: +38 097 946 90 79, +38 099 146 60 19, e-mail: natalya041162@gmail.com
ORCID: 0000-0002-6729-2226

ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ ЯК ЄВРОПЕЙСЬКОЇ ДЕРЖАВИ В УМОВАХ СУЧАСНИХ ЗАГРОЗ (АРХЕТИПНИЙ ПІДХІД)

Анотація. Представлено джерела антропоцентричної матриці понять та ідей в інформаційній сфері. Зазначено виклики і загрози інформаційній сфері України. Уточнено зовнішні та внутрішні чинники цих загроз. Розглянуто конкретні факти загроз у світі. Проаналізовано особливості регуляторної політики європейських держав у напрямі протидії загрозам та правового забезпечення інформаційної безпеки як підгалузі інформаційного права. Визначено ландшафт загрози інформаційної безпеки 2019 р. Приведено механізм етнічного лобізму як інструменту "м'якого" права. Наголошено на тенденції прагнення громадян не до безпеки, а до свободи. Виявлено, що заходи безпеки є одночасно факторами обмеження свободи громадян. Підкреслено важливість запуску системи протидії антиукраїнському мовлен-

ню в зоні проведення антитерористичної операції на Сході України у квітні 2018 р. та заходів у межах Рамкової програми співробітництва України з Радою Європи та Євросоюзом. Для протидії пропаганді запропоновано застосовувати та вдосконалювати універсальне міжнародно-правове регулювання медіапростору, будувати єдиний європейський простір. Визначено зміст національних інтересів України згідно з Доктриною інформаційної безпеки України. Об'єктами національних інтересів у інформаційній сфері названо інформацію, інформаційну інфраструктуру і статус суб'єкта в інформаційній сфері. Наголошено на ціннісному наповненні інформаційної політики держави. Реалізацію і виживання окремої особи, суспільства та держави визначено як мету інформаційної політики в умовах сучасних загроз. Безпеку держави, економічне процвітання, розвиток суспільства і гармонійне існування країни у світовому контексті зазначено як результат ефективної інформаційної політики. Запропоновано спиратися на державницькі підходи, притаманні історичному Києву та сучасній українській державі.

Ключові слова: геополітичне протиборство, пропаганда, маніпулювання, фейк, кібервійська, ландшафт загрози, джерела "м'якого" права, етнічний лобізм, національні цінності, системи європейської і національної безпеки, інформаційна безпека, інформаційна інфраструктура.

ИНФОРМАЦИОННАЯ ПОЛИТИКА УКРАИНЫ КАК ЕВРОПЕЙСКОГО ГОСУДАРСТВА В УСЛОВИЯХ СОВРЕМЕННЫХ УГРОЗ (АРХЕТИПИЧЕСКИЙ ПОДХОД)

Аннотация. Представлены источники антропоцентрической матрицы понятий и идей в информационной сфере. Указаны вызовы и угрозы информационной сфере Украины. Уточнены внешние и внутренние факторы этих угроз. Рассмотрены конкретные факты угроз в мире. Проанализированы особенности регуляторной политики европейских государств в направлении противодействия угрозам и правового обеспечения информационной безопасности как подотрасли информационного права. Определен ландшафт угрозы информационной безопасности 2019 г. Приведен механизм этнического лоббизма как инструмента "мягкого" права. Отмечены тенденции стремления граждан не к безопасности, а к свободе. Показано, что меры безопасности являются одновременно факторами ограничения свободы граждан. Подчеркнута важность запуска системы противодействия антиукраинской речи в зоне проведения антитеррористической операции на Востоке Украины в апреле 2018 г. и мероприятий в рамках Рамочной программы сотрудничества Украины с Советом Европы и Евросоюзом. Для противодействия пропаганде предложено применять и совершенствовать универсальное международно-правовое регулирование медиапространства, строить единое европейское пространство. Определено содержание национальных интересов Украины согласно Доктрине информационной безопасности Украины. Объектами национальных интересов в информационной сфере названы информация, информационная инфраструктура и статус субъекта в информационной сфере.

Отмечена важность ценностного наполнения информационной политики государства. Реализация и выживание отдельной личности, общества и государства определены как цель информационной политики в условиях современных угроз. Безопасность государства, экономическое процветание, развитие общества и гармоничное существование страны в мировом контексте указаны как результат эффективной информационной политики. Предложено опираться на государственные подходы, присущие историческому Киеву и современному украинскому государству.

Ключевые слова: геополитическое противоборство, пропаганда, манипулирование, фейк, кибервойска, ландшафт угрозы, источники "мягкого" права, этнический лоббизм, национальные ценности, системы европейской и национальной безопасности, информационная безопасность, информационная инфраструктура.

INFORMATION POLICY OF UKRAINE AS AN EUROPEAN STATE IN CONDITIONS OF CURRENT THREATS (ARCHITECTURE APPROACH)

Abstract. The sources of the anthropocentric matrix of concepts and ideas in the information sphere are presented. The challenges and threats to the information sphere of Ukraine are given. The external and internal factors of these threats are specified. Specific facts of threats in the world are considered. The peculiarities of the European countries' regulatory policy in the area of counteracting threats and legal security of information security as a sub-branch of information law are analyzed. The landscape of the threat of information security 2019 is defined. The mechanism of ethnic lobbying as a tool of soft law is given. It's shown that the tendency of citizens' strivings is not to safety, but to freedom. It is revealed that security measures are simultaneously factors limiting the freedom of citizens. The importance of launching the anti-Ukrainian language counteraction system in the area of the Anti-terrorist operation in the East of Ukraine in April 2018 and activities within the framework of the Framework Cooperation Program of Ukraine with the Council of Europe and the European Union was emphasized. To counter propaganda, it is proposed to apply and improve the universal international legal regulation of media space, to build a single European space. The content of Ukraine's national interests according to the Doctrine of Information Security of Ukraine is determined. Objects of national interests in the information sphere are called information, information infrastructure and status of the subject in the information sphere. It is emphasized on the value-filling of information policy of the state. The realization and survival of an individual, society and state are defined as the goal of information policy in the context of modern threats. State security, economic prosperity, the development of society and the harmonious existence of the country in the global context are indicated as the result of effective information policy. It is suggested to rely on the state-owned approaches inherent in historical Kyiv and the modern Ukrainian state.

Keywords: geopolitical confrontation, propaganda, manipulation, fake, cyber troops, landscape threats, sources of soft law, ethnic lobbying, national values, European and national security systems, information security, information infrastructure.

Постановка проблеми. Щодо сучасної геополітичної ситуації і політики європейських країн у частині застосування військово-політичних механізмів забезпечення безпеки й оборони, в умовах сьогодення на перший план висувається проблема будівництва нової системи європейської і національної безпеки, яка має включати всі наявні інститути безпеки та оборони за чіткого поділу їх функцій. Змінюються традиційні уявлення про символи могутності й способи досягнення світового панування. Раніше йшлося про наземний, повітряний і морський простори, нині йдеться про актуалізацію ролі інформаційного простору та про нове поле геополітичного протиборства — інформаційну сферу. Тому проблема сучасних викликів і загроз інформаційній безпеці України є вкрай актуальною. Панівної ролі набуває Інтернет, незаперечним лідером освоєння якого є США. Однак уже існує думка про необхідність оптимізації шляхів глобальних інформаційних потоків. Тобто можна говорити про те, що світ стоїть на порозі нової сутички за контроль над інформаційним простором і "транспортуванням інформації".

"Безумовно, в сучасних геополітичних умовах зростає значення інформаційного фактора. Чітко простежується тенденція підвищення ролі інформаційного ресурсу держав у загальній системі оборонного потенціалу. До найважливіших його елементів належать інформаційні системи і засоби стратегічного попередження, управління військами і зброєю, навігації, розвідки, радіоелектронної боротьби... Таким чином, геополітичні трансформації зумовлюють характер відносин співробітництва і протиборства у XXI ст. Головна сфера протиборства — інформаційний простір глобального, регіонального і національного рівнів. Геополітичні умови визначають військово-інформаційну політику держави в найбільш важливих сферах геополітичного суперництва і протиборства" [1, с. 44–45].

Агресивне зовнішнє середовище висунуло у 2014–2019 рр. перед Україною, насамперед перед інформаційною політикою держави, нові загрозливі виклики.

Аналіз останніх досліджень і публікацій. Деякі дослідники основними видами загроз інформаційній безпеці називають такі:

- масштабна інформатизація, збільшення залежності воєнного сектору від сучасних інформаційних технологій, спрощення комунікацій та пришвидшення руху інформаційних потоків;
- утворення інформаційної сфери, не прив'язної до державних кордонів;
- перетворення інформаційного простору західних держав у єдиний глобальний інформаційний простір, де домінуючу роль у контролі над ін-

формаційними потоками відіграють США і країни ЄС;

• формування глобальної інформаційної інфраструктури на основі мережі Інтернет, що може розглядатися як посилення просторової взаємозалежності держав;

• витіснення вітчизняних інформаційних агентств, засобів масової інформації із внутрішнього інформаційного ринку та посилення залежності духовної, економічної і політичної сфер громадського життя України від закордонних інформаційних структур;

• маніпулювання інформацією, фейки тощо;

• розробка інформаційної зброї або її елементів майже у 120 країнах світу (за оцінками американських експертів);

• інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку і реалізацію зовнішньої політики держави;

• поширення за кордоном дезінформації про зовнішню політику України;

• порушення прав громадян і юридичних осіб в інформаційній сфері України й за кордоном;

• спроби несанкціонованого доступу до інформації і впливу на інформаційні ресурси, інформаційну інфрастуктуру органів державної влади, які реалізують державну зовнішню політику, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях [1, с. 45–52].

Маємо такі основні групи загроз: інформаційна, інформаційно-технічна, електронний контроль за життям, використання нових інформаційних технологій з політичною метою.

Найсуттєвіші:

• загрози, пов'язані з руйнуванням або деградацією, внутрішнім та зовнішнім, інформаційно-культурного базису суспільства, основним зберігачем якого є система освіти і виховання нових поколінь суспільства;

• загрози, пов'язані з руйнуванням або деградацією продуктивної інформаційної підсистеми суспільства, як-то: наукові, технічні, аналітичні, ідеологічні центри, які створюють або імпортують відповідну інформаційну продукцію та інформаційні технології.

У системі забезпечення національної безпеки держави американські військові дослідники Яргер Річард та Джордж Барбер розглядають таку тріаду, як:

• національні цінності в інформаційній сфері;

• національні інтереси в інформаційній сфері;

• національні цілі в інформаційній сфері.

Згідно з Доктриною інформаційної безпеки України національні інтереси України в інформаційній сфері полягають у:

• дотриманні конституційних прав і свобод людини у можливості отримати інформацію, збереженні та зміцненні цінностей;

• представленні України в міжнародному середовищі та інформуванні українських громадян щодо державної інформаційної політики;

• розвитку сучасних інформаційних технологій;

• захисті інформаційних ресурсів [2].

Об'єктами національних інтересів у інформаційній сфері є інформація, інформаційна інфраструктура і статус суб'єкта в інформаційній сфері. Інформаційна політика держави спрямована на реалізацію і виживання окремої особи, суспільства та держави. Для держави загалом це означає її безпеку, економічне процвітання, розвиток суспільства і гармонійне існування країни у світовому контексті.

Важливе ціннісне наповнення інформаційної політики. Його чинять, як вважають Ч. Лерчі та А. Саїд, окремі громадяни, суспільство, держава, соціально зацікавлені групи та уряд [3, с. 11]. На базі цінностей формуються пріоритети інформаційної політики. Формування пріоритетів має носити системний характер.

М. Вебер вважає, що систему цінностей визначає передусім історична епоха [4, с. 64].

Б. Гогвуд та Л. Ган розглядають національні цінності як переконання, мораль, стандарти та інші конкретні орієнтири, що впливають на вироблення політики на всіх рівнях, бо творять контексти стримування, впливу, спонукання до прийняття учасниками процесу тих чи інших рішень [5, с. 160].

Як зазначається у праці В. Горбуліна та А. Качинського, ціннісним ядром, консолідуючим суспільство, є національна безпека, духовні надбання, добробут, міжнародні зв'язки, патріотизм і соціальна справедливість [6, с. 107].

Метою статті є з'ясування напрямів і принципів інформаційної політики України як європейської держави в умовах сучасних загроз.

Виклад основного матеріалу. З огляду на те, що факт, істина — поняття відносні, а підходи створюються людиною, на наш погляд, важливо одразу зумовити матрицю понять та ідей.

Матрицю понять та ідей визначимо як антропоцентричну, тобто за основу беремо те, що людина є центром Всесвіту і метою всіх подій, що вона замислена та створена Богом за Його образом та подобою.

Першоджерелами й першими законодавцями стали давні священні книги:

- Біблія (XV ст. до н. е. – I ст. н. е.);
- Танах;
- Коран;
- Трипітака (Палійський канон);
- Веди;
- У-Цзин;
- Дао цзан, Чжуан-цзи.

Біблійські заповіді блаженства:

- Блаженні [щасливі] вбогі духом [потребують Духу, усвідомлюють потребу в духовному самовдосконаленні, — духовно удосконалюються], бо їхнє Царство Небесне.
- Блаженні засмучені, бо вони будуть утішені.
- Блаженні лагідні, бо вони успадковують землю.
- Блаженні голодні та спраглі правди, бо вони наситяться.
- Блаженні милостиві, бо вони помилувані будуть.
- Блаженні чисті серцем, бо вони Бога побачать.
- Блаженні миротворці, бо вони синами Божими назвуться.
- Блаженні переслідувані за правду, бо їхнє Царство Небесне.

- Блаженні ви, коли ганьбитимуть вас і гнати і всіляко неправедно злословити за Мене. Радійте і веселіться, бо нагорода ваша велика на небесах! Бо так гнали й пророків, що були перед вами (Мф. 5:3-12).

Виклики і загрози інформаційній безпеці України становлять: наявність проблем формування і реалізації державної інформаційної політики, адекватної викликам і загрозам інформаційній безпеці України; відсутність ефективного інформаційно-аналітичного забезпечення діяльності керівництва держави та органів державної влади; спроби втручання у внутрішні справи України з боку іноземних держав, організацій, груп; використання інформаційного простору іноземними державами з метою інформаційної чи воєнної агресії; поширення негативних інформаційних та інформаційно-технологічних впливів на свідомість людини; створення іноземними державами кібервійськ, кіберпідрозділів у традиційних родах військ, розроблення нових видів інформаційної зброї та зброї кібернетичного характеру; залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції; неналежний рівень інформатизації діяльності державних органів, органів місцевого самоврядування та інших напрямів інформаційної діяльності; недосконалість державної стратегії та системи протидії зовнішній інформаційній експансії у національний інформаційний простір; обмеження свободи слова та поширення в засобах масової інформації культу насильства, жорстокості, зневажливого ставлення до людської і національної гідності, провокування протистояння в суспільстві; реалізація програмно-математичних засобів, що порушують функціонування інформаційних систем, радіоелектронне блокування засобів зв'язку та управління, включення у програмно-технічні засоби прихованих шкідливих функцій; використання неліцензованого і несертифікованого програмного забезпечення, відсутність пріоритетного розвитку національного програмного забезпечення; недостатній рівень розвитку національної інформаційної інфраструктури, низька конкурентоспроможність вітчизняних високотехнологічних виробництв інформаційних технологій, інформаційної продукції та послуг; недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій, відсутність ефективних загальнодержавних та місцевих систем сповіщення, завчасного прогнозування і реагування на надзвичайні ситуації; вияви неправомірного доступу до персональних даних та інформаційних ресурсів органів державної влади і місцевого самоврядування; порушення встановленого порядку збирання, обробки, зберігання і передачі даних; незаконне перехоплення інформації в телекомунікаційних мережах, сепаратистських та інших злочинних виявів в інформаційній сфері; невідповідність юридичної відповідальності сучасним викликам і загрозам інформаційній безпеці; відсутність ефективного демократичного контролю за діяльністю суб'єктів забезпечення інформацій-

ної безпеки, захищеності національної інформаційної інфраструктури та інформаційного простору України. Переважна більшість указаних загроз притаманна різним країнам, однак в умовах соціокультурного та економічного транзиту, який переживає Українська держава і суспільство, ці загрози актуалізуються й загострюються.

Сучасні виклики інформаційній безпеці України, як справедливо зазначають В. Конах та О. Лазоренко, зумовлені як внутрішніми, так і зовнішніми чинниками. Внутрішні — найбільшою мірою пов'язані з відсталістю інформаційних технологій в Україні від провідних країн світу, недостатньою дієвістю органів державної влади та законодавства в інформаційній сфері, а також байдужістю, низьким рівнем розуміння та професійної відповідальності як окремих груп, так і громадян, що нині провадять свою діяльність в інформаційному просторі України. Зовнішні — з намаганнями іноземних суб'єктів впливати на світовий та вітчизняний інформаційний простір з метою забезпечення власних інтересів" [7, с. 74–77].

У цій ситуації на перший план висуваються проблеми інформаційної безпеки, насамперед її інформаційно-психологічної складової. Нині очевидним постає і той факт, що чим більшими інформаційними можливостями володіє держава, тим імовірніше (за інших рівних умов), що вона досягне стратегічних переваг в інформаційному просторі. Це є особливо актуальним для визначення ролі й місця України в сучасних умовах інформаційної глобалізації.

Який досвід політики інформаційної безпеки зарубіжних країн?

Документ СМ (2002)49 проголошує п'ять основних принципів політики безпеки НАТО [8]:

- принцип широти;
- принцип глибини;
- принцип централізації;
- принцип управління доступом;
- принцип персонального контролю.

Важливим завданням НАТО є недопущення актів агресії у кіберпросторі, а також увага до кіберзахисту окремих країн-членів.

П. Корніш з лондонського Королівського інституту іноземних справ пропонує таку класифікацію інформаційних загроз: атаки хакерів-одинаків; організована злочинність у мережах; ідеологічний і політичний екстремізм; інформаційна агресія держав [9].

Корисним є досвід Австрії, Швейцарії, Фінляндії та Ірландії щодо захисту даних, раннього виявлення кіберзагроз і кібератак, підвищення стійкості критичної інфраструктури, зниження кіберризиків, кібершпигунства і кіберсаботажу [10].

Найважливішим аспектом інформаційної безпеки усіх без винятку країн ЄС є захист персональних даних, засади якого визначені директивою 95/46/ЄС "Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних". У документі одночасно декларується прагнення вільного переміщення інформації між країнами – членами ЄС. Нові правила захисту персональних даних (GDPR) посилюють зберігання персональних даних і запровадджують більш

суворе покарання за несвоєчасне повідомлення про витік даних [11]. Активно втілюють нові правила Румунія, Болгарія, Молдова.

Згідно з "Європейськими критеріями безпеки інформаційних технологій" (1991) для країн ЄС важливі захист безпеки та забезпечення цілісності інформаційних ресурсів, і за моделлю тріади (CIA Triad) основними характеристиками інформаційної безпеки є конфіденційність, цілісність і доступність. Проблемами є некоординовані національні підходи, а також відсутність на європейському рівні партнерства між державним та приватним секторами.

Німеччина займається розробленням методів "активної оборони". Подібну роботу веде і Франція.

Польща, Чехія і Словаччина розробили нове законодавство щодо захисту класифікованої інформації на підставі нових принципів.

Угорщина адаптувала до вимог НАТО колишнє законодавство про захист державних та офіційних секретів і першою з постсоціалістичних країн прийняла правовий акт про захист персональних даних.

Національну стратегію кібербезпеки було прийнято в Хорватії.

"За довгостроковими прогнозами, перспективи світового розвитку визначатиме глобальне перегрупування сил у результаті інформаційного прогресу в США, ЄС, Японії, Китаї, Індії та Росії. Передбачається розвиток трьох потужних геостратегічних та інформаційних "центрів світу": американського (США), європейського (Европейський Союз) й азійського (Китай, Індія, Японія). Подібним центром інформаційного впливу в сучасних умовах намагається стати і Російська Федерація. Україна в такій міжнародній конструкції посідає особливе місце завдяки геополітичному розташуванню" [1, с. 46].

"Ми живемо у світі, коли держави (і великі корпорації) переводять на свою користь будь-які технічні новинки, які спочатку здаються досить демократичними. Усе поступово стає керованим з боку держави або великого бізнесу, здатного оплатити витрати на керованість" [12].

Г. Почепцов наводить приклади перемоги держав над потенційно небезпечними для них тенденціями.

Соцмережі Китай, Ізраїль, Росія, США зробили керованими.

Відгуки в інтернет-магазинах здебільшого стали фальшивими.

Голлівуд має представництва усіх американських військових і розвідувальних відомств, які допомагають правильно знімати фільми.

У Британії серйозно вивчають поведінку футбольних уболівальників, а також протестувальників, у США вивчають поведінку натовпу, шукають автоматичне розпізнавання моделей аномальної поведінки пасажира в аеропорту.

Системи розпізнавання і спостереження розташовані на вулицях, у телефонах громадян.

Системною стала й робота з масовою свідомістю, де першість належить Китаю. Китай створив систему "де-екстремізації" для перевиховання свого уйгурського мусульманського населення, а також систему соціального кредиту для всіх: людина набирає бали за хорошу поведінку (наприклад, відвідує своїх старих

батьків) або втрачає їх. З малою кількістю балів неможливо узяти кредит або купити квиток на літак. Є додаток для телефона, який повідомляє, що поруч — боржник.

Також це приклади втручання у вибори інших держав.

Регуляторна політика європейських держав, зокрема, у сфері телерадіомовлення за умов інформаційних загроз беруть до уваги критерії точності, неупередженості, незалежності, відповідальності та встановлення стандартів як критерії підходів.

Світ, який технічно йде вперед, втрачає свої соціальні орієнтири позаду. Це наочно продемонстрували гіганти типу Фейсбук, коли добре сконструйована для заробляння грошей своїм творцям технічна модель зайшла в суперечність з моральними нормами, з людьми, особиста інформація яких є ресурсом, де Фейсбук заробляє свої гроші. А оскільки ця бізнес-модель побудована на монополізмі гігантів, то вони намагаються диктувати ці правила всім.

Щодо фейків, Г. Почепцов стверджує, що відповідь на них або скарга — це журналістика пост-фактум, вона не так ефективна, адже охоплює ширшу аудиторію або фейк охоплює одну аудиторію, а відповідь — іншу. Потрібний, на його думку, попереджаючий інформаційний удар — український контр-наратив [13].

Правове забезпечення інформаційної безпеки є підгалуззю інформаційного права. Ця підгалузь набуває особлиого значення в умовах негативного зовнішнього впливу на інформаційний простір.

На стан інформаційної безпеки впливають:

- зовнішньополітична обстановка у світі;
- внутрішньополітична обстановка у державі;
- наявність потенційних загроз;
- рівень розвитку медіапростору країни.

2015 року “Україна зайняла 5-те місце у світовому рейтингу з ризику зіткнення з веб-загрозами. За третій квартал 2015 року третина (33,7 %) користувачів антивірусних продуктів зіткнулася із загрозами, які розповсюджуються через мережу Інтернет. Проблемою є відсутність оновлення програмного забезпечення та використання піратських програм. Близько 17 % заражень було здійснено на користувачів застарілої Windows XP. Також небезпечними є шифрувальні програми, що вимагають гроші після шифрування файлів, доступ до яких не можливий без спеціального ключа. Великою проблемою є соціальна інженерія. Зловмисники завдяки соціальним мережам, фішинговим та зловмисним сайтам розповсюджують свої програми” [14, с. 87].

Ландшафт загрози інформаційної безпеки постійно розвивається. Щорічно Форум з інформаційної безпеки (ISF) — неприбуткова асоціація, яка досліджує та аналізує питання безпеки та управління ризиками від імені своїх членів — випускає звіт “Загроза небезпеки”, щоб представити перспективу найбільших загроз безпеці протягом двох років.

Найбільшими загрозами до 2019 р. є :

• надмірна залежність від ускладненості й чутливості (ненадійності) зв’язку;

• дії злочинних синдикатів;
• втрата довіри до інформації;
• проблема дотримання законодавчих норм [15].

В умовах сучасних загроз особливого значення набуває етнічний лобізм, який стає інструментом нарощування "м'якої сили" України [16, с. 280–283].

Водночас дослідники відзначають наявність тенденції прагнення громадян не до безпеки, а до свободи. При цьому заходи безпеки виявляються одночасно факторами обмеження свободи громадян [17; 18].

Особливостями філософії Київської Русі по праву стали:
• синкретизм;
• різноманітність підходів і поліфонія;
• кордоцентризм і любомудріє;
• києвоцентризм;
• єрусалимоцентризм і подорож.

Роль української столиці є вирішальною у націєутворюючому, історико-культурному, духовно-ціннісному, людиновимірному, мовному й геополітичному аспектах. Саме Київ як столиця є центром, який цементує єдність держави і забезпечує гармонійне співіснування регіонів України, надає ментальному полю, медіапростору країни національних духовних і естетичних властивостей, притаманних кращим особистостям і втіленим у кращі зразки науки і мистецтва. Прогностично саме Київ здатний бути зразком державницьких підходів.

19 квітня 2018 р. в Україні було оголошено про *запуск системи протидії антиукраїнському мовленню* в зоні проведення Антитерористичної операції на Сході України, розробленої за активної участі Міністерства інформаційної політики, Державної служби спеціального зв'язку та захисту інформації, Комітетів Верховної Ради з питань національної безпеки і оборони та з питань свободи слова та інформаційної політики, Національної ради з питань телебачення і радіомовлення, Служби безпеки України та інших органів державної влади.

Серед заходів у межах Рамкової програми співробітництва (РПС) України з РЄ та ЄС, проект "Свобода медіа в Україні", — створення малопотужного ефірного радіомовлення (мовлення громад) і контроль за дотриманням законодавства щодо мовних квот на радіо та телебаченні.

Дієвими є висновки Резолюції Європейського Парламенту від 23 листопада 2016 року про стратегічні комунікації ЄС для протидії пропаганді (2016/2030 (INI) [19].

Висновки і перспективи подальших досліджень. На порядку денному щодо інформаційної політики України як європейської держави в умовах сучасних загроз стоять:

• універсальне міжнародно-правове регулювання медіапростору, побудова єдиного європейського простору, з урахуванням простору світового;

• забезпечення якісного контенту телерадіопрограм, залучення до участі в передачах вчених, фахівців, експертів, дотримання кодексу мовлення, надавання переваг у частині ретрансляції програмам суспільного мовлення;

• усунення стереотипів;

• риторика миру;

• розвиток перекладацької діяльності й включення до Переліку адаптованих для трансляції в Україні те-

лерадіопрограм, показу фільмів країн Євросоюзу та інших країн світу;

• розвиток і підтримка комунікацій України зі світом, зокрема діалогу інтелектуальних еліт фахівців і експертів у світовому медіапросторі, ініціювання всеукраїнського, всеєвропейського та всесвітнього лінгвістичного діалогу;

• розвиток культурно-освітнього простору як частки соціального простору й медіапростору України епохи метамодерну і популяризація вивчення кожним українцем власної історії, в ідеалі — всезагальної гуманітарної освіти; визнання за університетами та академіями статусу центрів знань і джерел інноваційних ідей у суспільстві;

• запровадження політики ненасильства у суспільстві;

• запровадження на практиці принципів New Public Governance, приборкання "совкових" методів і підходів у інформаційній політиці, впровадження суб'єктно-суб'єктніс-них суспільних відносин, перехід від павутиння ієрархічних зв'язків до мережива взаємозв'язків і влади творчості;

• звернення до національної пам'яті, до філософських ідей Київської Русі, до ідей подорожі, кордоцентризму й відкритості;

• увага до контексту подій, текстів, тверджень; врахування ідей і думок одинаків (дослідників зі специфічним стилем роботи в умовах усамітнення та унезалежнення);

• прагнення пізнати Україну та українця як такого;

• залучення методів лінгвістики, нейронаук, штучного інтелекту, підходів постнекласичних наук;

• подолання захопленості законотворчістю;

• визнання істини як підвалини гуманістичного світогляду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Пилипчук В., Дзьобань О.* Глобальні виклики й загрози національній безпеці в інформаційній сфері [Електронний ресурс] // Вісн. Нац. акад. правових наук України // К. — № 3 (78). — 2014. — Режим доступу: http://nbuv.gov.ua/UJRN/vapny_2014_3_6
2. Указ президента України № 47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України" [Електронний ресурс] // 25.02.2017. — Режим доступу: https://www.president.gov.ua/documents/472017-21374
3. *Lerche Ch., A, Said.* Politics Concepts of International in Global Perspective / Ch. Lerche, A, Said. — USA, 1979. — 336 p.
4. *Вебер М.* Избранное. Образ общества. — Пер. с нем. / М. Вебер. — М.: Юристъ, 1994. — 704 с.
5. *Гогвуд Б., Ган Л.* Аналіз політики для реального світу. — Пер. з англ. А. Олійник; наук. ред. пер. В. Тертичка. — К.: Вид-во Соломії Павличко "Основи", 2004. — 396 с.
6. *Горбуін В., Качинський А.* Засади національної безпеки України. — К.: Інтер-технологія, 2009. — 272 с.
7. *Конах В., Лазоренко О.* Загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації [Електронний ресурс] / В. К. Конах, О. А. Лазоренко // Стратегічні пріоритети. — 2014. — № 2. — С. 73–78. — Режим доступу: http://nbuv.gov.ua/UJRN/spa_2014_2_13

8. *Roberts Al. S.* Entangling Alliances: Nato's security of information policy and the entrenchment of State Secrecy [Online tool]. — 2002. — Available at: https://www.researchgate.net/publication/228222455_Entangling_Alliances_NATO's_Security_Policy_and_the_Entrenchment_of_State_Secrecy
9. *Cornish P.* Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacs. – Brussels: European Parliament. — 2014. — 24 p.
10. National Strategy for Switzerland's protection against cyber risks [Online tool]. — 2012. — Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf
11. 2018 reform of EU data protection rules [Online tool]. — 2016. — https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
12. *Почепцов Г.* Світ базується на інформації та будується нею [Електронний ресурс] // Інтернет-видання. — К.: Детектор медіа. — 2019. — 4 лют. — Режим доступу: https://detector.media/withoutsection/article/144566/2019-02-04-svit-bazuetsya-na-informatsii-ta-buduetsya-neyu/
13. *Почепцов Г.* Как убить фейк, или где украинские контр-нарративы [Электронный ресурс] // Інтернет-видання. — К.: Хвиля. — 2019. — 13 лют. — Режим доступа: https://hvylya.net/analytics/society/kak-ubit-feyk-ili-gde-ukrainskie-kontr-narrativyi.html
14. *Платоненко А.* Сучасні загрози інформаційної безпеки для державних та приватних установ України [Електронний ресурс]. — К.: Сучасний захист інформації. — 2015. — № 4. — 120 с. — Режим доступу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/428
15. *Olavsrud T.* 9 biggest information security threats through 2019 [Online tool]. — 2017. — Available at: https://www.itworld.com/article/3185725/9-biggest-information-security-threats-through-2019.html
16. *Мусієнко І. В.* Етнічний лобізм як інструмент нарощування "м'якої сили" України // Гілея: наук. вісн.: зб. наук. пр. — К. : ВІР УАН. — 2013. — Вип. 77 (№ 10). — 352 с.
17. Інфографіка дня: у Західній Європі аудиторія найбільше довіряє суспільним мовникам [Online resourse]. — 2018. — https://ms.detector.media/mediaprosvita/research/infografika_dnya_u_zakhidniy_evropi_auditoriya_naybilshe_doviryae_suspilnim_movnikam/
18. Які законопроекти можуть дозволити правоохоронцям дізнаватися, що ви читаєте, дивитеся та пишете [Електронний ресурс]. — 2019. — https://detector.media/withoutsection/article/163840/2019-03-05-yaki-zakonoproekti-mozhut-dozvoliti-pravookhorontsyam-diznavatisya-shcho-vi-chitaete-divitesya-ta-pishete//
19. Договори та конвенції Ради Європи, ратифіковані Україною [Електронний ресурс]. — Режим доступу: http://www.coe.int/ru/web/conventions/search-on-states/-/conventions/treaty/country/U

REFERENCES

1. *Pylypchuk, V., Dzoban, O.* (2014). Hlobalni vyklyky y zahrozy natsionalnii bezpetsi v informatsiinii sferi [Global challenges and threats to national security in the information sphere]. Visnyk Natsionalnoi akademii

pravovykh nauk Ukrainy — Bulletin of the National Academy of Legal Sciences of Ukraine, 3 (78), 43–52. Retrieved from http://nbuv.gov.ua/UJRN/vapny_2014_3_6 [in Ukrainian].
2. Ukaz prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku "Pro Doktrynu informatsiinoi bezpeky Ukrainy" vid 25 liutoho 2017 roku, № 47/2017 [Decree of the President of Ukraine "On the decision of the Council of National Security and Defense of Ukraine dated December 29, 2016 "On the Doctrine of Information Security of Ukraine" from February 25 2017, № 47/2017]. www.president.gov.ua. Retrieved from https://www.president.gov.ua/documents/472017-21374 [in Ukrainian].
3. *Lerche Ch., Said A.* (1979). Politics Concepts of International in Global Perspective. Englewood Cliffs: Prentice-Hall [in English].
4. *Weber M.* (1994). Izbrannoe. Obraz obshchestva [Selected. The image of society]. Moscow: Yurist [in Russian].
5. *Gogwood B., Gan L.* (2004). Analiz polityky dlia realnoho svitu [Analysis of politics for the real world]. (A. Oliinyk, Trans). V. Tertychko (Eds.). Kyiv: Vyd-vo Solomii Pavlychko "Osnovy" [in Ukrainian].
6. *Horbuin V., Kachynskyi A.* (2009). Zasady natsionalnoi bezpeky Ukrainy [Principles of National Security of Ukraine]. Kyiv: Inter-tekhnolohiia [in Ukrainian].
7. *Konakh V., Lazorenko O.* (2014). Zahrozy ta vyklyky natsionalnym interesam Ukrainy v informatsiinii sferi v umovakh hlobalizatsii [Threats and challenges to the national interests of Ukraine in the information sphere in the conditions of globalization]. Strategichni priorytety — Strategic priorities, 2, 73-78. Retrieved from http://nbuv.gov.ua/UJRN/spa_2014_2_13 [in Ukrainian].
8. *Roberts Al. S.* (2002). Entangling Alliances: Nato's security of information policy and the entrenchment of State Secrecy. Cornell international law journal, 26(2). Retrieved from https://www.researchgate.net/publication/228222455_Entangling_Alliances_NATO's_Security_Policy_and_the_Entrenchment_of_State_Secrecy [in English].
9. *Cornish P.* (2014). Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacs. Brussels: European Parliament [in English].
10. National Strategy for Switzerland's protection against cyber risks. (2012). www.enisa.europa.eu. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf [in English].
11. 2018 reform of EU data protection rules (n.d.). ec.europa.eu. Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en [in English].
12. *Pocheptsov H.* (February 4, 2019). Svit bazuietsia na informatsii ta buduietsia neiu [World is based on information and is being built by it]. detector.media. Retrieved from https://detector.media/withoutsection/article/144566/2019-02-04-svit-bazuetsya-na-informatsii-ta-buduetsya-neyu/ [in Ukrainian].
13. *Pocheptsov H.* (February 13, 2019). Kak ubit feyk, ili gde ukrainskie kontrnarrativy [How to kill a fake, or where Ukrainian counter-narratives are]. hvylya.net. Retrieved from https://hvylya.net/analytics/society/kak-ubit-feyk-ili-gde-ukrainskie-kontrnarrativyi.html [in Ukrainian].

14. *Platonenko A.* (2015). Suchasni zahrozy informatsiinoi bezpeky dlia derzhavnykh ta pryvatnykh ustanov Ukrainy [Modern threats of information security for state and private institutions in Ukraine]. Suchasnyi zakhyst informatsii — Modern Information Security, 4, 86–90. Retrieved from http://journals.dut.edu.ua/index.php/dataprotect/article/view/428 [in Ukrainian].
15. *Olavsrud T.* (March 28, 2017). 9 biggest information security threats through 2019. www.itworld.com. Retrieved from https://www.itworld.com/article/3185725/9-biggest-information-security-threats-through-2019.html [in English].
16. *Musiienko I. V.* (2013). Etnichnyi lobizm yak instrument naroshchuvannia "miakoi syly" Ukrainy [Ethnic lobbyism as a tool for "soft power" expansion in Ukraine]. Hileia, 77(10), 280–283 [in Ukrainian].
17. Infohrafika dnia: u Zakhidnii Yevropi audytoriia naibilshe doviriaie suspilnym movnykam [Infographics of the day: in Western Europe, the audience trusts social broadcasters most]. (June 19, 2018). ms.detector.media. Retrieved from https://ms.detector.media/mediaprosvita/research/infografika_dnya_u_zakhidniy_evropi_auditoriya_naybilshe_doviryae_suspilnim_movnikam/ [in Ukrainian].
18. *Denysenko L.* (March 5, 2019). Yaki zakonoproekty mozhut dozvolyty pravookhorontsiam diznavatysia, shcho vy chytaiete, dyvytesia ta pyshete [What laws can allow law enforcement officers to know what you read, watch and write]. detector.media. Retrieved from https://detector.media/withoutsection/article/163840/2019-03-05-yaki-zakonoproekti-mozhut-dozvoliti-pravookhorontsyam-diznavatisya-shcho-vi-chitaete-divitesya-ta-pishete/ [in Ukrainian].
19. Dohovory ta konventsii Rady Yevropy, ratyfikovani Ukrainoiu [Agreements and conventions of the Council of Europe, ratified by Ukraine]. (n.d.). www.coe.int. Retrieved from http://www.coe.int/ru/web/conventions/search-on-states/-/conventions/treaty/country/U [in Ukrainian].