DOI: https://doi.org/10.26642/sas-2025-5(11)-19-25
УДК 327(437)

Корнійчук Любов
кандидат історичних наук
Національний університет «Острозька академія»
https://orcid.org/0000-0002-0541-5884

Матвійчук Наталія
кандидат історичних наук
Національний університет «Острозька академія»
https://orcid.org/0000-0003-0011-3681

Інформаційна політика Чеської Республіки як інструмент забезпечення інформаційної безпеки під впливом російсько-української війни

Анотація. У цій публікації проаналізовано сучасну інформаційну політику Чехії як інструмент забезпечення інформаційної безпеки в умовах російсько-української війни. Метою розвідки є дослідження особливостей реалізації інформаційної політики Чеської Республіки в умовах посилення гібридних впливів російської федерації. У статті простежено розвиток законодавства Чехії у сфері інформаційної безпеки, проаналізовано діяльність та роль відповідних державних структур. Аналізується вплив російсько-української війни на трансформацію інформаційної політики Чеської Республіки. Окрему увагу приділено з'ясуванню ефективності інформаційної політики країни в контексті забезпечення інформаційної безпеки.

У статті застосовано низку загальних та спеціальних методів, які в комплексі дозволяють досягти поставленої мети. У роботі використано порівняльний метод, контент-аналіз та моделювання. Отримані результати свідчать, що Чеська Республіка з початку повномасштабного вторгнення росії в Україну суттєво вдосконалює методи боротьби з інформаційними загрозами. Значну увагу в країні приділено створенню належної законодавчої бази, створено низку спеціалізованих державних інституцій, які забезпечують безпеку країни в інформаційній сфері. Водночас важливо, що поряд з цим проведена значна просвітницька робота серед населення Чехії для формування розуміння та вмінь сприйняття інформації в умовах постійних гібридних впливів (з боку впливових акторів міжнародних відносин).

Доведено, що інформаційна політика Чеської Республіки є ефективним інструментом забезпечення інформаційної безпеки країни попри значні впливи російсько-української війни. Прикметно, що Чехія в цьому контексті активно співпрацює із партнерами по НАТО та ЄС, що дозволяє більш ефективно та продумано протидіяти намаганням росії впливати на інформаційний простір країни.

Ключові слова: інформаційна політика; інформаційна безпека; дезінформація; загрози; російсько-українська війна.

Актуальність теми. Швидкі темпи розвитку інформаційно-комунікаційних технологій у XXI ст. актуалізували низку нових ризиків та загроз у сфері інформаційної безпеки держав, яка є невід'ємною складовою національної безпеки. У сучасному геополітичному середовищі гібридні війни стали досить поширеною формою глобального протистояння держав. Початок російсько-української війни у 2014 р. змінив безпекову ситуацію в Європі і стимулював європейські держави до початку перегляду своїх безпекових стратегій та інформаційної політики. Однак лише повномасштабна російська агресія проти України в лютому 2022 р. змусила держави пришвидшити зміни в стратегії реагування на інформаційні та інші безпекові загрози. Однією із держав-членів ЄС, що продемонструвала активність у боротьбі з російською пропагандою та дезінформацією, кіберзлочинністю і кібертероризмом стала Чеська Республіка (далі – ЧР). Дослідження політики Чехії у сфері інформаційної безпеки є актуальним з огляду на важливість і можливість використання Україною досвіду держави у боротьбі з гібридними загрозами, а також сприяє кращому розумінню ролі державних інституцій у цьому процесі. Зважаючи на конфліктогенний потенціал сучасного міжнародного середовища, вивчення та аналіз чеської інформаційної політики та еволюції її підходів до інформаційної безпеки сприяє формуванню цілісної картини політики інформаційної безпеки держав ЄС.

Аналіз останніх досліджень та публікацій. Вивчення питання інформаційної політики та інформаційної безпеки ЧР актуалізувалося на фоні посилення гібридних загроз після початку російсько-української війни, а особливо після повномасштабного російського вторгнення в Україну. Однак в українській науковій думці немає досліджень, які цілісно розкривають тематику наукової статті. Окремі

аспекти, що дотичні до аналізованої теми та стосуються безпекової політики ЧР загалом, російської пропаганди в Чехії, реакції держави на російсько-українську війну тощо досліджували у своїх працях такі автори, як В.Алексишинець [1], В.Андрейко [2], С.Віднянський [3], Л.Корнійчук [4]. Важливу роль для дослідження відіграли праці зарубіжних аналітиків та науковців, що присвячені вивченню впливу гібридної війни на ЧР, захисту кіберпростору, а також впливу росії на ЧР, особливо через поширення дезінформаційних компаній. Авторами таких праць є: Ж.Бакес-Кесада, Г.Колом-П'єлла (J.Baqués-Quesada, G.Colom-Piella) [12], Дж.Еберле, Дж.Даніель (J.Eberle, J.Daniel) [22], Ш.Данікс, Й.Смолік (Š.Danics, J.Smolík) [21], Л.Кабада (L.Cabada) [18], М.Мареш (M.Mareš) [26], (I.Smoleňová) [30], А.Яцух (A.Jacuch) [24]. Водночас питання особливостей сучасної політики Чехії щодо забезпечення інформаційної безпеки є недостатньо вивченим, що зумовлює дослідницький інтерес до запропонованої для розгляду теми.

Метою статті є аналіз особливостей реалізації інформаційної політики Чехії під впливом російсько-української війни та з'ясування її ефективності у контексті забезпечення інформаційної безпеки держави.

Викладення основного матеріалу. У сучасному світі, де неабиякого розвитку досягли інформаційно-комунікаційні технології, штучний інтелект та цифрові інновації, інформаційна безпека набуває дедалі важливого значення для кожної держави. Інформаційна безпека є однією з важливих структурних складових національної безпеки держави. Сьогодні інформація є не лише основою в комунікації між акторами міжнародних відносин, але й стратегічно важливим ресурсом, що безперечно впливає на внутрішню ситуацію, формує імідж країни на міжнародній арені тощо. З огляду на це інформація є не лише додатковим інструментом, а стратегічно важливим активом кожної країни, що прагне до розвитку та забезпечення безпеки громадян.

Інформаційна політика в цьому контексті покликана сприяти контролю над інформаційними потоками та роботою інформаційних систем. Інформаційну політику можна визначити як сукупність принципів, способів та механізмів роботи суб'єктів (держави, міжнародних організацій тощо), яка спрямована на збирання, створення, обробку, доступ, зберігання, використання, поширення, передачу, захист інформації. У широкому контексті інформаційна політика містить низку основних складових: створення і поширення інформації (з боку влади країни), розробку, контроль та використання інформаційної інфраструктури, інформаційну та юридичну інфраструктуру [5].

Зважаючи на посилення конфронтаційності у сучасних міжнародних відносинах, держави, прагнучи гарантувати національну безпеку та реагуючи на низку гібридних загроз, змушені приділяти значну увагу забезпеченню інформаційної безпеки, розробці норм, правил, стратегій інформаційної політики. Важливими тут є механізми, що спрямовані на захист інформаційного простору держави, систем та інституцій, які забезпечують інформаційну безпеку. До таких механізмів належать: організаційні (створення загальнодержавних систем, що об'єднують усі інституції), технічні (створення та контроль належного функціонування інфраструктури, технічний контроль), правові (розробка та регулювання на законодавчому рівні відповідних нормативних документів, які регулюють сферу інформаційної політики та інформаційної безпеки), освітньо-наукові (співпраця з експертними, науковими та освітянськими колами для навчання фахівців у галузі інформаційної політики), інформаційні (інформування населення країни та світової громадськості щодо стану інформаційної безпеки, загроз, інформаційної політики держави тощо, співпраця з міжнародними організаціями, інституціями для впровадження міжнародних стандартів інформаційної безпеки). Комплексне застосування усіх механізмів дозволяє державам формувати продуману і виважену інформаційну політику в сучасних умовах, адже це дозволяє захищати інформаційний простір. Кожна держава може зазнавати гібридних впливів, інформаційних атак, поширення дезінформації та пропаганди, що підривають стабільність в країні. Водночас керована і добре продумана інформаційна політика дозволяє протистояти цим загрозам, зберігати внутрішню стабільність, зменшувати вразливість громадян до маніпуляцій, ефективно захищати критично важливу інфраструктуру. Актуальними ці питання є й для ЧР, яка з часу повномасштабного вторгнення росії в Україну піддається російським інформаційним атакам, дезінформації та потужним пропагандистським кампаніям.

Основні засади чеської інформаційної політики були затверджені постановою уряду № 525 від 31 травня 1999 р. у документі «Державна інформаційна політика – шлях до інформаційного суспільства» [31]. У документі зазначалося, що невід'ємною частиною концепції державної інформаційної політики та її реалізації є міжнародне співробітництво, метою якого є поступова інтеграція ЧР у світовий процес створення інформаційного суспільства та визначено вісім пріоритетних напрямів інформаційної політики: інформаційна грамотність, інформаційна демократія, розробка інформаційних систем державного управління, комунікаційна інфраструктура, надійність та безпека інформаційних систем і захист персональних даних, електронна комерція, прозоре економічне середовище, стабільне та безпечне інформаційне суспільство [31]. Постановою Уряду Чеської Республіки № 961 від 24 листопада 2014 р. було створено Урядову раду з питань інформаційного суспільства – постійно діючий управлінський, дорадчий, ініціативний і координаційний орган уряду, відповідальний за реалізацію програми «Цифрова Чеська Республіка», спрямованої на реформування системи цифрових послуг у державному управлінні. Діяльність Ради охоплює розвиток електронного

урядування, впровадження Інформаційної концепції ЧР, використання інформаційно-комунікаційних технологій, зокрема штучного інтелекту, автоматизацію та роботизацію у державному секторі, а також координацію питань інформаційного суспільства й інших аспектів цифрового порядку денного в сукупності з його європейським виміром [33]. Інформаційна концепція ЧР була затверджена у 2018 р. і містить цілі ЧР в галузі електронного врядування, принципи розробки інформаційних систем державного управління та принципи управління ними [23].

Російсько-українська війна стимулювала перегляд безпекової політики держави загалом, а також інформаційної безпеки, зокрема. Постановою уряду від 28 червня 2023 р. було затверджено оновлену Безпекову стратегію Чеської Республіки [17], в якій зазначалося, що держава повинна бути здатною протистояти ворожим діям у кібернетичній, інформаційній, економічній та розвідувальній сферах [17, с. 4], а одним із безпекових інтересів визначено забезпечення комунікаційної, інформаційної та кібербезпеки й оборони ЧР та відкритий, стабільний і безпечний кіберпростір [17, с. 9]. У концепції також йдеться про те, що протидія дезінформації, інформаційним операціям та спробам маніпулювати інформаційним простором, які здійснюються на користь іноземних державних суб'єктів і спрямовані на підрив демократичного характеру держави та її безпеки, є важливою складовою політики Чехії [17, с. 19]. Важливо, що у документі констатовано потребу комплексного підходу для захисту від загроз, який би вміщував «підтримку освіти в галузі медіа та інформаційної грамотності, зміцнення громадянського суспільства, стратегічних державних комунікацій, розбудову потенціалу для виявлення та аналізу загроз, ефективну співпрацю і координацію державних установ, що діють у цій галузі, а також співпрацю в межах ЄС та НАТО» [17, с. 19]. Як бачимо, у стратегії акцентовано на важливості інформаційної безпеки та боротьби із кіберзагрозами як важливих складових національної безпеки загалом.

Важливим стало створення у 2017 р. Національного агентства кібернетичної та інформаційної безпеки (Národní úřad pro kybernetickou a informační bezpečnost, NÚKIB), яке стало центральним органом з питань кібербезпеки, зокрема захисту інформації. Слід підкреслити, що основні принципи, на яких базується кібербезпека ЧР, її майбутній стратегічний напрям у сфері кібербезпеки та основне бачення у цій сфері було описано у затвердженій агентством у 2020 р. Національній стратегії кібербезпеки Чеської Республіки на 2021–2025 рр. [27]. Стратегія зосереджена на побудові стійкого суспільства та інфраструктури, здатної ефективно протидіяти кіберзагрозам, у ній акцентується на розвитку можливостей прогнозування, виявлення та ефективного реагування на кібератаки, а також на міжнародній співпраці. У 2021 р. було прийнято Національну стратегію протидії гібридним загрозам [28], яка визначає цілі та інструменти, необхідні для захисту життєво важливих, стратегічних та інших важливих інтересів ЧР. У Стратегії зазначено, що ЧР зазнає гібридного впливу в таких сферах, як ідейно-ціннісні орієнтири суспільства та конституційно-правовий устрій держави, економіка, безпека та оборона, тому держава посилюватиме можливості раннього виявлення ворожої гібридної діяльності та своєчасного реагування на неї в межах своєї системи безпеки [28]. Також із метою більш ефективного обміну інформацією задекларовано необхідність створення оптимізованих платформ в межах Ради державної безпеки та створена посада координатора порядку денного протидії гібридним діям [28].

Загалом гібридні загрози дуже інтенсивно обговорювалися в державі протягом кількох років (перша пряма згадка з'являється в Аудиті національної безпеки 2016 р.) і з 1 січня 2017 р. у складі Міністерства внутрішніх справ почав діяти Центр боротьби з тероризмом та гібридними загрозами (з 1 липня 2022 р. – Центр проти гібридних загроз (Centrum proti hybridním hrozbám), а у відповідь на повномасштабну російську агресію проти України Міністерство оборони ЧР у грудні 2022 р. узгодило з ЄС спільний інструмент для захисту від гібридних загроз – Гібридний інструментарій (Hybridní Toolbox, EUHT) [25]. Зокрема, також у грудні 2022 р. урядом було створено нову посаду Радника з національної безпеки (зайняв тодішній радник прем'єр-міністра Томаш Пояр) з метою координації з питань гібридних загроз, дезінформації та інших серйозних надвідомчих питань безпеки, а також для забезпечення співпраці між розвідувальними та безпековими службами задля ефективності їхніх дій [29]. На засіданні 7 грудня 2023 р. уряд ЧР затвердив План дій Національної стратегії протидії гібридним загрозам на 2024–2025 рр., у якому завдання сформовані відповідно до трьох стовпів стратегії: системний та цілісний підхід, зміцнення стійкості суспільства, критичної інфраструктури та держави, а також здатність до адекватного реагування [25]. Для прикладу, на Міністерство закордонних справ покладалося завдання здійснення систематичного моніторингу та аналізу впливу гібридних операцій у засобах масової інформації і публічному онлайн-просторі у сферах, пов'язаних із захистом та просуванням зовнішньополітичних інтересів ЧР [25]. Крім того, 14 листопада 2024 р. було опубліковано постанову, якою Рада державної безпеки затвердила Національну політику криптографічного захисту секретної інформації на період 2024–2030 рр. з перспективою до 2040 р., розроблену Національним агентством кібербезпеки та інформаційної безпеки [16]. Схвалення цього документу стало важливим кроком до посилення боротьби із кіберзагрозами.

Загалом на інституційному рівні відповідальність за виконання зазначених вище стратегій покладається на Міністерство оборони, Міністерство промисловості та торгівлі, Міністерство внутрішніх справ, Міністерство закордонних справ, Міністерство освіти, молоді та спорту, Національне агентство кібербезпеки та інформаційної безпеки. Водночас важливу роль у системі державних органів ЧР відіграє

Служба безпеки та інформації ЧР (Bezpečnostní informační služba), яка є розвідувальною установою, що передає знайдену інформацію президенту Республіки, уряду, державним та поліцейським органам. Також ця Служба займається отриманням, збором та оцінкою інформації, що стосується: загрози тероризму; діяльності, яка загрожує безпеці або значним економічним інтересам держави; діяльності іноземних розвідувальних служб на території ЧР, намірів або дій, спрямованих проти демократичних основ, суверенітету та територіальної цілісності ЧР; діяльності організованої злочинності; діяльності, що загрожує секретній інформації [20].

Варто підкреслити, що після початку повномасштабної російсько-української війни ЧР посилила боротьбу з дезінформацією як однією із гібридних загроз, що може послаблювати довіру до державних інституцій і впливати в інтересах інших держав на громадську думку. 15 лютого 2023 р. урядом схвалено «Аналіз готовності Чеської Республіки до протидії серйозній хвилі дезінформації», де вказано, що ЧР не має концептуальних, організаційних, кадрових, процедурних, правових чи інших інструментів та можливостей, які були б ефективними у реагуванні на потенційну атаку проти неї, спричинену навмисно створеною або спонтанно згенерованою серйозною хвилею дезінформації [11]. Таким чином, питання боротьби з дезінформацією досі залишаються актуальними для інформаційної безпеки ЧР.

Зауважимо, що колишній прем'єр-міністр ЧР А.Бабіш вважався противником активної боротьби із дезінформацією. За його каденції діяльність Центру боротьби з тероризмом та гібридними загрозами була досить обмеженою і навіть у липні 2021 р. під час дебатів у Раді національної безпеки щодо звіту про дезінформацію, підготовленого Центром, прем'єр-міністр відклав його, попросивши час для переробки матеріалу, тобто фактично він відхилив рекомендацію централізувати боротьбу з дезінформацією під керівництвом згаданого департаменту. Оскільки останнє засідання Ради національної безпеки перед парламентськими виборами у жовтні 2021 р. було скасовано, то і перероблений звіт не обговорювався [18, с. 377]. Обмежена діяльність уряду Бабіша проти дезінформаційних кампаній стимулювала виявлення таких кампаній та джерел дезінформації неурядовими організаціями: Празький інститут досліджень безпеки (PSSI), Чеські ельфи (Čeští elfové), Manipulátori.cz, Demagog.cz, проєкт «NELEŽ» як чеська франшиза Глобального індексу дезінформації тощо [18, с. 378]. Із березня 2022 р. до лютого 2023 р. існувала посада Урядового, уповноваженого з питань ЗМІ та дезінформації, однак вона була скасована і повноваження були передані Раднику з питань національної безпеки. Департамент, що підпорядковувався Урядовому уповноваженому розробляв у 2022 р. План дій щодо протидії дезінформації, однак він не був оприлюднений офіційними джерелами і піддавався критиці через приховування імен експертів, що його розробляли, незрозумілість процедури ухвалення та дій, а також суперечливі способи боротьби із дезінформацією в ЗМІ тощо [19].

До початку російської агресії щодо України в країнах Європи, зокрема й у ЧР, діяла російська агентурна мережа, яка збирала інформацію для поширення свого впливу. Із початком повномасштабного вторгнення така діяльність більше активізувалася й перейшла на інший рівень. Міністр внутрішніх справ ЧР Віт Ракушан у 2024 р. заявляв про кратне збільшення активності росії у сфері кібершпіонажу та кібератак, водночас міністр закордонних справ країни Ян Ліпавський зазначав про використання росіянами різних застосунків та хакерських груп для атак на чеську інформаційну інфраструктуру та безпеку країни загалом [8]. У 2025 р. у виступі на конференції «Стійка Європа» Ян Ліпавський підкреслив, що співпрацюючи разом, російські хакери та пропагандисти відповідальні за понад 80 % маніпуляцій в інформаційній сфері Європи [9].

Варто зазначити, що вже у щорічному звіті про діяльність Служби безпеки та інформації ЧР за 2021 р. (опублікований 17.10.2022 р.) наголошено на тому, що російські спецслужби відповідальні за вибухи на складах боєприпасів біля с. Врбетиці у жовтні 2014 р., і змінюється сприйняття росії, яка тепер створює фундаментальну загрозу для безпеки ЧР, особливо після вторгнення в Україну [13]. У звіті за 2022 р. підкреслюється, що після 24 лютого 2022 р. росія активізувала дезінформаційні кампанії на території ЧР, пов'язуючи війну в Україні з соціально чутливими темами, крім того наратив про так звану українізацію чеської держави став об'єднувальною ланкою для дезінформаційних вебсайтів [7, с. 4]. 25 лютого 2022 р. було заблоковано вісім вебсайтів, які поширювали дезінформацію про російсько-українську війну, а 1 березня 2022 р. чеські мобільні оператори заблокували шість дезінформаційних вебсторінок чеською мовою, що також поширювали фейки про війну [18, с. 384]. Важливим кроком у боротьбі з російською пропагандою стало підписання 17 липня 2025 р. Президентом ЧР Петером Павелом закону, що вносить поправку до Кримінального кодексу країни, яка криміналізує пропаганду комуністичної ідеології, прирівнюючи її до нацистської [10].

У російських дезінформаційних кампаніях у Чехії, метою яких був вплив на чеську громадськість, домінувала тема надання допомоги Україні. Так, згідно зі звітом Служби безпеки та інформації ЧР за 2023 р., ця тематика була предметом операції впливу, керованої з росії Віктором Медведчуком, а роль місцевого координатора цієї операції виконував Артем Марчевський, який заснував і керував у Празі онлайн-медіа «Voice of Europe» [14, с. 11]. Метою цієї операції було формування громадської думки та створення умов для впливу на кандидатів на виборах до Європейського парламенту 2024 р. Поза тим, інформаційний вплив на чеську громадськість тривалий створювали також російські державні ЗМІ, зокрема Sputnik. Хоча це медіа не може через санкції в ЄС діяти як повноцінний засіб масової

інформації, проте його діяльність у Чехії продовжувалася також протягом 2023 р., а саме через деякі інтернет-сайти та канали [14, с. 12].

Міністерство закордонних справ ЧР було мішенню російських фішингових атак, зокрема постраждали сигнальні системи і мережі чеського національного залізничного оператора České dráhy. Інформаційна інфраструктура різних чеських установ та організацій з початку війни в Україні неодноразово ставала мішенню так званих «проросійських патріотичних хакерських груп» [14, с. 15]. Крім того, поширеним стало так зване онлайн-вербування на платформі Telegram («агенти Telegram»), де завербовані агенти виконують різноманітні завдання: від перевезення людей і вантажів, фотографування та зйомки конфіденційних об'єктів, таких як військові бази чи пункти перевалки військової допомоги до України, до підпалів та створення загрози життю цивільного населення [15, с. 15]. Така діяльність спрямована також на психологічний вплив на населення, зокрема залякування чеських громадян, створення негативного образу України та поширення ідеї про те, що допомога Україні шкодить для ЧР.

У 2024 р. Служба безпеки та інформації ЧР зафіксувала активність кіберсуб'єктів, пов'язаних із російськими розвідувальними службами. Найактивнішою була діяльність APT28, що зв'язана з Головним розвідувальним управлінням росії, яка зосереджується переважно на військовій справі, міжнародних відносинах, політиці, енергетиці та оборонній, авіаційній і космічній галузях. Використовуючи вразливості MS Outlook для отримання даних для входу, APT28 спрямувала кібератаки на низку чеських державних установ [15, с. 16]. Невдовзі після початку війни в Україні був створений канал «Selský rozum», діяльність якого теж пов'язана з російськими спецслужбами. Наприклад, у лютому 2024 р. канал поширив відкритий заклик до збору інформації про одного із чеських виробників ракет та його співробітників, адже росія критикує ЧР за постачання зброї Україні, зокрема за ймовірне використання чеської зброї проти російських цивільних осіб і намагалася перенести цей наратив у чеське медіасередовище [15, с. 20].

Загалом для втручання в інформаційний простір ЧР росія використовує широкий набір способів та методів: кібератаки, викрадення даних, втручання в роботу критичної інфраструктури, поширення дезінформації та фейків, інформаційно-психологічні прийоми. Із часу повномасштабного вторгнення росії в Україну російська дезінформація та кібератаки в ЧР лише посилилися. Така ситуація змушує владу країни уважно ставитися до інформаційної безпеки, формувати інформаційну політику, яка б відповідала цим загрозам. Попри всі намагання росії, система інформаційного захисту, яка на сьогодні сформована у ЧР, є ефективною, адже країна протистоїть російським наративам та численним атакам в інформаційній сфері. Свідченням цього є звіт Служби безпеки та інформації ЧР за 2024 р., у якому вказується, що попри витрачені зусилля та кошти, росії не вдалося досягти помітних результатів [32]. Інституція, залучаючи усі доступні методи боротьби, протистоїть інформаційним впливам рф.

Варто підкреслити, що не лише росія прагне поширювати свій інформаційний вплив в Чехії, а ще й Китай. Щоправда тоді як Китай фінансово підтримує ЗМІ та осіб, які бажають поширювати виключно свій позитивний образ, щоб вплинути на його сприйняття громадянами Чехії, росія зосередилася на своїй довгостроковій стратегії спроб використати події в ЧР для розпалювання заворушень у чеському суспільстві та для цілей внутрішньої пропаганди [15, с. 20]. Враховуючи побоювання з приводу китайських сервісів штучного інтелекту, в Чехії у липні 2025 р. рішенням Національного агентства з інформаційної безпеки було заблоковано DeepSeek, адже в агентстві вважають, що використання продуктів DeepSeek є загрозою кібербезпеці держави, а продукти цієї компанії можуть потенційно використовуватися КНР у розвідувальних цілях, особливо з огляду на попередні кампанії з кібершпіонажу проти Чехії та інших країн НАТО і ЄС [6].

Висновки та перспективи подальших досліджень. Війна в Україні стала каталізатором системних змін у багатьох аспектах функціонування чеської держави. Тож інформаційну політику ЧР формує відповідно до тих викликів, які постають перед країною. Попри численні намагання росії впливати на громадян та втручатися в інформаційний простір, в ЧР створена відповідна інфраструктура, яка дозволяє мінімізувати негативні впливи та формувати безпечний інформаційний простір. Реагуючи на виклики, які спровокувала російсько-українська війна, можна виокремити низку досягнень у сфері інформаційної безпеки ЧР. Варто підкреслити значну увагу влади країни на формування інституційної бази для боротьби із гібридними загрозами (NÚKIB, Centrum proti hybridním hrozbám, Bezpečnostní informační služba та ін.), які активно протидіють російським впливам. Важливим кроком було прийняття цілісної безпекової стратегії, концепції боротьби з дезінформацією та напрацювання відповідної нормативно-правової і регулятивної бази. Не менш значущою є співпраця в галузі інформаційної безпеки із партнерами по ЄС та НАТО, імплементація відповідних міжнародних норм та угод. Здійснено низку зусиль щодо покращення стратегічної комунікації та захисту від дезінформації, зокрема через введення посади Радника з національної безпеки в Апараті уряду ЧР як надвідомчого координатора з питань гібридних загроз, дезінформації та інших серйозних питань безпеки, а також як платформу для координації та комунікації між структурами політики безпеки, щоб забезпечити тіснішу співпрацю між розвідкою та силами безпеки задля ефективності дій проти дезінформації та гібридних загроз. Варто згадати і про посаду Урядового уповноваженого з питань ЗМІ та дезінформації, яка існувала з лютого 2022 р. до березня 2023 р.

Водночас значну увагу (інформаційну, освітню та фінансову підтримку) було приділено підвищенню цифрової грамотності населення країни загалом шляхом впровадження інформаційних кампаній, освітніх курсів тощо. Країна виділила значні ресурси на технічне оснащення й підготовку фахівців у сфері кібероборони. Зважаючи на всі сучасні виклики, ЧР і надалі має продовжувати співпрацю з міжнародними партнерами та розвивати технічні спроможності, які б забезпечували сталу безпеку країни в інформаційному просторі. Інформаційна політика держави трансформується і поступово перетворюється в ефективний інструмент забезпечення інформаційної безпеки ЧР.

Попри те, що російська агресія прискорила формування інституційної бази і стимулювала конкретні кроки до забезпечення інформаційної безпеки, для ЧР варто звертати увагу на подальше підвищення обізнаності суспільства про ситуацію щодо маніпуляцій інформацією шляхом моніторингу, виявлення та аналізу відкритих джерел інформації; протидіяти іноземному втручанню та маніпуляціям через проєкти підвищення обізнаності, передові технологічні рішення та кращу координацію; посилити співпрацю з громадянським суспільством в сфері боротьби з дезінформацією, активізувати участь у міжнародних ініціативах по боротьбі із гібридними загрозами. З огляду на досить динамічний характер сучасних інформаційних загроз, розвиток штучного інтелекту тощо перспективним напрямком для подальшого вивчення є порівняльний аналіз інформаційної політики ЧР з політикою інших держав регіону, що стикаються із подібними викликами у контексті російсько-української війни, дослідження цифрової дипломатії Чехії, поглиблений аналіз дієвості окремих ініціатив у сфері забезпечення інформаційної безпеки та їх суспільна оцінка в ЧР тощо.

References:

1. Aleksyshynets, V.V. (2024), «Propahanda RF u Chekhii: zahroza informatsiinoi bezpeky yak dosvid postiuhoslavskoho prostoru», *Interaction of the experience of post-yugoslav and ukrainian areas: cultural, linguistic, literary, artistic, historical, and journalistic aspects*, international scientific conference, 23–24 february, Slovenia, Latvia, pp. 129–132.
2. Andreiko, V. (2023), «Viina Rosii proty Ukrainy: ohliad mediinoho prostoru Chekhii ta Slovachchyny», *Mizhnarodnyi naukovyi visnyk*, zb. nauk. pr., DVNZ «UzhNU», Uzhhorod, Vol. 1–2 (27–28), pp. 25–34.
3. Vidnianskyi, S. (2023), «Evoliutsiia polityky Slovachchyny ta Chekhii shchodo viiny rosii proty Ukrainy (do 30-richchia proholoshennia nezalezhnosti Slovatskoi ta Cheskoi respublik)», *Ukraina dyplomatychna. Naukovyi shchorichnyk*, Vol. 24, pp. 62–76.
4. Korniichuk, L. (2024), «Evoliutsiia bezpekovoi polityky Cheskoi Respubliky pid vplyvom rosiisko-ukrainskoi viiny», *Filosofiia ta politolohiia v konteksti suchasnoi kultury*, Vol. 16 (1), pp. 188–199, doi: 10.15421/352435.
5. Mokhova, Yu.L. and Lutska, A.I. (2018), «Sutnist ta osnovni napriamky derzhavnoi informatsiinoi polityky Ukrainy», *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, No. 12, [Online], available at: http://nbuv.gov.ua/UJRN/Duur_2018_12_15
6. «Chekhiia zablokuvala DeepSeek cherez poboiuvannia, shcho dani korystuvachiv vytechut u Kytai», *UNIAN*, [Online], available at: https://www.unian.ua/techno/neiroseti/chehiya-zablokuvala-deepseek-cherez-poboyuvannya-shcho-dani-koristuvachiv-vitechut-u-kitay-13066080.html#goog_rewarded
7. Palyvoda, V.O. (2023), «Otsinka spetssluzhbamy Cheskoi Respubliky bezpekovoi sytuatsii v kraini na navkolo nei», *Natsionalnyi instytut stratehichnykh doslidzhen*, [Online], available at: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/otsinka-spetssluzhbamy-cheskoyi-respubliky-bezpekovoyi
8. «MZS Chekhii vyklykalo rosiiskoho posla cherez kiberataky», *Suspilne novyny*, [Online], available at: https://suspilne.media/740041-mzs-cehii-viklikalo-rosijskogo-posla-cerez-kiberataki/
9. «Rosiia vidpovidaie za ponad 80% informatsiinykh manipuliatsii v Yevropi, – hlava MZS Chekhii», *RBK-Ukraina*, [Online], available at: https://www.rbc.ua/rus/news/rosiya-vidpovidae-ponad-80-informatsiynih-1748521318.html
10. «Chekhiia pryrivniala komunizm do natsyzmu, za propahandu – kryminalne pokarannia», *Ukrinform*, [Online], available at: https://www.ukrinform.ua/rubric-world/4016399-cehia-pririvnala-komunizm-do-nacizmu-i-zaprovadila-kriminalne-pokaranna-za-jogo-propagandu.html
11. «Analýza připravenosti České republiky čelit závažné dezinformační vlně», *Ministerstvo vnitra České Republiky*, [Online], available at: https://mv.gov.cz/chh/clanek/analyza-pripravenosti-ceske-republiky-celit-zavazne-dezinformacni-vlne.aspx
12. Baqués-Quesada, J. and Colom-Piella, G. (2021), «Russian Influence in the Czech Republic as a Grey Zone Case Study», *Politics in Central Europe*, Vol. 17, Iss. 1, pp. 29–56.
13. «Bezpečnostní informační služba. Výroční zpráva 2021», *Bezpečnostní informační služba*, [Online], available at: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf
14. «Bezpečnostní informační služba. Výroční zpráva 2023», *Bezpečnostní informační služba*, [Online], available at: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2023-vz-cj.pdf
15. «Bezpečnostní informační služba. Výroční zpráva 2024», *Bezpečnostní informační služba*, [Online], available at: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2024-vz-cj.pdf
16. «Bezpečnostní rada státu schválila Národní politiku kryptografické ochrany utajovaných informací», *Národní úřad pro kybernetickou a informační bezpečnost*, [Online], available at: https://nukib.gov.cz/cs/infoservis/aktuality/2195-bezpecnostni-rada-statu-schvalila-narodni-politiku-kryptograficke-ochrany-utajovanych-informaci/
17. «Bezpečnostní strategie České republiky 2023», *Ministerstvo obrany České Republiky*, [Online], available at: https://mocr.mo.gov.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_Ceske_republiky_2023.pdf

18. Cabada, L. (2023), «Struggle against Disinformation in the Czech Republic: Treading the Water», *Politics in Central Europe*, Vol. 19, No. 1S, pp. 371–391, doi: 10.2478/pce-2023-0017.
19. «Vláda tají plán proti dezinformacím. ‚Podíleli se na něm odborníci', tvrdí, jejich jména ale nezná», *iROZHLAS*, [Online], available at: https://www.irozhlas.cz/zpravy-domov/dezinformace-plan-vlada-klima-vnitro-chh-cthh_2301191230_cib
20. «Čím se zabýváme», *Bezpečnostní informační služba*, [Online], available at: https://www.bis.cz/cim-se-zabyvame/
21. Danics, Š. and Smolík, J. (2023), «Czech Security Policy in the Context of Hybrid Warfare in Ukraine», *The War in Ukraine and the Policy of the V4 countries*, Marie Curie Skłodowska University Press, Lublin, pp. 123–151.
22. Eberle, J. and Daniel, J. (2023), *Politics of Hybrid Warfare: The Remaking of Security in Czechia after 2014*, Palgrave Macmillan, Cham, 229 p.
23. «Informační koncepce České republiky», *Architektura eGovernmentu ČR*, [Online], available at: https://archi.gov.cz/ikcr
24. Jacuch, A. (2024), Czech-Russian Relations. Russian Disinformation Campaign, *Polish Political Science Yearbook*, Vol. 53 (1), pp. 145–146.
25. «Odolnost a obrana proti hybridnímu působení. Hlavními protivníky jsou i v této doméně Rusko a Čína», Cz.defence, [Online], available at: https://www.czdefence.cz/clanek/odolnost-a-obrana-proti-hybridnimu-pusobeni-hlavnimi-protivniky-jsou-i-v-teto-domene-rusko-a-cina
26. Mareš, M. (2023), «Česká republika v hybridní válce: bilance a perspektivy», *Region v rozvoji společnosti 2023*, sborník příspěvků z 11 mezinárodní vědecké konference, 5–6 května, Brno, pp. 69–74.
27. «Národní strategie kybernetické bezpečnosti ČR na období let 2021-2025», *Národní úřad pro kybernetickou a informační bezpečnost*, [Online], available at: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf
28. «Národní strategie pro čelení hybridnímu působení (2021)», [Online], available at: https://mocr.mo.gov.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf
29. «Pojar bude novým vládním poradcem pro národní bezpečnost», Seznam Zprávy, [Online], available at: https://www.seznamzpravy.cz/clanek/domaci-politika-pojar-novym-vladnim-poradcem-pro-narodni-bezpecnost-221884
30. Smoleňová, I. (2015), *The pro-russian disinformation campaign in the Czech. Republic and Slovakia*, Prague Security Studies Institute, Prague, 18 p.
31. «Státní informační politika – Cesta k informační společnosti», *Vláda České Republiky*, [Online], available at: https://vlada.gov.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089/
32. «Czech Security Information Service: While Russian Intelligence persists with direct and indirect activity, the harms here are minor», Romea, [Online], available at: https://romea.cz/en/czech-republic/czech-security-information-service-while-russian-intelligence-persists-with-direct-and-indirect-activity-the-harms-here-are-minor
33. «Zpráva o činnosti Rady vlády pro informační společnost od 1. ledna do 31. prosince 2023», [Online], available at: https://vlada.gov.cz/assets/ppov/rvis/vyrocni_zpravy/Zprava-o-cinnosti-RVIS-od-1--1--do-31--12--2023.pdf

---

Korniichuk L., Matviichuk N.

Information Policy of the Czech Republic as an Instrument for Ensuring Information Security under the Influence of the russian–Ukrainian War

Abstract. This publication analyses the contemporary information policy of the Czech Republic as a tool for ensuring information security in the context of the russian–Ukrainian war. The aim of this study is to examine the particularities of the implementation of the Czech Republic's information policy amidst the intensification of hybrid influences from the russian federation. The article traces the development of Czech legislation in the field of information security and analyses the activities and roles of the relevant state institutions. It also explores the impact of the russian–Ukrainian war on the transformation of the Czech Republic's information policy. Particular attention is given to assessing the effectiveness of the country's information policy in the context of securing information security.

A range of general and specialised methods have been employed in this study, which collectively facilitate the achievement of the stated aim. The work is primarily based on comparative analysis, content analysis, and modelling. The results demonstrate that since the onset of russia's full–scale invasion of Ukraine, the Czech Republic has significantly enhanced its methods for countering information threats. Considerable emphasis has been placed on the establishment of an appropriate legislative framework, alongside the creation of specialised state institutions tasked with ensuring the country's security in the information domain. Concurrently, substantial educational efforts have been undertaken among the Czech population to foster understanding and skills for processing information in the face of ongoing hybrid influences exerted by influential actors in international relations.

It is demonstrated that the information policy of the Czech Republic constitutes an effective instrument for safeguarding the country's information security despite the substantial pressures arising from the russian–Ukrainian war. Notably, the Czech Republic actively cooperates with NATO and EU partners in this regard, which enables a more effective and strategic response to russia's attempts to influence the national information space.

Keywords: information policy; information security; disinformation; threats; russian–Ukrainian war.

Стаття надійшла до редакції 05.08.2025.