МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ФАКУЛЬТЕТ ПРАВА ТА МІЖНАРОДНИХ ВІДНОСИН

Кафедра міжнародних відносин

Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

Освітня програма 291.00.01 «Суспільні комунікації»

БАКАЛАВРСЬКА РОБОТА

на тему: ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ КРАЇН БАЛТІЇ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ (2022-2026)

Студентки 4 курсу

денної форми навчання

Швець Вероніки Сергіївни

Науковий керівник:

д-р іст. наук, професор

Жалоба Ігор

Володимирович

Київ – 2026

ВСТУП……...

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УМОВАХ ВОЄННОГО КОНФЛІКТУ….

1.1. Стан наукової розробки проблеми та джерельна база дослідження……...

1.2. Понятійно-категоріальний апарат апарат та методи аналізу інформаційної політики країн Балтії…….

1.3. Поняття інформаційної політики в системі міжнародних відносин……...

1.4. Інформаційна безпека як складова національної безпеки……...

1.5.Теорії інформаційних війн та гібридних загроз……

РОЗДІЛ 2. МЕХАНІЗМИ ТА ІНСТРУМЕНТИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ КРАЇН БАЛТІЇ (2022-2026)…….

2.1. Законодавче регулювання та інституційні механізми…….

2.2. Протидія російській дезінформації та пропаганді……

2.3. Стратегічні комунікації та публічна дипломатія……..

РОЗДІЛ 3. ПОРІВНЯЛЬНИЙ АНАЛІЗ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ЕСТОНІЇ, ЛАТВІЇ ТА ЛИТВИ……..

ВИСНОВКИ……..

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….

ДОДАТКИ.....….

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AOTD	Defence Intelligence and Security Service (Служба оборонної розвідки і безпеки Литви)
AVMSD	Audiovisual Media Services Directive (Директива ЄС про аудіовізуальні медіапослуги)
CCDCOE	Cooperative Cyber Defence Centre of Excellence (Центр передового досвіду НАТО у сфері кіберзахисту, Таллін)
CERT-EE	Computer Emergency Response Team of Estonia (Команда реагування на комп'ютерні надзвичайні ситуації Естонії)
DSA	Digital Services Act (Закон ЄС про цифрові послуги)
EAK	Eesti Ajakirjanike Liit (Спілка журналістів Естонії)
EEAS	European External Action Service (Служба зовнішніх дій ЄС)
EIS	Estonian Information System (Естонська інформаційна система)
EMFA	European Media Freedom Act (Регламент ЄС про свободу медіа)
ENISA	European Union Agency for Cybersecurity (Агентство ЄС з кібербезпеки)
ERR	Eesti Rahvusringhääling (Естонське громадське мовлення)
EU	European Union (Європейський Союз)
GCI	Global Cybersecurity Index (Глобальний індекс кібербезпеки)

GDPR	General Data Protection Regulation (Загальний регламент ЄС про захист даних)
IT	Information Technology (Інформаційні технології)
ITU	International Telecommunication Union (Міжнародний союз електрозв'язку)
KAPO	Kaitsepolitseiamet (Департамент поліції безпеки Естонії / Служба внутрішньої безпеки)
LRT	Lietuvos nacionalinis radijas ir televizija (Литовське національне радіо і телебачення)
LRTK	Lietuvos radijo ir televizijos komisija (Комісія з радіо і телебачення Литви)
LSM	Latvijas Sabiedriskie Mediji (Латвійські громадські медіа)
LTV	Latvijas Televīzija (Латвійське телебачення)
LVRTC	Latvijas Valsts radio un televīzijas centrs (Державний центр радіо і телебачення Латвії)
NATO	North Atlantic Treaty Organization (Організація Північноатлантичного договору)
NEPLP	Nacionālā elektronisko plašsaziņas līdzekļu padome (Національна рада з електронних ЗМІ Латвії)
NIS2	Network and Information Security Directive 2 (Директива ЄС про мережеву та інформаційну безпеку, 2022)
SAB	Satversmes aizsardzības birojs (Бюро захисту Конституції Латвії)

SEPLS	Savivaldybių elektros skirstomųjų tinklų plėtros studija (Студія розвитку електромереж самоврядувань Литви)
TTJA	Tarbijakaitse ja Tehnilise Järelevalve Amet (Департамент захисту споживачів і технічного нагляду Естонії)
VSD	Valstybės saugumo departamentas (Департамент державної безпеки Литви)
ЗМІ	Засоби масової інформації

ВСТУП

Актуальність теми дослідження. Повномасштабне збройне вторгнення Російської Федерації в Україну 24 лютого 2022 року докорінно змінило безпековий ландшафт Європи. Одночасно з військовими операціями Росія розгорнула безпрецедентну за масштабом і системністю інформаційну агресію, спрямовану на легітимізацію власних дій, дестабілізацію союзників України та підрив суспільної підтримки міжнародної допомоги Києву. Країни Балтії опинилися в центрі цього протистояння одночасно як безпосередні цілі, як «фронтові держави» НАТО і як найдосвідченіші в Євросоюзі суб'єкти протидії кремлівській дезінформації.

Балтійський досвід є унікальним з кількох причин. По-перше, ці держави накопичували інституційний та правовий досвід протидії російській інформаційній агресії ще від часів відновлення незалежності у 1991 році, фактично виконуючи роль «лабораторії» для розробки методів захисту демократичного інформаційного простору. По-друге, їхня євроатлантична орієнтація та членство в НАТО і ЄС з 2004 року забезпечили інституційну основу для трансформації національних практик. По-третє, специфічна демографічна, мовна та геополітична ситуація кожної з трьох держав зумовила формування відмінних елементів інформаційної безпеки, що у своїй сукупності охоплюють широкий спектр можливих відповідей на гібридні загрози.

Від лютого 2022 року до 2026 року всі три держави здійснили системне оновлення законодавчої бази, інституційної архітектури та стратегічних підходів у сфері інформаційної безпеки трансформацію. Разом із тим інформаційний вимір балтійської безпекової політики продовжує видозмінюватися та покращуватися під час війни і через це залишається недостатньо дослідженим як цілісний феномен, що й зумовлює актуальність цієї роботи.

Об'єктом дослідження є інформаційна політика держав в умовах збройного конфлікту.

Предметом дослідження є механізми, інструменти та стратегії інформаційної політики Естонії, Латвії та Литви у 2022-2026 роках.

Мета дослідження полягає у комплексному аналізі особливості інформаційної політики країн Балтії в умовах російсько-української війни у 2022-2026 роках, виявити спільні та відмінні риси підходів Естонії, Латвії та Литви і визначити їхнє значення для формування загальноєвропейської системи захисту інформаційного простору.

Для досягнення мети поставлено такі **завдання**:

- розглянути стан наукової розробки проблеми та охарактеризувати джерельну базу дослідження;
- визначити понятійно-категоріальний апарат і методи дослідження;
- охарактеризувати поняття інформаційної безпеки як складової національної безпеки та концептуальний апарат теорій інформаційних воєн і гібридних загроз;
- проаналізувати законодавче регулювання та інституційні механізми інформаційної політики Естонії, Латвії та Литви у 2022-2026 рр.;
- дослідити конкретні заходи протидії російській дезінформації та пропаганді у кожній із трьох держав;
- охарактеризувати стратегічні комунікації та публічну дипломатію балтійських країн в умовах воєнного конфлікту;
- здійснити порівняльний аналіз інформаційних стратегій Естонії, Латвії та Литви і визначити їхні спільні елементи та відмінності.

Практичне значення одержаних результатів полягає у тому, що вперше здійснено комплексний порівняльний аналіз інформаційних стратегій Естонії, Латвії та Литви у 2022-2026 роках як єдиного феномену в рамці ЄС та НАТО, виробили відмінні, функціонально взаємодоповнюючі моделі: Естонія технологічного цифрового лідерства; Латвія - жорсткого медіарегулювання; Литва інтегрованої «тотальної оборони». Встановлено, що спільними системоутворюючими елементами є чотирирівнева інституційна архітектура

(державний регулятор - спецслужби - суспільне мовлення - громадянське суспільство) та поєднання обмежувальних і позитивних заходів.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел та додатків.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УМОВАХ ВОЄННОГО КОНФЛІКТУ

1.1. Стан наукової розробки проблеми та джерельна база дослідження

Дослідження особливостей інформаційної політики країн Балтії (Литви, Латвії та Естонії) в умовах сучасної російсько-української війни знаходиться на перетині одразу кількох наукових дисциплін: політології, теорії міжнародних відносин, комунікацій та безпекових студій. Актуалізація гібридних методів ведення війни з боку Російської Федерації після 2014 року, і особливо після повномасштабного вторгнення 2022 року, зумовила значний інтерес наукової спільноти до механізмів інформаційної протидії, які застосовують найбільш вразливі «фронтові» держави НАТО[1].

Огляд наукової літератури. За рівнем висвітлення та проблематикою наукову літературу, що лягла в основу цього дослідження, можна поділити на кілька тематичних груп.

Першу групу становлять праці, присвячені загальнотеоретичним питанням національної безпеки, інформаційної війни та гібридних загроз. Фундаментальні засади національної безпеки в умовах сучасних інформаційних викликів ґрунтовно розкрито у працях українських науковців В. Горбуліна[2], А. Качинського та Г. Почепцова[3]. Теоретичне осмислення феномену гібридних загроз у сучасному міжнародному середовищі знаходить відображення у дослідженнях О. Бусол[4], З. Гбура[5], В. Демченка[6], а також у спільних розвідках А. Геращенка і І. Поліщука[7]. Особливості функціонування інформаційної сфери під

---

[1] Бусол О. Ю. Феномен гібридних загроз національній безпеці. *Юридична Україна*. 2020. № 4. С. 5–11. DOI: https://doi.org/10.37749/2308-9636-2020-4(208)-1.
[2] Горбулін В. П., Качинський А. Б. Засади національної безпеки України : підручник. Київ : Інтертехнологія, 2009. 272 с.
[3] Почепцов Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2015. 496 с.
[4] Бусол О. Ю. Феномен гібридних загроз національній безпеці. *Юридична Україна*. 2020. № 4. С. 5–11. DOI: https://doi.org/10.37749/2308-9636-2020-4(208)-1.
[5] Гбур З. В. Актуальні гібридних загрози економічній безпеці України. *Інвестиції: практика та досвід*. 2018. № 7. С. 100.
[6] Демченко В. С. Інформаційна війна як складова гібридної агресії Російської Федерації. *Вісник Прикарпатського університету. Серія : Політологія*. 2023. Вип. 15. С. 27–32.
[7] Геращенко А. М., Поліщук І. М. Інформаційна безпека в умовах гібридної війни: виклики та стратегії протидії. *Юридичний науковий електронний журнал*. 2023. № 5. С. 343-346.

час глобалізації та війни досліджували В. Пилипчук та О. Дзьобань[8], В. Конах та О. Лазоренко[9].

Друга група - це зарубіжна історіографія концептуальних підходів до гібридної війни. Сучасні трансформації конфліктів досліджено у роботах Ф. Гоффмана[10], С. Бахманна та Х. Гуннеріуссона[11,12], Е. Райхборн-Кьєннеруд та П. Каллена[13], що дозволило адаптувати їхні концепції до балтійських реалій. Значний внесок у розуміння природи інформаційних розладів (дезінформації, місінформації та малінформації) зробили К. Вордл та Х. Деракшан у своєму рамковому звіті для Ради Європи[14].

Третю, більш вузькоспеціалізовану групу становлять праці, що безпосередньо аналізують інформаційну політику, кіберпростір та безпекове середовище країн Балтії. Визначальним у цьому контексті є комплексне дослідження Я. Чакарса та І. Екманіса «Інформаційні війни в країнах Балтії: Довга тінь Росії»[15], яке детально розкриває історичні передумови та сучасні механізми російського впливу на медіапростір Литви, Латвії та Естонії. Вплив російської пропаганди та застосування «м'якої сили» проти держав Балтії ґрунтовно висвітлено у працях І. Бурдулі[16] та А. Петрика («Північний фронт»)[17]. Окремі аспекти правового регулювання та еволюції стратегічних концепцій

---

[8] Пилипчук В., Дзьобань О. Глобальні виклики та загрози національній безпеці в інформаційній сфері. *Вісник Національної академії правових наук України*. 2014. № 3 (78). С. 43–52.
[9] Конах В. К., Лазоренко О. А. Загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації. *Стратегічні пріоритети*. 2014. № 2 (31). С. 73-78.
[10] Hoffman F. Hybrid Warfare and Challenges. *The Routledge Handbook of Civil-Military Relations*. 2012. DOI: 10.4324/9781315814803-35.
[11] Bachmann S. D., Gunneriusson H. Hybrid wars: The 21st-century's new threats to global peace and security. *Scientia Militaria: South African Journal of Military Studies*. 2015. Vol. 43. P. 77–98.
[12] Bachmann S. D., Gunneriusson H. Terrorism and cyberattacks as hybrid threats: Defining a comprehensive approach for countering 21st century threats to global risk and security. *The Journal on Terrorism and Security Analysis*. 2013. Vol. 9. P. 27-36.
[13] Reichborn-Kjennerud E., Cullen P. What is Hybrid Warfare? *Norwegian Institute of International Affairs (NUPI) Policy Brief*. 2016. No. 1. URL: http://hdl.handle.net/11250/2380867 (дата звернення: 01.04.2026).
[14] Wardle C., Derakshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and policy Making / Council of Europe. 2017. URL: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (дата звернення: 01.04.2026).
[15] Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії: Довга тінь Росії / пер. І. Ємельянової. Бостон : Academic Studies Press, 2025. 306 с.
[16] Burduli I. Russian Soft Power in the Baltics: Testing NATO Vulnerabilities. *Per Concordiam*. 2019. Vol. 10, No. 2. P. 19-23.
[17] Петрик А. М. «Північний фронт»: Російська пропаганда проти держав Балтії. Клайпедський університет, 2023. URL: https://www.istpravda.com.ua/articles/2023/10/20/163257/ (дата звернення: 01.04.2026).

безпеки балтійських держав досліджували І. Яковюк і С. Шестопал[18], питання оборонної співпраці країн Балтії - О. Нікерс та О. Табунс[19], а питання політики кібербезпеки та дослідницької кооперації в регіоні ґрунтовно проаналізовані у працях С. Василевської та ін.. Сучасні тенденції зовнішньої та безпекової політики досліджували вітчизняні експерти О. Каракуць[20] та М. Москалюк[21].

Попри значний масив наукової літератури, питання трансформації інформаційної політики країн Балтії саме після 24 лютого 2022 року залишається недостатньо висвітленим у вітчизняному науковому дискурсі. Більшість існуючих праць аналізують ситуацію до початку повномасштабної війни, тоді як нові безпрецедентні заходи (заборона російських телеканалів, блокування веб-ресурсів, посилення кібербезпеки за стандартами європейської директиви NIS2) потребують комплексного узагальнення, що й визначає актуальність цієї роботи.

Огляд джерельної бази дослідження. Для досягнення мети та виконання завдань роботи було залучено широку джерельну базу, яку за типологією можна умовно поділити на чотири основні групи.

Першу групу становлять нормативно-правові акти та концептуальні документи міжнародного рівня, зокрема документи Європейського Союзу. Сюди належить Загальний регламент про захист даних (GDPR)[22], Директива (ЄС) 2022/2555 (NIS2 Directive)[23], що формує єдиний рівень кібербезпеки в ЄС, Директива 95/46/ЄС[24], Резолюція Європейського Парламенту про стратегічні

---

[18] Яковюк І. В., Шестопал С. С. Правове регулювання політики національної безпеки країн Балтії в контексті еволюції стратегічних концепцій НАТО. Проблеми законності. 2018. Вип. 143. С. 218-227. DOI: 10.21564/2414-990x.143.148488.

[19] Nikers O., Tabuns O. Bureaucratic policy and defense cooperation among the Baltic states. Security and Defence Quarterly. 2022. Vol. 37, No. 1. P. 41-54. DOI: https://doi.org/10.35467/sdq/145571.

[20] Каракуць О. Основні тенденції зовнішньої політики і національної безпеки Литви. Київ: НІСД, 2024.

[21] Москалюк М. Ф. Безпекова політика країн Балтії в умовах російсько-української війни. Регіональні студії. 2024. № 37. С. 59-63.

[22] Регламент (ЄС) 2016/679 Європейського Парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних даних (GDPR) від 27.04.2016. URL: https://gdpr-info.eu/ (дата звернення: 01.04.2026).

[23] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022.

[24] Директива 95/46/ЄС Європейського Парламенту та Ради про захист осіб стосовно обробки персональних даних та про вільне переміщення таких даних від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 01.04.2026).

комунікації ЄС для протидії пропаганді третіх сторін (2016 р.)[25], а також Посилений кодекс практики щодо дезінформації (2022)[26] . Ці документи формують загальноєвропейський правовий контур, у межах якого діють країни Балтії.

Другу групу складають акти національного законодавства та стратегічні доктрини держав Балтії. Зокрема, це Кримінальний кодекс[27], Закон про медіапослуги[28] та Закон про правоохоронну діяльність[29] Естонської Республіки; зміни до Закону про електронні засоби масової інформації Латвії[30]. До стратегічних документів належать: Стратегія кібербезпеки Латвії на 2023-2026 роки[31], Національна стратегія кібербезпеки Литви (2022 р.)[32], План розвитку згуртованої Естонії 2021-2030[33], Цифровий порядок денний 2030 Естонії[34] та Національна оборонна стратегія[35]. Вони дають змогу проаналізувати нормативно-правові інструменти, якими держави захищають свій інформаційний суверенітет.

Третя група охоплює офіційні звіти державних структур і безпекових відомств Естонії, Латвії та Литви. Ключове значення для аналізу гібридних

---

[25] Резолюція Європейського Парламенту про стратегічні комунікації ЄС для протидії пропаганді третіх сторін від 23.11.2016 (2016/2030 (INI)). URL: https://www.eeas.europa.eu/node/16198_en (дата звернення: 01.04.2026).
[26] 2022 Strengthened Code of Practice on Disinformation: Policy and Legislation. Publication 16 June 2022. URL: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (дата звернення: 01.04.2026).
[27] Естонія. Кримінальний кодекс: Закон Естонської Республіки від 06 черв. 2001 р. (зі змінами та допов.). URL: https://www.riigiteataja.ee/akt/123052024017 (дата звернення: 15.05.2026).
[28] Естонія. Про медіапослуги (Meediateenuste seadus) : Закон Естонської Республіки від 14 черв. 2022 р. URL: https://www.riigiteataja.ee/en/eli/514062022001/consolide (дата звернення: 01.04.2026).
[29] Естонія. Про правоохоронну діяльність (Korrakaitseseadus) : Закон Естонської Республіки від 23 лют. 2011 р. URL: https://www.riigiteataja.ee/akt/123022011 (дата звернення: 15.05.2026).
[30] Andersone I. New amendments to the Latvian Electronic Mass Media Law enter into force. IRIS. 2022. 2022-9:1/9. URL: https://merlin.obs.coe.int/iris/2022/9/article9.en.html (дата звернення: 01.04.2026).
[31] Latvian Cybersecurity Strategy 2023-2026: Cabinet Regulation No. 158 / Latvian Cabinet of Ministers. 2023. URL: https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf (дата звернення: 01.04.2026).
[32] National Cyber Security Strategy 2022 / Ministry of National Defence of the Republic of Lithuania. 2022. URL: https://kam.lt/en/cyber-security/ (дата звернення: 04.04.2026).
[33] Cohesive Estonia Development Plan 2021-2030 / Ministry of the Interior of the Republic of Estonia. URL: https://www.siseministeerium.ee/sidest (дата звернення: 01.04.2026).
[34] Digital Agenda 2030 / Ministry of Economic Affairs and Communications of the Republic of Estonia. 2021. URL: https://mkm.ee/en/objectives-activities/digital-agenda-2030 (дата звернення: 01.04.2026).
[35] National Defence Strategy Estonia. URL: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf (дата звернення: 01.04.2026).

загроз мають щорічні звіти: Поліції безпеки Естонії (KAPO)[36], Бюро захисту Конституції Латвії (SAB)[37] та Національна оцінка загроз Департаменту державної безпеки Литви (VSD)[38]. Також важливими є звіти інституцій з реагування на кіберінциденти, таких як CERT-LV[39]. Ці матеріали містять первинну фактологічну базу та статистику щодо поточних ворожих операцій в інформаційному просторі.

Четверта група джерел включає аналітичні матеріали, звіти неурядових організацій, експертних центрів та ініціатив з фактчекінгу. Серед них: матеріали балтійської ініціативи Propastop[40], що розвінчує російські наративи; звіти Центру глобалістики «Стратегія XXI»[41]; звіти Міжнародного союзу електрозв'язку (зокрема Глобальний індекс кібербезпеки GCI 2024)[42], звіти Інституту досліджень безпеки ЄС (EUISS)[43,44]та матеріали української ініціативи StopFake, які моніторять російську дезінформацію в європейському контексті[45,46].

Використання зазначеного комплексу наукової літератури та першоджерел (на які зроблено відповідні посилання) забезпечує міцну емпіричну та теоретичну базу для всебічного розкриття теми та виконання завдань бакалаврської роботи.

---

[36] Estonian Internal Security Service (KAPO). Annual Review 2024-2025. Tallinn: KAPO, 2025. URL: https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf (дата звернення: 05.04.2026)
[37] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report 2025. Riga : SAB, 2026. 35 p. URL: https://www.sab.gov.lv (дата звернення: 01.04.2026).
[38] Defence Intelligence and Security Service (AOTD); State Security Department (VSD). National Threat Assessment 2026. Vilnius, 2026. 90 p. URL: https://www.vsd.lt/en/reports/national-threat-assessment-2026/ (дата звернення: 04.04.2026).
[39] CERT-LV. Latvian cybersecurity and CERT.LV technical activities: Annual report 2023. Information Technology Security Incident Response Institution of the Republic of Latvia. 2023.
[40] Propastop. Чи є якась користь від обмеження кремлівських каналів? 27.11.2023. URL: https://www.propastop.org (дата звернення: 01.04.2026).
[41] Гібридні загрози України і суспільна безпека. Досвід ЄС і східного партнерства. Аналітичний документ центру глобалістики «Стратегія XXI». 2018. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf (дата звернення: 01.04.2026).
[42] Global Cybersecurity Index (GCI) 2024 / International Telecommunication Union. 2024. URL: https://www.itu.int/pub/D-HDB-GCI.01-2024 (дата звернення: 01.04.2026).
[43] Andersson J., Tardy T. Hybrid: What's in a name? European Union Institute for Security Studies. 2015. P. 3-4.
[44] Gaub F. Hybrid tactics: ISIL & Co. European Union Institute for Security Studies. Issue Alert 47. Paris, 2015. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_47_hybrid_ISIL.pdf (дата звернення: 01.04.2026).
[45] Churanova O., Romaniuk V. Anti-EU narratives through the Russian-Ukrainian war in the light of StopFake.org's debunks. Disinformation and fact-checking in contemporary society. Madrid : Dykinson, 2023. P. 39-61.
[46] Horbyk R., Dutsyk D., Shalaiskyi S. Effectiveness of Russian disinformation counteraction in Ukraine in a full-scale war: analytical report / Ukrainian Media and Communication Institute NGO. 2023. 66 p.

1.2. Понятійно-категоріальний апарат та методи дослідження

Дослідження проблематики інформаційної політики та безпеки вимагає чіткого визначення ключових дефініцій, що складають понятійно-категоріальний апарат роботи. Базовим концептом виступає поняття «інформаційна політика». У вузькому сенсі її розглядають як діяльність держави щодо регулювання інформаційного простору, проте в контексті дослідження більш доцільним є широке розуміння.

Інформаційна політика - це комплексний, системний напрям державної політики, що охоплює сукупність цілей, принципів, правових та інституційних механізмів, за допомогою яких держава забезпечує інформаційний суверенітет, захищає національний інформаційний простір від зовнішніх деструктивних впливів та формує власний стратегічний наратив на внутрішній і міжнародній аренах. В умовах війни ця політика набуває вираженого оборонного характеру і неминуче втрачає свій суто ліберальний характер і набуває чітко вираженого оборонного, проактивного та безпекового спрямування, стаючи невід'ємним елементом загальної системи національної оборони країни.

Тісно пов'язаним з вищезазначеним є поняття «інформаційна безпека», яке відображає стан і результативність впровадження інформаційної політики держави. Згідно із сучасними безпековими підходами та концепціями, інформаційну безпеку слід розуміти не просто як захист технічних засобів чи каналів зв'язку, а як динамічний стан захищеності життєво важливих інтересів людини, громадянського суспільства і держави в цілому[47]. При такому стані мінімізується або повністю запобігається нанесення моральної, політичної, економічної чи військової шкоди через неповноту, невчасність, викривленість або несправжність поширюваної інформації. Крім того, цей концепт включає захист соціуму від навмисного деструктивного інформаційно-психологічного впливу, маніпуляцій масовою свідомістю, а також від несанкціонованого,

[47] Геращенко А. М., Поліщук І. М. Інформаційна безпека в умовах гібридної війни: виклики та стратегії протидії. *Юридичний науковий електронний журнал*. 2023. № 5. С. 343-346.

ворожого втручання в функціонування критично важливих інформаційних та кібернетичних мереж.

Для всебічного розуміння характеру, логіки та спрямованості дій Російської Федерації проти Естонії, Латвії та Литви ключовим у роботі є концепт «гібридної війни» (hybrid warfare). Цей термін описує складне, багаторівневе та асиметричне протистояння, в якому держава-агресор раціонально інтегрує традиційні кінетичні (суто військові) інструменти з широким спектром некінетичних засобів - економічним тиском, кібератаками, енергетичним шантажем, дипломатичним маневруванням та масштабними інформаційними операціями[48]. Характерною рисою такої війни є те, що агресор намагається уникати прямого, офіційного оголошення класичної війни, діючи в так званій «сірій зоні» з метою створення атмосфери невизначеності, хаосу та стратегічного паралічу системи прийняття рішень у противника. У цій парадигмі інформаційна агресія є не просто допоміжним або обслуговуючим елементом воєнних дій, а стержневою, самостійною і надзвичайно ефективною складовою сучасної гібридної війни[49].

Окремої наукової уваги в рамках дослідження загроз потребують конкретні інструменти реалізації інформаційної агресії, серед яких провідне місце посідає «дезінформація». Спираючись на концептуальні розробки К. Вордл, під дезінформацією ми розуміємо завідомо неправдиву, викривлену або маніпулятивну інформацію, яка навмисно створюється, структурується та поширюється з метою завдання системної шкоди конкретній особі, соціальній групі, організації чи державі в цілому[50]. Вона виступає основним інструментом російського деструктивного впливу в країнах Балтії, спрямованим на розкол суспільства та дискредитацію державних інститутів. Натомість головним

[48] Bachmann S. D., Gunneriusson H. Hybrid wars: The 21st-century's new threats to global peace and security. *Scientia Militaria: South African Journal of Military Studies*. 2015. Vol. 43. P. 77-98.
[49] Бусол О. Ю. Феномен гібридних загроз національній безпеці. *Юридична Україна*. 2020. № 4. С. 5-11. DOI: https://doi.org/10.37749/2308-9636-2020-4(208)-1.
[50] Wardle C., Derakshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and policy Making / Council of Europe. 2017. URL: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (дата звернення: 01.04.2026).

інструментом протидії та оборони в інформаційній політиці виступає «стратегічна комунікація» (Strategic Communications або StratCom). Це системне, скоординоване використання державою та її інститутами всіх наявних комунікативних можливостей (включаючи публічну дипломатію, зв'язки з громадськістю, інформаційні, психологічні та кібероперації) задля формування об'єктивного сприйняття дій держави, просування національних інтересів, зміцнення суспільної стійкості та ефективної нейтралізації ворожих пропагандистських наративів[51].

Успішне вирішення поставлених у бакалаврській роботі завдань та забезпечення об'єктивності її результатів здійснювалося шляхом застосування вивіреної методологічної матриці. Методологічну основу роботи становить чітко визначений комплекс загальнонаукових і спеціальних методів пізнання, які застосовувалися у взаємозв'язку та з урахуванням специфіки об'єкта й предмета дослідження.

Порівняльний (компаративний) метод використовувався як один із ключових інструментів для системного зіставлення підходів трьох балтійських держав, Естонії, Латвії та Литви, до стратегічного регулювання та захисту національного інформаційного простору. Незважаючи на спільність зовнішніх викликів та загроз, кожна з цих держав продемонструвала унікальну внутрішню специфіку (зокрема, через різний відсоток етнічного російськомовного населення, що суттєво відрізняє Естонію та Латвію від більш моноетнічної Литви). Застосування компаративного аналізу до їхніх конкретних законодавчих ініціатив (наприклад, жорсткості підходів до повної заборони ретрансляції російських телеканалів або ліцензування локальних медіа) та інституційних рішень уможливило виявлення як спільних загальнорегіональних тенденцій балтійського солідарного захисту, так і специфічних національних особливостей та відмінностей у темпах адаптації до кризових умов[52].

---

[51] Резолюція Європейського Парламенту про стратегічні комунікації ЄС для протидії пропаганді третіх сторін від 23.11.2016 (2016/2030 (INI)). URL: https://www.eeas.europa.eu/node/16198_en (дата звернення: 01.04.2026).
[52] Nikers O., Tabuns O. Bureaucratic policy and defense cooperation among the Baltic states. *Security and Defence Quarterly*. 2022. Vol. 37, No. 1. P. 41-54. DOI: https://doi.org/10.35467/sdq/145571.

Системно-структурний аналіз застосовувався в роботі для детального розкриття складної інституційної архітектури інформаційної та кібернетичної безпеки країн Балтії. Цей підхід дозволив розглянути інформаційну політику досліджуваних держав не як хаотичний набір розрізнених, реактивних дій на російську загрозу, а як цілісну, структуровану систему. У межах цієї системи взаємопов'язано функціонують правові рамки, спеціалізовані державні органи, сектори цивільно-військового співробітництва, медіарегулятори та інститути громадянського суспільства. Крім того, системно-структурний аналіз допоміг простежити архітектуру інтеграції національних безпекових механізмів країн Балтії у наднаціональні, загальноєвропейські та євроатлантичні структури, такі як кіберпідрозділи НАТО та профільні комісії Європейського Союзу[53].

Контент-аналіз як спеціальний метод дослідження уможливив ретельне, систематизоване та текстове вивчення великого масиву емпіричних матеріалів, що склали основу роботи. Зокрема, за допомогою цього методу було детально проаналізовано офіційні стратегічні документи (національні стратегії безпеки та кіберзахисту країн Балтії), чинні законодавчі акти, що регулюють медіасферу, а також щорічні відкриті доповіді національних спецслужб (KAPO в Естонії, SAB у Латвії, VSD у Литві) та різноманітні аналітичні огляди європейських експертних центрів. Контент-аналіз дозволив об'єктивно виокремити ключові змістовні тренди, зафіксувати еволюцію урядових пріоритетів, а також верифікувати специфіку, структуру та спрямованість деструктивних російських наративів, що розповсюджуються в балтійському регіоні.

Нормативно-правовий метод слугував надійним інструментом для детальної характеристики, класифікації та аналізу законодавчої бази регулювання медіапростору та кібернетичної сфери країн Балтії. У межах цього методу було досліджено процеси імплементації європейського законодавства на національному рівні (зокрема, Директиви NIS2), проаналізовано юридичну силу

[53] Яковюк І. В., Шестопал С. С. Правове регулювання політики національної безпеки країн Балтії в контексті еволюції стратегічних концепцій НАТО. Проблеми законності. 2018. Вип. 143. С. 218-227. DOI: 10.21564/2414-990x.143.148488.

та ефективність нових законів про обмеження ворожого контенту, посилення відповідальності за поширення мови ворожнечі та захисту критичної інформаційної інфраструктури. Це дозволило оцінити правову спроможність держав Балтії протидіяти загрозам у межах правового поля та принципів демократичного врядування.

Геополітичний підхід дозволив у процесі дослідження повноцінно ураховувати специфічне та надзвичайно вразливе стратегічне положення балтійських держав у сучасному міжнародному контексті. Завдяки цьому підходу інформаційна політика Естонії, Латвії та Литви розглядається не ізольовано, а крізь призму глобального та регіонального протистояння між Російською Федерацією та блоком НАТО й Європейським Союзом. Геополітична оптика допомогла обґрунтувати статус країн Балтії як «фронтових» держав, які першими приймають на себе удари гібридної агресії, та показати, як їхнє географічне розташування та історичний досвід безпосередньо зумовлюють високу радикалізацію, безкомпромісність та проактивність їхньої сучасної інформаційної політики.

Таким чином, поєднання зазначеного понятійно-категоріального апарату та вивіреного, цілісного методологічного інструментарію дозволило провести всебічне дослідження особливостей інформаційної політики країн Балтії в сучасних умовах інтенсивного гібридного протистояння, забезпечуючи високу вірогідність та академічну цінність отриманих висновків.

1.3. Поняття інформаційної політики в системі міжнародних відносин

Інформаційна політика держави є комплексним явищем, що охоплює сукупність принципів, механізмів і інструментів, за допомогою яких держава регулює виробництво, поширення та споживання інформації як усередині країни, так і на міжнародній арені. В умовах стрімкої цифровізації суспільства та глобалізації комунікаційних процесів інформаційна політика набула значення повноцінного інструменту зовнішньої політики, здатного суттєво впливати на

міжнародні відносини та баланс сил на світовій арені[54]. Традиційні уявлення про символи влади та способи досягнення світового панування змінюються: раніше йшлося про суходільний, повітряний та морський простір, а тепер говориться про оновлення ролі інформаційного простору як нового поля геополітичного протистояння інформаційної сфери[55].

Як зазначають дослідники, в сучасних геополітичних умовах зростає важливість інформаційного чинника, спостерігається чітка тенденція до підвищення ролі інформаційних ресурсів держав у загальній системі оборонних можливостей, а геополітичні умови визначають військово-інформаційну політику держави в найважливіших сферах геополітичного суперництва та протистояння[56]. Головним полем протистояння є інформаційний простір глобального, регіонального та національного рівнів. Відповідно до довгострокових прогнозів, перспективи глобального розвитку визначатимуть глобальне перегрупування сил внаслідок прогресу в інформаційній сфері в США, ЄС, Японії, Китаї, Індії та Росії, і остання намагається стати аналогічним центром інформаційного впливу в сучасних умовах[57].

У системі міжнародних відносин інформаційна політика виконує кілька взаємопов'язаних функцій. По-перше, вона слугує засобом формування міжнародного іміджу держави та просування її інтересів у глобальному інформаційному просторі. По-друге, вона є інструментом захисту національного інформаційного суверенітету від зовнішнього втручання. По-третє, в руках агресивних держав вона перетворюється на зброю впливу на внутрішню та зовнішню політику інших країн[58]. Саме в цьому останньому вимірі інформаційна політика Російської Федерації привертає особливу увагу дослідників, оскільки Росія систематично застосовує інформаційні ресурси для досягнення своїх

[54] Burduli I. Russian Soft Power in the Baltics: Testing NATO Vulnerabilities. *Per Concordiam.* 2019. Vol. 10. No. 2. P. 19–23.
[55] Пилипчук В., Дзьобань О. Глобальні виклики та загрози національній безпеці в інформаційній сфері. *Вісник Національної академії правових наук України.* 2014. № 3 (78). С. 43-52.
[56] Так само. С. 43-52.
[57] Так само. С. 43-52.
[58] Демченко В. С. Інформаційна війна як складова гібридної агресії Російської Федерації…

стратегічних цілей, підриваючи стабільність і демократичні інститути сусідніх держав[59].

Концепція м'якої сили, розроблена американським політологом Джозефом Наєм, тривалий час залишалась домінуючою парадигмою для розуміння невійськових інструментів зовнішньої політики. Однак застосування цієї концепції до Росії потребує суттєвих застережень: на відміну від класичного розуміння м'якої сили як привабливості власних цінностей і способу життя, російська версія цього інструменту ґрунтується не на привабленні, а на дестабілізації, маніпуляції та дискредитації опонентів[60]. Це принципово відрізняє її від підходів демократичних держав і визначає руйнівний характер російської інформаційної присутності в міжнародному просторі. Зокрема, в країнах Балтії інформаційна агресія Росії проявляється через систематичне поширення наративів про слабкість балтійських держав, фальсифікацію історії та дискримінацію російськомовного населення, що реалізується переважно через платформи Telegram, TikTok та Facebook[61].

Стратегія дезінформації Росії є гнучкою та динамічною системою, яка безперервно еволюціонує у відповідь на зміни в інформаційному середовищі: від відвертих фейкових новин і тролінг-ферм до складних багаторівневих операцій, що поєднують маніпулювання фактами, технології штучного інтелекту та цілеспрямований вплив через міжнародні медіа[62]. Особливо важливим для розуміння сучасних форм інформаційної агресії є концепція «напівправди» - поширення дезінформації на основі реальних подій, що принципово ускладнює її спростування та підвищує довіру до такого контенту[63].

---

[59] Геращенко А. М., Поліщук І. М. Інформаційна безпека в умовах гібридної війни…
[60] Burduli I. Russian Soft Power in the Baltics: Testing NATO Vulnerabilities. *Per Concordiam*. 2019. Vol. 10, No. 2. P. 19-23.
[61] Так само. P. 19-23.
[62] Horbyk R., Dutsyk D., Shalaiskyi S. Effectiveness of Russian disinformation counteraction in Ukraine in a full-scale war: analytical report / Ukrainian Media and Communication Institute NGO. 2023. 66 p.
[63] Churanova O., Romaniuk V. *Anti-EU narratives through the Russian-Ukrainian war in the light of StopFake.org's debunks*. Madrid: Dykinson, 2023. P. 39-61.

Регуляторна відповідь на ці загрози формується на кількох рівнях. На рівні ЄС нові правила GDPR посилюють захист персональних даних[64], а Резолюція Європейського Парламенту від 23 листопада 2016 року про стратегічні комунікації ЄС для протидії пропаганді (2016/2030 (IHI)) закладає інституційні засади протидії дезінформації[65]. На рівні спеціалізованих структур діють Центр передового досвіду зі стратегічних комунікацій НАТО (StratCom COE, Рига), ресурс EUvsDisinfo та механізми Закону про цифрові послуги (DSA), що забезпечують моніторинг і спростування дезінформаційних кампаній[66]. Аналіз конкретних кейсів засвідчує транснаціональний характер російської інформаційної агресії: вона застосовувалась для легітимізації військового втручання в Грузії (2008), маніпулювання громадською думкою в молдовсько-придністровському конфлікті, дестабілізації країн Балтії, просування інтересів у сирійському конфлікті та втручання у виборчі процеси в США[67]. Це наочно демонструє, що інформаційна агресія Росії є системним інструментом зовнішньої політики, що застосовується глобально.

1.4. Інформаційна безпека як складова національної безпеки

У сучасному світі військова сила вже не є достатньою умовою для гарантування безпеки держави. Національна безпека нині тісно пов'язана з людським капіталом, а сила чи слабкість останнього визначається станом системи освіти та науки держави. Інформаційна безпека є невід'ємним компонентом системи національної безпеки сучасної держави. Вона охоплює захист інформаційних ресурсів і систем від зовнішніх загроз, протидію дезінформації та маніпулятивним впливам, а також забезпечення умов для вільного й достовірного інформаційного обміну в суспільстві[68]. В умовах

---

[64] Регламент (ЄС) 2016/679 Європейського Парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних даних (GDPR) від 27.04.2016. URL: https://gdpr-info.eu/ (дата звернення: 01.04.2026).
[65] Регламент (ЄС) 2016/679 Європейського Парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних даних (GDPR). 2016. URL: https://gdpr-info.eu/
[66] Burduli I. Russian Soft Power in the Baltics: Testing NATO Vulnerabilities. *Per Concordiam.* 2019. Vol. 10. No. 2. P. 19–23.
[67] Демченко В. С. Інформаційна війна як складова гібридної агресії Російської Федерації…
[68] Так само.

наростання гібридних загроз межа між інформаційною безпекою та іншими складовими національної безпеки стає дедалі умовнішою: інформаційні операції безпосередньо впливають на обороноздатність держави, стабільність її політичних інститутів і соціальну згуртованість суспільства.

Дослідники виокремлюють п'ять основних загроз, що мають високий потенціал актуалізації: загроза для економічного зростання і конкурентоспроможності; загроза для військової безпеки; загроза для інформаційної безпеки; загроза для глобальних інтересів держави; загроза для єдності і згуртованості нації[69].

Інформаційна безпека охоплює щонайменше три взаємопов'язані виміри. Технічний вимір стосується захисту інформаційних систем і критичної інфраструктури від кібератак і несанкціонованого доступу. Когнітивний вимір охоплює захист суспільної свідомості від маніпуляцій, дезінформації та пропаганди. Інституційний вимір передбачає наявність правових механізмів і державних структур, здатних ефективно реагувати на інформаційні загрози[70]. В системі забезпечення національної безпеки держави американські військові дослідники Джаггер Річард та Джордж Барбер виділяють тріаду: національні цінності в інформаційній сфері; національні інтереси в інформаційній сфері; національні цілі в інформаційній сфері[71].

Розуміння та ефективна протидія інформаційній війні є важливими завданнями для країн, що стикаються з російською агресією, з метою збереження безпеки, стабільності та демократичних цінностей[72]. Це особливо актуально для країн Балтії, які перебувають під систематичним інформаційним тиском з боку Москви. Балтійські держави стикаються з впливом російської агресії в політичному секторі, інформаційній сфері та через військові провокації, а у 2025

---

[69] Гібридні загрози України і суспільна безпека. Досвід ЄС і східного партнерства. Аналітичний документ центру глобалістики «Стратегія XXI». 2018. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf (дата звернення: 01.04.2026).

[70] Wardle C., Derakshan H. Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe, 2017. URL: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[71] Пилипчук В., Дзьобань О. Глобальні виклики…

[72] Геращенко А. М., Поліщук І. М. Інформаційна безпека…

році повністю відключилися від енергомереж Росії та приєдналися до об'єднаної системи Європи, що зменшує потенційний ризик впливу на свій енергетичний сектор; інформаційна війна використовується для створення напруженості та дезорієнтації в цих країнах[73].

Особливої уваги заслуговує інформаційна грамотність населення як ключовий компонент інформаційної безпеки. Вона означає здатність людей критично оцінювати, аналізувати та розуміти інформацію, яку вони споживають. До основних критеріїв інформаційної грамотності належать: здатність до критичного аналізу, що передбачає вміння розрізняти факти від дезінформації та оцінювати достовірність джерел; навички фактчекінгу, активна перевірка інформації перед її довірою чи поширенням; застосування критеріїв оцінки інформації за параметрами авторитетності, доказової бази, об'єктивності та контексту[74]. Без належного рівня інформаційної грамотності населення будь-які технічні чи правові заходи захисту є недостатніми, оскільки вразливість кожного окремого громадянина стає вразливістю всього суспільства.

Головною небезпекою гібридної війни РФ є використання громадськості у процесі досягнення потрібних агресору цілей через інформаційну пропаганду. Так відбувається вплив на свідомість, який породжує та утримує недовіру до державних органів, залякує людей, породжує невпевненість, змушує їх покидати державу[75].

Щодо стратегічних орієнтирів забезпечення інформаційної безпеки, документ НАТО СМ (2002) 49 проголошує п'ять ключових принципі безпекової політики: «принцип широти», «принцип глибини», «принцип централізації», «принцип контролю доступу» та «принцип персонального контролю»[76]. Найважливішим аспектом інформаційної безпеки всіх країн ЄС є захист

---

[73] Демченко В. С. Інформаційна війна…
[74] Так само.
[75] Гібридні загрози України і суспільна безпека. Досвід ЄС…Аналітичний документ центру глобалістики «Стратегія XXI»…
[76] Roberts Al. S. Entangling Alliances: Nato's security of information policy and the entrenchment of State Secrecy. *Cornell International Law Journal*. 2002. Vol. 26 (2). URL: https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1536&context=cilj (дата звернення: 01.04.2026).

персональних даних, принципи якого визначено Директивою 95/46/ЄС[77]. Новий Регламент GDPR посилює зберігання персональних даних та встановлює більш суворе покарання за несвоєчасне повідомлення про витік даних. Досвід Австрії, Швейцарії, Фінляндії та Ірландії у сфері захисту даних, раннього виявлення кіберзагроз та посилення критичної інфраструктури є корисним орієнтиром для формування національної моделі інформаційної безпеки[78].

З метою посилення захищеності держави від гібридних загроз серед першочергових заходів дослідники визначають: розробку та прийняття нової оперативної національної Концепції протидії гібридній війні; вдосконалення Доктрини інформаційної безпеки з конкретизацією заходів для проведення інформаційної політики та кібербезпеки; збільшення ефективності використання інструментів публічної дипломатії; посилення кіберзахисту державних об'єктів; а також, разом з партнерами по НАТО, напрацювання інструментарію щодо об'єднання зусиль для протидії загрозам військового, політичного та економічного характеру, які виникають з боку РФ.

1.5. Теорії інформаційних війн та гібридних загроз

Теоретичне осмислення феномену інформаційних воєн є відносно молодою, але надзвичайно динамічно розвиненою галуззю наукового знання. Проблемам гібридної війни та гібридним загрозам присвячені наукові праці таких вчених як Гбур З. В., Грищук Р. В., Магда Є. М., Мартинюк В., Gaub F., Niruthan N., Bachmann S. D., Gunneriusson H., Andersson J., Tardy T., Miklaucic M. та інших[79]. У закордонній політичній науці такі дослідники, як Рід Т. («Кібервійна не відбудеться»), Джайлс К. та Гофман Ф. Г. («Гібридна війна та

[77] Директива 95/46/ЄС Європейського Парламенту та Ради про захист осіб стосовно обробки персональних даних та про вільне переміщення таких даних. 1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text
[78] Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Brussels: European Parliament, 2014. 86 p.
URL:https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf (дата звернення: 01.04.2026).
[79] Гібридні загрози України і суспільна безпека. Досвід ЄС…Аналітичний документ центру глобалістики «Стратегія XXI»…

виклики»), розглядають гібридну війну, включно з її інформаційною складовою, як сучасну стратегічну загрозу та виклик для національної безпеки[80].

Для розуміння основних концептів гібридних загроз слід виокремити ключові дефініції. Безпека - це стан збереження та захищеності сталого існування, розвитку об'єкта (системи), за яким ймовірність змін, спричинених зовнішніми чи внутрішніми впливами, є мінімальною. Загроза - це стан переважання ймовірності неминучості виникнення надзвичайної ситуації над ймовірністю її уникнення. Гібридна загроза - це будь-який противник, який одночасно та адаптовано використовує співвідношення звичайного озброєння, нерегулярну тактику, тероризм та злочинну поведінку в зоні бойових дій для досягнення своїх політичних цілей[81]. Концепція гібридної війни, як визначають деякі зарубіжні науковці, бере свій початок з часу Другої Ліванської війни між Хезболлою та Ізраїлем у 2006 році[82]. Однак інші вчені визначили, що теорія «гібридної війни» започаткована наприкінці 1990-х - початку 2000-х рр. американськими військовими експертами[83].

Сучасний термін «гібридна війна» розглядається з трьох боків. По-перше, гібридність може відноситися до військової ситуації та умов. По-друге, до стратегії та тактики противника. По-третє, до видів сил, які повинна створювати та підтримувати держава з метою захисту її громадян[84]. Нині очевидно, що характер воєн у світі суттєво змінився. Традиційні межі між військовими та цивільними особами стираються: хакер, пропагандист чи контрабандист зброї можуть бути такими самими учасниками військових дій, якими є солдати[85]. Як стверджують Райхборн-К'єннеруд та Каллен, «головний простір боїв відбувається всередині когнітивних просторів ключових груп населення та ключових політиків, які приймають рішення»[86].

---

[80] Frank Hoffman, Hybrid Warfare and Challenges…
[81] Гібридні загрози України і суспільна безпека…
[82] Бусол О. Ю. Феномен гібридних загроз національній безпеці. *Юридична Україна*. 2020. № 4. С. 5–11.
[83] Так само.
[84] Bachmann S. D., Gunneriusson H. Hybrid wars…
[85] Niruthan N. How Hybrid Warfare Could Change Asia…
[86] Reichborn-Kjennerud E., Cullen P. What is Hybrid Warfare? Policy Brief…

Інформаційна війна визначається як систематичне використання інформаційних ресурсів із метою впливу на громадську думку, створення сприятливих умов для досягнення власних політичних чи військових цілей. Вона є важливою складовою гібридної війни, яка поєднує різні форми агресії та застосовується для досягнення одночасно політичних, економічних і військових цілей[87]. Ключова роль інформаційної війни в гібридних конфліктах полягає в тому, що вона допомагає створити незбалансовану інформаційну картину, підриває стабільність і довіру в суспільстві та може вирішально вплинути на результати конфлікту[88].

Дослідники виділяють п'ять основних цілей, які переслідуються в інформаційній війні[89]. По-перше, маніпуляція громадською думкою через поширення фейкових новин, дезінформацію та пропаганду з метою зміни переконань і поведінки суспільства. По-друге, створення хаосу та дезорієнтації шляхом спотворення фактів і генерування конфліктів, що підривають суспільну стабільність і довіру до влади. По-третє, зниження морально-психологічного стану противника через психологічний тиск і поширення загроз[90]. По-четверте, вплив на політичну ситуацію через дискредитацію лідерів і формування сприятливого для агресора політичного середовища. По-п'яте, загроза кібербезпеці через злам інформаційних систем і викрадення конфіденційних даних[91].

До основних рис інформаційної війни в контексті російської агресії відносимо такі елементи. По-перше, психологічна операція: інформаційна війна передбачає психологічні операції, спрямовані на вплив на свідомість та емоції людей - психологічний тиск, створення страху, злочини з метою дискредитації опонентів і збільшення підтримки власної агресії. По-друге, пропаганда та дезінформація: використання спотвореної або фальшивої інформації, поширення

[87] Демченко В. С. Інформаційна війна як складова…
[88] Так само.
[89] Так само.
[90] Геращенко А. М., Поліщук І. М. Інформаційна безпека в умовах гібридної війни…
[91] Демченко В. С. Інформаційна війна як складова…

фейкових новин. По-третє, використання соціальних медіа та інтернету: створення фейкових акаунтів, ботів і спеціальних коментаторів, які підтримують агресію та спотворюють дійсність. По-четверте, кібератаки та хакерські атаки, спрямовані на злам інформаційних систем, розповсюдження вірусів та крадіжку конфіденційної інформації, що дає змогу перешкоджати роботі урядових структур і впливати на критичну інфраструктуру[92].

Природа гібридних воєн, як визначено ще К. фон Клаузевіцем, складається з трьох складових - емоції, випадковості та розуму. Ці незалежні змінні та новітні сучасні технології мають великий вплив на характер війни: вони впливають на тактику, оперативне мистецтво, військову стратегію[93]. Кібератаки є найбільш очевидним прикладом. Збір та оцінка інформації, що було вирішальним у всіх війнах, нині набуває ще більшого значення. Серед основних методів інформаційної війни виокремлюють: пропаганду, дезінформацію, кібератаки, використання соціальних мереж і медіа, застосування штучного інтелекту та автоматизації, викрадення та злам інформаційних систем[94].

Аналіз конкретних кейсів застосування російської інформаційної агресії засвідчує її транснаціональний характер. Росія використовувала інформаційну війну для легітимізації військового втручання в Грузії, маніпулювання громадською думкою в молдовсько-придністровському конфлікті, дестабілізації країн Балтії, просування своїх інтересів у сирійському конфлікті та втручання у виборчі процеси в США. Починаючи з 2022 року, з моменту початку повномасштабного російського вторгнення на територію України, Росія веде військові дії, порушуючи суверенітет і територіальну цілісність України, тим самим започатковуючи фазу відкритої, зокрема інформаційної, війни[95]. Цей перелік наочно демонструє, що інформаційна агресія Росії є системним інструментом зовнішньої політики, що застосовується глобально, а не ситуативною реакцією на конкретні події.

---

[92] Так само.
[93] Клаузевіц К. Про війну / пер. з англ. Дж. Дж. Грехем…
[94] Демченко В. С. Інформаційна війна як складова…
[95] Так само. 27-32.

Стратегія дезінформації Росії є гнучкою системою, яка еволюціонує у відповідь на зміни в інформаційному середовищі: від фейкових новин і тролінг-ферм до складних багаторівневих операцій, що поєднують маніпулювання фактами, технології штучного інтелекту та цілеспрямований вплив через міжнародні медіа[96]. Використовуючи як традиційні ЗМІ, так і цифрові платформи, вона адаптується до змін у споживанні медіа та суспільній думці, що дозволяє формувати сприятливі інтерпретації подій та впливати на процеси прийняття політичних рішень[97]. Такі заходи, як кіберзахист, підвищення інформаційної грамотності та співпраця міжнародних партнерів - ключові інструменти протидії цій загрозі.

Таким чином, проведений аналіз концептуальних підходів до вивчення інформаційної політики держави дозволяє зробити такі висновки. По-перше, інформаційна політика держави є багатофункціональним інструментом, що виконує одночасно захисну, комунікаційну та проективну функції в системі міжнародних відносин. В умовах цифровізації вона перетворилась на повноцінний інструмент зовнішньої політики, здатного суттєво впливати на міжнародний порядок денний[98]. Ефективна реалізація цих функцій вимагає комплексного використання інформаційних технологій, де кожен канал комунікації, від мережі Інтернет до прямих дипломатичних контактів, виконує власну незамінну роль[99].

По-друге, інформаційна безпека є невід'ємною складовою національної безпеки, що охоплює технічний, когнітивний та інституційний виміри. Особливої значущості набуває інформаційна грамотність населення як фундаментальний елемент стійкості суспільства до маніпулятивних впливів. По-третє, гібридна війна є якісно новим видом конфлікту, в якому інформаційна складова відіграє стратегічну роль. Її головним полем є когнітивний простір суспільства та осіб, що приймають рішення. Російська інформаційна агресія є

[96] Horbyk R., Dutsyk D., Shalaiskyi S. Effectiveness of Russian disinformation…
[97] Churanova O., Romaniuk V. Anti-EU narratives through the Russian-Ukrainian…
[98] Burduli I. Russian Soft Power in the Baltics…
[99] Король А. Інформаційні технології в системі… С. 60–66.

системним глобальним явищем, а не ситуативною реакцією, і потребує комплексної міжнародної відповіді через координацію зусиль держав, інститутів ЄС та НАТО[100].

[100] Bachmann S. D., Gunneriusson H. Terrorism and cyber attacks as hybrid threats…

РОЗДІЛ 2. МЕХАНІЗМИ ТА ІНСТРУМЕНТИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ КРАЇН БАЛТІЇ (2022–2025)

2.1. Законодавче регулювання та інституційні механізми

Інформаційна політика країн Балтії у 2022-2025 рр. зазнала безпрецедентної трансформації, зумовленої повномасштабним вторгненням Росії в Україну. Якщо до лютого 2022 р. регуляторні заходи в інформаційній сфері носили переважно точковий характер, то в наступний період усі три держави - Естонія, Латвія та Литва здійснили системне оновлення законодавчої бази та інституційної архітектури протидії дезінформації. Разом із тим законодавче регулювання балтійського інформаційного простору не є явищем виключно сучасності. Воно має глибоке коріння, що сягає реформ безпекової сфери після вступу до НАТО та ЄС у 2004 р. і розгорталося паралельно до трансформацій загальної системи колективної безпеки Альянсу.

Це підкреслюють І. Яковюк та С. Шестопал, які здійснили комплексний аналіз правового регулювання політики національної безпеки країн Балтії в контексті еволюції стратегічних концепцій НАТО: «зі вступом до НАТО проблема забезпечення безпеки країн Балтії почала розглядатися в контексті проблеми забезпечення міжнародної безпеки, що обумовило потребу спочатку у формуванні, а згодом перегляді нормативно-правових актів у відповідних сферах»[101]. Спільним вектором сучасних перетворень стало поєднання жорсткого обмеження контенту з проактивним формуванням якісного медіапростору та підвищенням суспільної стійкості через медіаграмотність. Паралельно відбувалася глибока імплементація загальноєвропейських інструментів: Закону про цифрові послуги (DSA), Директиви про аудіовізуальні медіапослуги (AVMSD) та Директиви NIS2. І це надало балтійським заходам додаткову правову легітимність та міжнародний вимір.

[101] Яковюк І. В., Шестопал С. С. Правове регулювання політики національної безпеки країн Балтії в контексті еволюції стратегічних концепцій НАТО. *Проблеми законності*. 2018. Вип. 143. С. 218–227. DOI: 10.21564/2414-990x.143.148488.

Правове регулювання інформаційного простору в країнах Балтії будується на двох взаємопов'язаних рівнях: загальноєвропейському, що задає обов'язкові стандарти для всіх держав-членів ЄС, та національному, де кожна з трьох держав виробила власні акценти відповідно до специфіки загроз. Базовими загальноєвропейськими інструментами є Директива про аудіовізуальні медіапослуги (AVMSD, 2018/1808), Закон про цифрові послуги (DSA, 2022), Загальний регламент захисту даних (GDPR, 2016/679), Зміцнений кодекс практики щодо дезінформації (2022) та Директива NIS2 (2022/2555). Їхня спільна основна ідея полягає у зобов'язанні цифрових платформ та медіасервісів активно виявляти і обмежувати системні ризики, пов'язані з дезінформацією, забезпечуючи при цьому прозорість того, хто є власником та фінансування.

Важливим новим інструментом є Європейська декларація цифрових прав та принципів, яку країни Балтії активно імплементують, оскільки вона забезпечує захист персональних даних, свободу слова та безпеку в мережі, окреслюючи нові стандарти для цифрового інформаційного простору в умовах нарощування гібридних загроз. 13 лютого 2025 р. Комісія ЄС та Рада у сфері цифрових послуг схвалили інтеграцію Кодексу практики щодо дезінформації 2022 р. як Кодексу поведінки щодо дезінформації в рамки Закону про цифрові послуги (DSA)[102]. Це рішення посилило обов'язкову силу кодексу і розширило перелік платформ, зобов'язаних дотримуватися його стандартів: дематеріалізацію фінансування дезінформації, прозорість політичної реклами, розширення співпраці з фактчекерами та спрощення доступу дослідників до даних.

Естонія не має єдиного кодифікованого законодавства, що спеціально регулювало б дезінформацію: особи, які її поширюють, підпадають під загальні норми. Зокрема, поєднання § 262 Кримінального кодексу[103] та § 55 Закону про

[102] Nikers O., Tabuns O. Bureaucratic policy and defense cooperation among the Baltic states. *Security and Defence Quarterly*. 2022. Vol. 37, No. 1. P. 41–54. DOI: https://doi.org/10.35467/sdq/145571.
[103] Естонія. Кримінальний кодекс: Закон Естонської Республіки від 06 черв. 2001 р. (зі змінами та допов.). URL: https://www.riigiteataja.ee/akt/123052024017 (дата звернення: 15.05.2026).

правоохоронну діяльність[104] передбачає, що розповсюдження свідомо неправдивої інформації може каратися штрафом або арештом, якщо доведено зловмисний характер і шкоду для суспільного порядку. Ключовим актом стало оновлення Закону про медіапослуги 9 березня 2022 р. (зміни, що транспонують Директиву AVMSD), яким додано окрему главу про сприяння медіаграмотності. Відповідно до § 532, медіаграмотність означає «навички, знання та розуміння, що уможливлюють ефективне та безпечне використання медіа»[105].

Наступним кроком стало прийняття у 2025 р. закону, що забороняє ретрансляцію російських пропагандистських каналів, та підготовлений урядом законопроект про внесення змін до Закону про медіапослуги, мета якого - привести естонське правове середовище у відповідність до Регламенту ЄС про свободу медіа (EMFA, набув чинності 8 серпня 2025 р.): посилення медіаплюралізму, прозорість медіавласності та державної реклами, захист джерел журналістів і членів їхніх сімей[106].

Практичні наслідки законодавчих змін виявились вимірними. Завдяки санкціям ЄС та ініціативі Агентства захисту прав споживачів (TTJA) в Естонії було заблоковано доступ до 389 телеканалів, вебсайтів та акаунтів у соціальних мережах, пов'язаних із Кремлем[107]. Реакцією Росії стало закриття офісу «Спутніка» в Естонії, що відбулося через санкції не через пряму заборону контенту, а через фінансові обмеження. Реєстраційні дані домену sputnik-news.ee (зареєстрований на «Россія сєгодня», реєстратор Ascio Technologies Inc.) фіксують статус «Реєстрація замінника заборонена», що показує механізм блокування:

---

[104] Естонія. Про правоохоронну діяльність (Korrakaitseseadus): Закон Естонської Республіки від 23 лют. 2011 р. URL: https://www.riigiteataja.ee/akt/123022011 (дата звернення: 15.05.2026).
[105] Естонія. Про медіапослуги (Meediateenuste seadus): Закон Естонської Республіки від 14 черв. 2022 р. URL: https://www.riigiteataja.ee/en/eli/514062022001/consolide (дата звернення: 01.04.2026).
[106] The Media Services Bill will reach the Riigikogu/Estonian Ministry of Culture. 06.02.2026. URL: https://ifacca.org/news/2026/02/06/media-services-bill-will-reach-riigikogu/ (дата звернення: 01.04.2026).
[107] Propastop. Чи є якась користь від обмеження кремлівських каналів? 27.11.2023. URL: https://www.propastop.org (дата звернення: 01.04.2026).

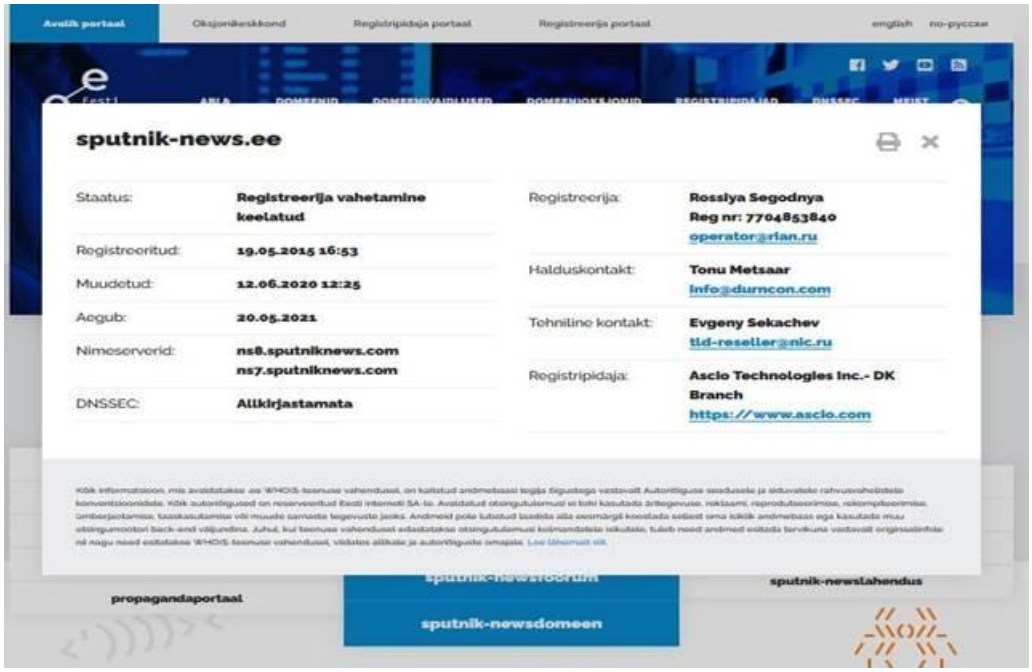


Рис. 2.1 Реєстраційні дані домену sputnik-news.ee - заблокована реєстрація замінника (Estonian Internet Foundation, 2020–2021 рр.). Джерело: Estonian Internet Foundation (EIS), est.ee, публічний реєстр доменів .ee[108].

Дослідження ефективності обмежень показує суперечливі результати. З одного боку, щорічне опитування Міністерства оборони Естонії засвідчило, що від запровадження обмежень кількість неестонців, які регулярно переглядають російські телеканали, скоротилася майже вдвічі - з 62% навесні 2021 р. до 33% навесні 2022 р. та 24% навесні 2023 р.; аудиторія російських новинних порталів відповідно знизилась із 51% до 32%[109]. З іншого боку, самі дослідники застерігають, що «вплив обмежень потребує кращого вимірювання», адже зміни аудиторії можуть зумовлюватися й іншими факторами — зокрема, природним зниженням телеперегляду ще до запровадження обмежень:

[108] Так само.
[109] Так само.

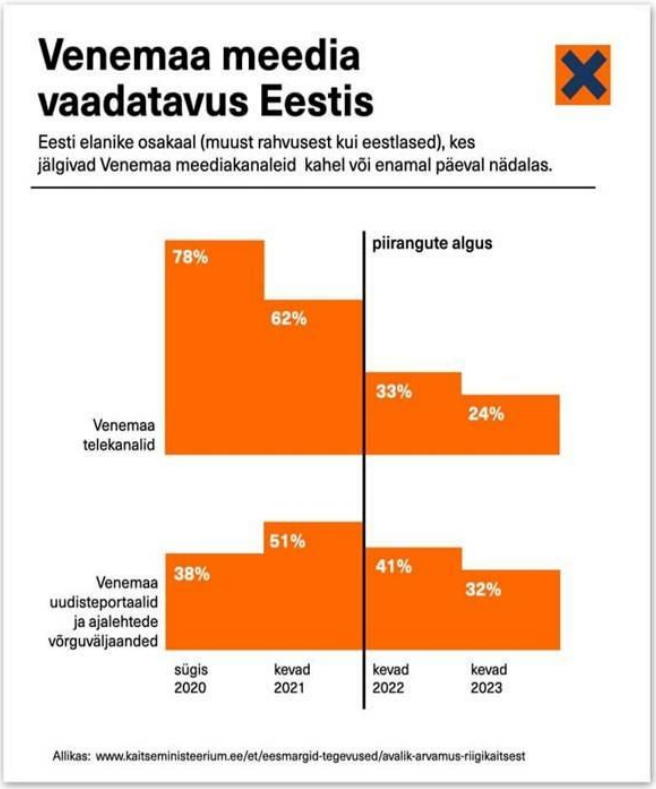


Рис. 2.2 Динаміка перегляду російських медіаканалів в Естонії (2020–2023 рр.) серед нееестонського населення. Вертикальна лінія позначає момент запровадження обмежень (весна 2022 р.). Джерело: Міністерство оборони Естонії (Kaitseministeerium), щорічне опитування громадської думки. URL: www.kaitseministeerium.ee/et/eesmargid-tegevused/avalik-arvamus-riigikaitsest[110].

Не менш важливим є застереження «Propastop»: навіть за зниження аудиторії «кількість людей в Естонії, які поділяють цінності та погляди інформаційного простору Кремля, все ще велика» - на що вказує дослідження Фонду Фрідріха Еберта (вересень 2023 р.)[111]. Цей висновок підкреслює принципову обмеженість суто обмежувальних заходів і необхідність їх поєднання з позитивними стратегіями: медіаграмотністю, альтернативним якісним контентом та інтеграційними програмами.

Латвія застосовує найбільш радикальні заходи медіарегулювання серед трьох балтійських держав. Ключовими законодавчими актами стали суттєві зміни до Закону про електронні медіа, що набули чинності 24 вересня 2022 р.

[110] Так само.
[111] Так само.

Вони розширили повноваження регулятора на обмеження ретрансляції каналів, що становлять загрозу безпеці, та встановили нові вимоги щодо розкриття реальних бенефіціарів медіа[112].

Зокрема, новий закон забороняє видавати ліцензії на мовлення телепрограмам, виключеним із латвійського переліку ретрансляції, якщо країна їхньої юрисдикції «загрожує територіальній цілісності, суверенітету або національній незалежності іншої держави». Окремо встановлено мовні вимоги: при поширенні програм із мовним треком, що не є офіційною мовою країни ЄС або ЄЕП (на практиці передусім російською), кабельні оператори зобов'язані забезпечити основний мовний трек латвійською мовою[113]. Це є принципово важливим заходом, оскільки він не забороняє контент як такий, але усуває мовний привілей, який де-факто перетворював латвійський кабельний ефір на канал поширення кремлівських наративів.

Реальним наслідком змін стало те, що у червні 2022 р. Національна рада з електронних медіа (NEPLP) заблокувала 80 російських телеканалів[114]. Закон також зобов'язав усі електронні медіа, що отримали дозволи на ретрансляцію та мовлення, повідомити NEPLP про реальних бенефіціарів до 31 жовтня 2022 р., надавши регулятору право виключати медіа зі списку ретрансляції у разі непредставлення або фальсифікації відповідних відомостей[115].

Структурно важливою новиною є те, що з 2025 р. в Латвії розпочало роботу об'єднане Латвійське громадське медіа (LSM), що поєднало суспільне радіо і телебачення під управлінням Ради з громадських електронних медіа (SEPLP). Метою реструктуризації є підвищення якості контенту, зокрема для

---

[112] Andersone I. New amendments to the Latvian Electronic Mass Media Law enter into force. *IRIS*. 2022. 2022-9:1/9. URL:https://merlin.obs.coe.int/iris/2022/9/article9.en.html (дата звернення: 01.04.2026).
[113] Так само.
[114] Оксентюк А., Радь П., Клімов Р. та ін. Регіональний аспект союзу РФ і Білорусі: наслідки для сусідів / за ред. Я. Чорногора. Київ : Рада зовнішньої політики "Українська призма", 2025.
[115] Andersone I. New amendments to the Latvian Electronic Mass Media Law enter into force. *IRIS*. 2022. 2022-9:1/9. URL:https://merlin.obs.coe.int/iris/2022/9/article9.en.html (дата звернення: 01.04.2026).

російськомовної аудиторії, та підсилення спроможності протидіяти дезінформації альтернативними якісними продуктами[116].

Литва поєднує жорстке регулювання медіапростору з проактивним захистом інформаційної інфраструктури. Правовою базою слугує Закон про інформацію суспільства, який дозволяє обмежувати трансляцію пропагандистських програм, а Комісія з радіо і телебачення Литви (LRTK) активно застосовує ці повноваження для блокування незаконних джерел, включаючи вебсайти, що ретранслюють пропаганду без дозволу[117].

Окремим напрямом впровадження Директиви NIS2 загальноєвропейського стандарту кібербезпеки для критичної інфраструктури. Литва посідає лідерські позиції серед балтійських держав за швидкістю та жорсткістю імплементації: литовський уряд оперативно інтегрував вимоги NIS2 до Закону про кібербезпеку, розширивши перелік «суттєвих» та «важливих» суб'єктів. Регуляторні органи очікуються найсуворіші у регіоні щодо дотримання, особливо у секторах енергетики, фінансів та комунального управління. Регулювання охоплює не лише IT-системи, але й операційні технології (OT), зокрема промислові системи управління та комунальну інфраструктуру[118].

Латвія рухається повільніше: процес транспозиції NIS2 у національне законодавство тривав, а компанії зіткнулися з невизначеністю щодо того, які з них потраплять до категорії «важливих суб'єктів». Більшість організацій у Латвії перебувала на стадії обізнаності та базових оцінок ризиків, а не повноцінних програм відповідності. Естонія, що позиціонується як «цифровий лідер» регіону, має найбільш розвинені е-уряд та системи кібербезпеки, однак NIS2 вводить нові виклики: розширення сфери охоплення (постачальники IT-послуг середнього

[116] Nikers O., Tabuns O. Bureaucratic policy and defense cooperation among the Baltic states. *Security and Defence Quarterly*. 2022. Vol. 37, No. 1. P. 41–54. DOI: https://doi.org/10.35467/sdq/145571.
[117] Так само.
[118] NIS2 in the Baltics: How Lithuania, Latvia, and Estonia Differ / Baltic Amadeus. 23.09.2025. URL: https://www.balticamadeus.lt (дата звернення: 01.04.2026).

розміру, хмарні компанії), суворіші строки повідомлення про інциденти (24-72 години) та посилений контроль за безпекою ланцюгів постачання[119].

Суттєвою спільною рисою є те, що санкції за порушення NIS2 є однаковими для всіх трьох держав і є вельми значними: до €10 млн або 2% глобального обороту для суттєвих суб'єктів; до €7 млн або 1,4% для важливих суб'єктів[120]. Ці санкції є потужним стимулом для медіаорганізацій та платформ підтримувати безпеку своєї інфраструктури на рівні, що відповідає стандартам захищеного інформаційного простору.

Інституційна архітектура інформаційної безпеки країн Балтії є результатом тривалої еволюції, що розпочалася із вступом до НАТО та ЄС у 2004 р. Яковюк та Шестопал фіксують, що вступ до НАТО «призвів до суттєвих змін оборонних концепцій і концепцій національної безпеки», а балтійські держави сформулювали серед пріоритетів своєї нової архітектури безпеки «будівництво і розвиток сучасних збройних сил і структур безпеки» та «цілеспрямоване та ефективне використання ресурсів, виділених на національну безпеку і оборону». Концепції та стратегії національної безпеки 2004-2012 рр. охоплювали не лише оборону, але й «зовнішню політику, економіку, навколишнє середовище, енергетичну і інформаційну безпеку», демонструючи комплексний підхід, що є безпосереднім фундаментом нинішньої інституційної архітектури[121].

Відповідно до Концепції широкої безпеки, КАРО та Служба зовнішньої розвідки щорічно публікують детальні звіти про дезінформаційних акторів, платформи, наративи та цілі де-факто публічну базу знань для всіх інших гравців. Медіаграмотність інституційно закріплена за Міністерством освіти і науки (§ 533 Закону про медіапослуги). Завдання з протидії дезінформації відображені у чотирьох стратегічних документах: Плані розвитку національної оборони до 2031 р., Цифровій програмі до 2030 р., Плані розвитку внутрішньої

[119] Так само.
[120] Так само.
[121] Яковюк І. В., Шестопал С. С. Правове регулювання політики національної безпеки країн Балтії в контексті еволюції стратегічних концепцій НАТО. Проблеми законності. 2018. Вип. 143. С. 218-227. DOI: 10.21564/2414-990x.143.148488.

безпеки до 2030 р. та Плані розвитку згуртованої Естонії до 2030 р. Відзначається лише брак єдиної спільної термінології між ними як перешкоду для повноцінної міжвідомчої координації[122].

Центральним незалежним регулятором Латвії є NEPLP, що здійснює моніторинг, видачу дозволів і блокування. Після 2022 р. її повноваження суттєво розширились: NEPLP отримала право виключати програми зі списку ретрансляції за ненадання або фальсифікацію даних про бенефіціарів[123]. Центр передового досвіду НАТО зі стратегічних комунікацій (StratCom COE) у Ризі, що діє з 2014 р., є ключовою установою з дослідження інформаційних операцій та розробки рекомендацій для всього Альянсу[124]. Щорічна доповідь Бюро захисту Конституції Латвії (SAB) за 2025 р. є одним із найбільш деталізованих публічних документів регіону щодо природи інформаційної агресії Росії. Вона фіксує, що Москва застосовує проти Заходу широкий спектр інструментів впливу з метою підриву єдності у підтримці України або навіть повного припинення цієї підтримки[125].

Литва вирізняється найбільш комплексним підходом, що поєднує медіарегулювання з кібербезпековою стратегією та загальнонаціональною обороною. LRTK активно блокує вебсайти без ліцензії, що ретранслюють пропагандистський контент[126]. VSD та AOTD здійснюють щорічні «Національні оцінки загроз»: у «Національній оцінці загроз 2026» зафіксовано систематичну ворожу інформаційну діяльність з боку Росії та Білорусі[127]. Особливим рішенням було інтегрування медіастійкості в систему загальнонаціональної оборони: курс із громадянської освіти та навичок оборони для учнів 9 класів, запроваджений

[122] Estonian Internal Security Service (KAPO). Annual Review 2024–2025. Tallinn: KAPO, 2025. URL: https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf
[123]Andersone I. New amendments to the Latvian…
[124] Nikers O., Tabuns O. Bureaucratic policy…
[125] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report 2025. Riga : SAB, 2026. 35 p. URL: https://www.sab.gov.lv/en/annual-reports/ (дата звернення: 01.04.2026).
[126] Nikers O., Tabuns O. Bureaucratic policy and defense cooperation among the Baltic states. *Security and Defence Quarterly*. 2022. Vol. 37, No. 1. P. 41–54. DOI: https://doi.org/10.35467/sdq/145571.
[127] Defence Intelligence and Security Service (AOTD); State Security Department (VSD). National Threat Assessment 2026. Vilnius, 2026. 90 p.

2022 р., передбачав 100-відсоткове охоплення до 2024-2025 рр.[128]. Цей захід є інституціоналізацією готовності суспільства до спротиву як освітнього стандарту і прямим продовженням тієї логіки «широкої безпеки», де суспільна стійкість до інформаційних маніпуляцій є рівноцінним елементом поряд з військовим потенціалом.

Спільною рисою інституційних моделей усіх трьох держав є поєднання Державного регулятора (верхній рівень), спецслужбового моніторингу (безпековий рівень), суспільного мовника як джерела альтернативного контенту (медійний рівень) та громадянського суспільства і освітніх ініціатив (рівень стійкості). Ця модель цілком узгоджується з висновком Яковюка та Шестопала про те, що сучасна балтійська безпекова політика реалізується на основі «комплексного підходу, при якому зовнішня політика, оборонна політика та політика внутрішньої безпеки, а також забезпечення єдності та стійкості суспільства були визнані запорукою досягнення цілей політики безпеки»[129]. Концептуально це відповідає і висновку дослідників НАТО: «протидія гібридним загрозам потребує не стільки нових спроможностей, скільки нових партнерів, нових процесів і, головне, нового мислення» [130].

2.2. Протидія російській дезінформації та пропаганді

Після лютого 2022 р. протидія російській дезінформації перетворилася з одного із завдань інформаційної безпеки країн Балтії на її системоутворюючий пріоритет. Якщо у попередній період відповідні зусилля були переважно реактивними та фрагментарними, то впродовж 2022-2026 рр. усі три держави здійснили перехід до комплексної багаторівневої системи протидії, що поєднує правові, технічні, комунікаційні та освітні інструменти. Принциповим для розуміння балтійського досвіду є те, що жодна з держав не обмежилася суто

[128] Каракуць О. Основні тенденції зовнішньої політики і національної безпеки Литви. Київ : НІСД, 2024.
[129] Яковюк І. В., Шестопал С. С. Правове регулювання політики національної безпеки країн Балтії в контексті еволюції стратегічних концепцій НАТО. *Проблеми законності*. 2018. Вип. 143. С. 218–227. DOI: 10.21564/2414-990x.143.148488.

заборонними заходами: кожна виробила власну конфігурацію між обмежувальними й позитивними стратегіями, детерміновану специфікою аудиторій, мовним складом населення та наявними інституційними спроможностями.

Коректне розуміння механізмів протидії неможливе без попереднього аналізу того, яку загрозу вони покликані нейтралізувати. Щорічна доповідь Бюро захисту Конституції Латвії (SAB) за 2025 р. фіксує: Москва застосовує проти Заходу широкий спектр інструментів впливу з метою підриву єдності у підтримці України або навіть повного припинення цієї підтримки, а також підготовки до потенційного протистояння з НАТО[131]. Ключовою умовою ефективності цих інструментів є глибоко викривлене сприйняття реальності самими авторами кремлівських наративів: SAB констатує, що ізоляція еліти Кремля та відсутність критичних голосів усередині системи підсилюють перекручене бачення Заходу як екзистенційної загрози режиму, що своєю чергою генерує дедалі агресивніші інформаційні операції[132].

Особливу тривогу викликає те, що, на оцінку SAB, сприйняття Росією Латвії дедалі більше нагадує те, яким воно було щодо України напередодні війни[133]. Поширювані наративи зображують Латвію як «русофобну державу», що пригнічує російськомовне населення, як «нацистську державу», «маріонетку Великої Британії та США» і «державу, що не відбулася». До початку повномасштабного вторгнення аналогічні наративи Москва застосовувала щодо України, а нині поширює їх на всі три балтійські країни. Цей паралелізм є не випадковим: він свідчить про функціонування стандартизованого нарративного шаблону, що адаптується до конкретного об'єкта дезінформаційного впливу.

Литовська «Національна оцінка загроз 2026», підготовлена AOTD та VSD, підтверджує цей висновок із власної перспективи. Документ фіксує, що Адміністрація Президента Росії формує пропагандистські наративи, які

---

[131] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report 2025. Riga: SAB, 2026. 35 p. URL: https://www.sab.gov.lv (дата звернення: 01.04.2026).
[132] Так само.
[133] Так само.

звинувачують балтійські держави у систематичному спотворенні історії Другої світової війни, прославлянні нацистських колаборантів та переслідуванні російськомовних[134]. Міністерство закордонних справ Росії відіграє ключову роль у поширенні звинувачень у русофобії в міжнародних інституціях, що є частиною спроби чинити тиск на Литву та інші балтійські держави[135].

Важливим виміром загрози стало використання штучного інтелекту в інформаційних операціях. SAB фіксує зростаюче застосування ІІ в російських інформаційних операціях для генерування контенту, більш відповідного цільовій аудиторії та зрозумілішого для неї[136]. Штучний інтелект також суттєво знижує вартість виробництва контенту іншими мовами та його розповсюдження поза традиційними російськими цільовими групами. Литовська оцінка загроз, у свою чергу, акцентує на активному використанні Росією платформи TikTok для поширення наративів серед молоді у форматі розважальних відео, мемів та аудіодоріжок, що приховують проросійські меседжі[137].

Окремим виміром загрози стало використання правових механізмів як нового гібридного інструмента. SAB документує, що МЗС Росії внутрішньо визнало необхідність «правової боротьби» проти Заходу і систематично готує позови до міжнародних судових органів, зокрема, до Міжнародного суду ООН, проти балтійських держав. Заявлена підстава порушення прав російськомовного населення відповідно до Міжнародної конвенції про ліквідацію всіх форм расової дискримінації (ICERD). Підготовчий процес, за оцінкою SAB, перебуває у завершальній фазі, і Росія, ймовірно, подасть заявку проти Латвії у 2026 р.[138]. Таким чином, правовий інструментарій перетворюється на новий гібридний інструмент, органічно вбудований у загальну архітектуру інформаційної агресії.

Серед трьох балтійських держав Латвія обрала найбільш радикальний шлях у протидії пропаганді, що пояснюється специфічним демографічним

---

[134] Defence Intelligence and Security Service (AOTD); State Security Department (VSD). National Threat Assessment 2026. Vilnius, 2026. 90 p.
[135] Так само.
[136] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[137] Defence Intelligence and Security Service (AOTD)…
[138] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…

контекстом: значна частка російськомовного населення країни традиційно споживала контент із Росії, формуючи стійкі канали кремлівського впливу. Ключові законодавчі зміни до Закону про електронні медіа, що набули чинності у вересні 2022 р., розширили повноваження Національної ради з електронних медіа (NEPLP) і встановили нові вимоги щодо розкриття реальних бенефіціарів медіа[139]. У червні 2022 р. NEPLP заблокувала 80 російських телеканалів - безпрецедентний захід навіть у балтійському контексті[140].

SAB у своїй доповіді за 2025 р. підкреслює, що Москва продовжує впливати на латвійський та міжнародний інформаційний простір, поширюючи наративи, спрямовані на збільшення розколу і суперечностей у латвійському суспільстві та зниження довіри до державних інституцій і союзників у ЄС та НАТО[141]. Соціальні мережі та комунікаційні застосунки набувають дедалі більшого значення для поширення російських наративів. Паралельно розгорталося формування позитивної медіа альтернативи. З 2025 р. в Латвії розпочало роботу об'єднане Латвійське громадське медіа (LSM), яке об'єднало суспільне радіо і телебачення під управлінням SEPLP з метою підвищення якості контенту для різних мовних груп та посилення спроможності протидіяти дезінформації[142].

Важливим виміром є кіберзахист як складова протидії інформаційній агресії. SAB фіксує, що загальний рівень зареєстрованих кіберзагроз щодо Латвії досяг рекордного рівня у 2025 р., збільшившись багатократно порівняно з 2022 р.[143]. Атаки типу DDoS на урядові установи систематично прив'язувалися до національно значущих дат або політичних рішень наприклад, масштабна атака у липні після оголошення латвійської компанії переможцем міжнародного тендеру на безпілотники. Це свідчить про те, що кібератаки є органічним компонентом

---

[139] Andersone I. New amendments to the Latvian Electronic Mass Media Law enter into force. *IRIS*. 2022. 2022-9:1/9. URL: https://merlin.obs.coe.int/iris/2022/9/article9.en.html (дата звернення: 01.04.2026).
[140] Nikers O., Tabuns O. Bureaucratic policy and defense cooperation…
[141] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[142] Nikers O., Tabuns O. Bureaucratic policy and defense cooperation…
[143] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…

ширших інформаційних операцій, спрямованих на підрив суспільної довіри до державних інституцій.

SAB також фіксує зростаючу загрозу кіберінцидентів в операційних технологіях системах моніторингу й управління фізичними процесами та критичною інфраструктурою[144]. Конкретні приклади з 2025 р. ілюструють реальність цієї загрози: у квітні 2025 р. російські хактивісти здійснили кібератаку на дамбу в Норвегії на озері Рисетватнет, скориставшись слабким паролем до панелі управління, підключеної до Інтернету; у серпні 2025 р. атаці зазнала гідроелектростанція в Гданську, де під час другої спроби нападникам вдалося дистанційно отримати доступ до систем управління і змінити операційні параметри, що призвело до повного відключення електростанції[145].

Одним із найбільш показових прикладів ескалації загроз є серія цілеспрямованих кібератак, яких зазнала Латвія у листопаді 2022 року. Зокрема, 14 та 22 листопада хактивістське угруповання «Killnet», яке відкрито підтримує політику Кремля, використало платформу Telegram для координації масштабних розподілених атак на відмову в обслуговуванні (DDoS) проти критичної інфраструктури всього балтійського регіону[146]. Головними цілями цих атак стали державні установи, структури сектору національної безпеки та оборони (включно з CERT-LV), а також підприємства життєзабезпечення. Цей інцидент яскраво продемонстрував, що інформаційна війна не обмежується лише пропагандою в медіа, а включає прямі спроби паралізувати цифрову життєдіяльність держав, що, своєю чергою, вимагає від них створення надійних інструментів раннього виявлення та реагування на кіберінциденти[147].

Естонська модель протидії дезінформації вирізняється поєднанням чіткого інституційного розподілу повноважень, прозорої публічної комунікації щодо загроз і вимірюваного моніторингу ефективності вжитих заходів. Річний огляд

---

[144] Так само.
[145] Так само.
[146] CERT-LV. (2023). Latvian cybersecurity and CERT.LV technical activities: Annual report 2023. Information Technology Security Incident Response Institution of the Republic of Latvia.
[147] Vasilevska, S., Vasilevskis, E., & Vitolina, Z. (2025). Cybersecurity policy analysis and research cooperation in the Baltic States. Research for Rural Development, 40, 326-332. DOI: 10.22616/RRD.31.2025.043

Естонської служби внутрішньої безпеки (КАРО) за 2024-2025 рр. констатує: незалежно від публічної риторики, Росія активно працює над демонтажем архітектури безпеки Європи та формуванням привілейованої сфери впливу, де НАТО було б змушене відступити[148].

У 2024 р., за даними КАРО, по всій Європі відбулася серія підпалів, актів вандалізму та саботажу під керівництвом ГРУ - військової розвідки Росії. Через ці гібридні операції Росія прагне дестабілізувати Європу та послабити колективну рішучість підтримувати Україну[149]. В Естонії зафіксовано конкретний інцидент: у Тарту підпалено автомобіль із українськими номерними за підбурюванням Росії. За рекомендацією КАРО з початку повномасштабного вторгнення в Естонії скасовано 15 посвідок на проживання з міркувань національної безпеки[150].

КАРО виявила систематичну переорієнтацію кремлівських зусиль впливу на молодь: оскільки контрольовані Кремлем ЗМІ стикаються з дедалі більшими обмеженнями, проросійська пропаганда переміщується до соціальних мереж. Фіксується зростання кількості діпфейків та маніпуляцій за допомогою штучного інтелекту і алгоритмів. Соціальні мережі формують уявлення людей про світ і визначають інформаційні бульбашки, у які потрапляють користувачі, в результаті чого ті можуть опинитися в інформаційних камерах луна або петлях дезінформації з дедалі меншою можливістю перевірити те, що вони бачать[151].

Завдяки санкціям ЄС та ініціативі Агентства захисту прав споживачів (TTJA) в Естонії заблоковано доступ до 389 телеканалів, вебсайтів та акаунтів у соціальних мережах, пов'язаних із Кремлем[152]. Щорічне опитування Міністерства оборони Естонії засвідчило вимірювані результати: частка неестонців, які регулярно переглядали російські телеканали, скоротилася з 62% навесні 2021 р. до 33% навесні 2022 р. і до 24% навесні 2023 р.; аудиторія

[148] Estonian Internal Security Service (KAPO). Annual Review 2024–2025. Tallinn: KAPO, 2025.
[149] Так само.
[150] Так само.
[151] Так само.
[152] Propastop. Чи є якась користь від обмеження кремлівських каналів? 27.11.2023. URL: https://www.propastop.org

російських новинних порталів відповідно знизилась із 51% до 32%[153]. Проте самі дослідники застерігають, що «вплив обмежень потребує кращого вимірювання», оскільки зміни аудиторії можуть зумовлюватися й іншими факторами.

Волонтерська ініціатива «Propastop» за участю Кайтселійт доповнює офіційну систему публічним моніторингом пропагандистських каналів і забезпечує зворотний зв'язок, якого бракує централізованим структурам[154]. При цьому «Propastop» принципово наголошує на обмеженості суто заборонних заходів: навіть за зниження аудиторії «кількість людей в Естонії, які поділяють цінності та погляди інформаційного простору Кремля, все ще велика» - на що вказує дослідження Фонду Фрідріха Еберта (вересень 2023 р.)[155]. Цей висновок є одним із найвагоміших аргументів на користь поєднання обмежень із позитивними стратегіями медіаграмотністю, альтернативним якісним контентом та інтеграційними програмами.

Литовська «Національна оцінка загроз 2026» документує специфічний механізм проросійської пропагандистської діяльності: використання литовських громадян, прихильників російського режиму, для реалізації ворожої інформаційної політики зсередини[156]. Ці особи співпрацюють співробітниками білоруських та російських пропагандистських структур, надають їм інтерв'ю, беруть участь у антилитовських пропагандистських кампаніях, зображуючи Литву як недемократичну державу під контролем Заходу з нацистським та русофобським режимом при владі[157].

Визначальною рисою російської пропаганди в литовському контексті є повторюваність наративів. Пропагандистські кампанії базуються на кількох циклічних наративах, що діють як стандартні моделі і адаптуються до конкретних ситуацій[158]. Це наочно виявилося під час кампанії щодо відключення Литви та інших балтійських держав від енергосистеми БРЕЛЛ: Росія

[153] Так само.
[154] Так само.
[155] Так само.
[156] Estonian Internal Security Service (KAPO)…
[157] Так само.
[158] Так само.

використовувала чотири усталені пропагандистські наративи «Радянська ера принесла більше користі, ніж шкоди»; «Литва не є суверенною державою»; «Литва проводить провокаційну політику щодо Росії»; «Ворожість до Росії шкодить економіці Литви»[159]. Пропагандистські канали та автоматизовані акаунти в соціальних мережах поширювали згенеровані ШІ зображення, підвищуючи охоплення кампанії.

Фундаментальним каналом розповсюдження пропагандистських наративів у Литві стала ідеологічна роль Московського Патріархату. «Національна оцінка загроз 2026» фіксує, що Московський Патріархат здійснює значний вплив на підпорядковані йому єпархії за кордоном, включно 3 Православною єпархією Вільнюса і Литви, що дозволяє Росії поширювати свій вплив у православній общині країни[160]. Православна церква відіграє суттєву роль у формуванні та підтримці ідеологічних наративів російського режиму, зокрема, ідеї «Руського світу» та зміцнення впливу в зарубіжних країнах.

Литовська розвідка також задокументувала використання псевдонаукових академічних структур у пропагандистських цілях. Такі організації, як Балтійський федеральний університет імені Іммануїла Канта, Фонд підтримки і захисту прав співвітчизників за кордоном (заснований МЗС Росії) та Фонд «Historical Memory» (заснований з ініціативи Адміністрації Президента Росії), мають завдання демонструвати, що балтійські держави підтримують нацистську ідеологію та проводять русофобську політику[161]. Ці організації проводять конференції та виставки, де проросійські діячі з Литви виступають як «експерти», представляючи сфабриковані звинувачення Росії як експертні оцінки.

Ключовим механізмом формування стійкої інформаційної політики країн Балтії у період 2022-2026 років є гармонізація національного законодавства з жорсткими нормативно-правовими рамками Європейського Союзу.

[159] Так само.
[160] Так само.
[161] Так само.

Центральним інструментом у цьому контексті стала Директива (ЄС) 2022/2555 (більш відома як NIS2), ухвалена Європейським Парламентом та Радою ЄС 14 грудня 2022 року[162]. Директива NIS2 зобов'язує держави-члени впровадити безпрецедентно високі та єдині стандарти кібербезпеки, що поширюються на значно ширше коло суб'єктів, ніж раніше, включаючи постачальників цифрових послуг, енергетичні компанії, транспортний сектор, охорону здоров'я та державні адміністрації. Цей правовий механізм змусив Естонію, Латвію та Литву ініціювати масштабні зміни до внутрішнього законодавства, посилюючи вимоги для приватного сектору та розширюючи повноваження регуляторних органів.

Варто зазначити, що стаття 7 Директиви NIS2 містить імперативну вимогу до держав-членів: у рамках своїх національних стратегій кібербезпеки вони зобов'язані сприяти розробці та розвитку науково-дослідних та дослідно-конструкторських (R&D) ініціатив. До переліку критично важливих секторів відтепер віднесено й науково-дослідні організації. Як реакція на ці вимоги, Кабінет Міністрів Латвії 28 березня 2023 року ухвалив Постанову № 158 "Про Стратегію кібербезпеки Латвії на 2023-2026 роки"[163]. Цей стратегічний документ чітко визначає, що ефективна інформаційна політика неможлива без інвестицій в людський капітал. Тому основними напрямами дій у Латвії було визначено не лише технічний захист, а й підвищення обізнаності громадськості, реформування системи освіти, стимулювання наукових досліджень та розвиток міжнародного співробітництва у кіберпросторі[164].

На інституційному рівні країни Балтії активно розбудовують спеціалізовані центри, які виконують функцію "інформаційного щита". Важливим інструментом є використання наднаціональних платформ, таких як структури НАТО та ініціативи ЄС. Зокрема, Стратегія ЄС для регіону Балтійського моря, започаткована ще у 2009 році, залишається дієвим

---

[162] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union.

[163] Latvian Cabinet of Ministers. (2023). Latvian Cybersecurity Strategy 2023–2026 [Cabinet Regulation No. 158].

[164] Vasilevska, S., Vasilevskis, E., & Vitolina, Z. (2025). Cybersecurity policy analysis and research cooperation in the Baltic States. Research for Rural Development, 40, 326-332. DOI: 10.22616/RRD.31.2025.043

інструментом для стимулювання транскордонної співпраці у сфері кібербезпеки. Проте, як свідчать дослідження, попри приналежність усіх трьох країн до одних і тих самих політичних та військових блоків (ЄС і НАТО), їхня інституційна розбудова історично відбувалася асиметрично і переважно ізольовано. Це призвело до фрагментації інформаційної політики на регіональному рівні, де замість єдиного кіберфронту можна спостерігати три окремі національні системи, які лише починають вибудовувати ефективні механізми взаємодопомоги[165].

Не менш критичним викликом для механізмів інформаційної політики є фінансове та ресурсне забезпечення. Аналіз джерел фінансування наукових досліджень у сфері кібербезпеки країн Балтії вказує на структурну вразливість. Близько 56% усіх дослідницьких бюджетів у регіоні формуються за рахунок коштів фондів Європейського Союзу, зокрема грантових програм Horizon 2020 (нині Horizon Europe), програми Digital Europe та Європейського фонду регіонального розвитку (ERDF)[166]. Хоча таке фінансування дозволило країнам здійснити технологічний ривок, воно водночас створило ефект надмірної залежності (overreliance). За відсутності довгострокових, стабільних національних механізмів фінансування, стратегічна автономія країн Балтії в інформаційній сфері залишається під загрозою. Для сталого розвитку їм необхідно переходити від грантової моделі до моделі системних державних інвестицій у дослідження та розробку вітчизняних рішень з кіберзахисту.

2.3. Стратегічні комунікації та публічна дипломатія

Стратегічні комунікації посідають особливе місце в загальній архітектурі інформаційної безпеки країн Балтії, виконуючи подвійну функцію: формування стійкого до маніпуляцій внутрішнього інформаційного простору та позиціонування держав на міжнародній арені в умовах систематичних

[165] Так само.
[166] Так само.

дезінформаційних атак. Обидва виміри набули якісно нового значення після лютого 2022 р.

На рівні НАТО ключовою установою регіону є Центр передового досвіду зі стратегічних комунікацій (StratCom COE) у Ризі, що діє з 2014 р.: він системно аналізує методологію і тактику російських інформаційних операцій та надає аналітичну підтримку урядам країн-членів і командуванню НАТО. Центр передового досвіду НАТО з кіберзахисту (CCDCOE) у Таллінні, заснований у 2008 р. після кібератак на Естонію 2007 р., є визнаним аналітичним центром із питань кіберзахисту та нормативної бази кіберпростору[167].

На національному рівні Естонія побудувала найбільш чітку інституційну конструкцію: координаційним центром є Відділ стратегічних комунікацій Державної канцелярії. KAPO у 2024 р. охопила близько 2000 офіційних осіб навчальними заходами та брифінгами з безпеки[168] - реалізуючи принцип превентивної дипломатії безпеки. У Латвії SAB здійснює інформування громадськості через щорічні публічні доповіді. Директор SAB Егілс Звієдріс прямо закликає громадян до особистої відповідальності: «наші противники хотіли б виконати значну частину роботи руками латвійців, без їхнього усвідомлення цього» і рекомендує «зробити глибокий вдих перед тим, як ділитися, здавалося б, скандальною інформацією»[169]. Литовські органи AOTD та VSD реалізують стратегічні комунікації через спільну «Національну оцінку загроз», що містить консолідовану несекретну оцінку загроз та закликає громадян до критичного мислення[170].

Одним із найсуттєвіших зрушень стало переосмислення медіаграмотності: з освітньої дисципліни вона трансформувалася в інструмент стратегічної комунікації та складову системи національної безпеки. В Естонії медіаграмотність законодавчо закріплена за Міністерством освіти і науки (§ 533

[167] Nikers O., Tabuns O. Bureaucratic policy and defense cooperation…
[168] Estonian Internal Security Service (KAPO)…
[169] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[170] Defence Intelligence and Security Service (AOTD); State Security Department (VSD). National Threat Assessment 2026. Vilnius, 2026. 90 p.

Закону про медіапослуги), а критичне мислення визначено як «єдиний надійний антидот» зростаючим дезінформаційним загрозам[171]. Литва пішла найдалі, інтегрувавши медіастійкість у систему загальнонаціональної оборони: курс із громадянської освіти та навичок оборони для учнів 9 класів, запроваджений 2022 р., передбачає 100-відсоткове охоплення до 2024-2025 рр.[172]. Литовська оцінка загроз наголошує: кожен громадянин робить свій внесок у оборонний потенціал, розвиваючи здатність виявляти загрози та запобігати їм[173]. Латвія реалізує медіаграмотність переважно через публічну комунікацію SAB та превентивні звернення - «не піддаватися емоціям і не потрапляти до пасток, розставлених в інформаційній сфері»[174]; Міністерство оборони фінансує централізований захист від DDoS-атак, що надається від LVRTC[175].

Країни Балтії активно використовують свій досвід протидії дезінформації як ресурс зовнішньої публічної дипломатії. Вони відіграли активну роль у просуванні DSA та EMFA, а їхній досвід вплинув на вимоги щодо прозорості медіавласності та обмеження пропагандистського контенту[176]. Важливим вектором є партнерство з Україною: SAB у 2025 р. вів переговори щодо угоди про захист класифікованої інформації - символ стратегічного зближення у сфері безпеки[177]. Литовська «Національна оцінка загроз 2026» наголошує, що підтримка Заходу України значною мірою визначатиме здатність України протистояти агресії[178]. Регулярна публікація доповідей KAPO[179], SAB[180] та оцінок загроз AOTD/VSD[181] англійською мовою формує міжнародний порядок денний і є формою стратегічної комунікації, що впливає на союзницький консенсус. Балтійський підхід підтверджує висновок дослідників НАТО:

---

[171] Естонія. Про медіапослуги (Meediateenuste seadus): Закон Естонської Республіки від 14 черв. 2022 р. URL: https://www.riigiteataja.ee/en/eli/514062022001/consolide (дата звернення: 01.04.2026).
[172] Каракуць О. Основні тенденції…
[173] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…
[174] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[175] Так само.
[176] Nikers O., Tabuns O. Bureaucratic policy…
[177] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[178] Так само.
[179] Estonian Internal Security Service (KAPO). Annual Report…
[180] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[181] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…

«протидія гібридним загрозам потребує не стільки нових спроможностей, скільки нових партнерів, нових процесів і, головне, нового мислення»[182].

Попри суттєві досягнення, балтійські стратегічні комунікації стикаються з системними викликами. По-перше, фрагментарність термінологічного апарату між стратегічними документами ускладнює міжвідомчу координацію. По-друге, зростаюче використання Росією ШІ для генерування цільового контенту вимагає технологічної модернізації інструментів виявлення і нейтралізації дезінформації: SAB фіксує, що ШІ знижує вартість створення контенту іншими мовами та розширює традиційне коло цільових груп[183]. По-третє, частина суспільства залишається сприйнятливою до кремлівських наративів - це підтверджується і естонськими даними[184], і литовськими спостереженнями[185]. KAPO наголошує, що Росія переорієнтовує операції впливу на молодих російськомовних естонців[186], отже виклики не будуть зменшуватися, а трансформуватися.

Концептуальним рамковим документом слугує EMFA (набрав чинності 8 серпня 2025 р.), що поєднує свободу медіа як цінність із безпекою медіапростору як необхідністю[187]. Його імплементація у всіх трьох балтійських державах у 2025-2026 рр. створює якісно новий нормативний фундамент. Підсумовуючи, можна виокремити кілька закономірностей: усі три держави здійснили перехід від переважно реактивного до проактивно-превентивного підходу; балтійська практика демонструє ефективність поєднання обмежень із позитивними заходами - медіаграмотністю, публічними комунікаціями розвідувальних відомств і розбудовою якісного публічного мовлення; загальноєвропейські інструменти, DSA, EMFA, NIS2, слугують не лише правовою базою, а й механізмом координації, що надає балтійській практиці виміру, який виходить за межі регіону.

---

[182] Aaronson M. et al. NATO Countering the Hybrid Threat. *PRISM*. 2011. Vol. 2, No. 4. P. 112–124.
[183] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[184] Propastop. Чи є якась користь від обмеження…
[185] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…
[186] Estonian Internal Security Service (KAPO). Annual Report…
[187] The Media Services Bill will reach the Riigikogu/Estonian Ministry of Culture. 06.02.2026. URL: https://ifacca.org/news/2026/02/06/media-services-bill-will-reach-riigikogu/ (дата звернення: 01.04.2026).

РОЗДІЛ 3. ПОРІВНЯЛЬНИЙ АНАЛІЗ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ЕСТОНІЇ, ЛАТВІЇ ТА ЛИТВИ

Порівняльний аналіз інформаційних стратегій трьох балтійських держав є методологічно необхідним продовженням вивчення механізмів та інструментів, розглянутих у попередньому розділі. Методологічною основою аналізу є концепція «широкої безпеки», яка, за Яковюком та Шестопалом, охоплює як «тверді», так і «м'які» виміри безпекової взаємодії та передбачає, що «питання вищого рівня - суверенітет та територіальна цілісність - є однаковими для всіх трьох держав», тоді як «щодо забезпечення складових сфери «м'якої» безпеки кожна держава може мати свої пріоритети»[188]. Саме до сфери «м'якої» безпеки відноситься регулювання інформаційного простору, і саме тут найбільш чіткими є відмінності між підходами трьох країн.

Порівняльний аналіз ускладнюється тим, що балтійські держави є одночасно схожими та різними: схожими у своїй спільній радянській спадщині, євроатлантичній орієнтації та стратегічному становищі «фронтових держав» щодо Росії, різними є у демографічних характеристиках, правових традиціях, ступені цифрового розвитку та конкретних пріоритетах інформаційної безпеки. Дослідники Чакарс та Екманіс підкреслюють, що попри спільні загрози «три країни відрізняються одна від одної в питаннях масштабу, демографії та ступеня їхньої залученості до різних питань»[189].

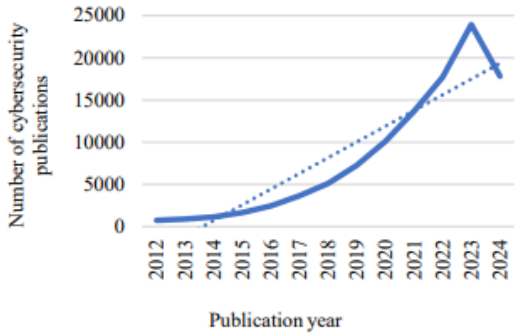
3.1. Інформаційна стратегія Естонії: цифровий лідер на передовій кіберзахисту

Незважаючи на спільний геополітичний контекст, схоже історичне минуле та ідентичні зовнішні загрози, порівняльний аналіз інформаційної політики та стратегій кібербезпеки Латвії, Литви та Естонії виявляє суттєві диспропорції у їхньому розвитку. Ці розбіжності найбільш яскраво простежуються у рівнях інституційної спроможності, науково-дослідної активності та впровадженні

[188] Яковюк І. В., Шестопал С. С. Правове регулювання політики…
[189] Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії: Довга тінь Росії/пер. І. Ємельянової. Бостон : Academic Studies Press, 2025. 306 с.

стратегічних ініціатив. Для об'єктивного вимірювання цих показників міжнародне співтовариство використовує Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI) від Міжнародного союзу електрозв'язку (ITU). Цей індекс комплексно оцінює зусилля держав за п'ятьма критеріями: законодавча база, технічні заходи, організаційні структури, розвиток потенціалу та міжнародне співробітництво[190]. Дані GCI за 2024 рік підтверджують, що всі країни Балтії мають показники, вищі за середньосвітові, проте всередині регіону існує чітка ієрархія[191].

Figure 1
Growth in cybersecurity research publications (2012-2024)



Source: Scopus.

Рис. 3.1. Показники Глобального індексу кібербезпеки (GCI) 2024 року.

Естонія є безперечним та стабільним регіональним лідером, її показник GCI у 2024 році досяг позначки 88.5, що виводить країну в десятку світових лідерів з кібербезпеки. Такий результат не є випадковістю, а радше наслідком стратегічної далекоглядності та ранніх інвестицій у цифрову інфраструктуру. Каталізатором для Естонії стали політично вмотивовані кібератаки у квітні 2007 року (т.зв. події «Бронзової ночі»), які тривали 22 дні і були спрямовані на паралізацію урядових порталів, банківської системи та медіа[192]. Відповіддю на цю кризу стало ухвалення вже у 2008 році першої у світі всеосяжної Національної стратегії кібербезпеки. Успіхи Естонії підкріплюються

[190] International Telecommunication Union. (2024). Global Cybersecurity Index (GCI) 2024. Retrieved from https://www.itu.int/pub/D-HDB-GCI.01-2024
[191] Vasilevska, S., Vasilevskis, E., & Vitolina, Z. (2025). Cybersecurity policy analysis and research…
[192] Center for Security Studies. (2020). Estonia's National Cybersecurity and Cyberdefense Posture. Cyber Reports 2020.

розміщенням у Таллінні Об'єднаного центру передового досвіду НАТО з кіберзахисту (CCDCOE), що забезпечило країні не лише доступ до передових світових практик, але й глибоку інституційну готовність та міцні зв'язки з провідними глобальними експертами[193].

Домінування Естонії підтверджується і бібліометричним аналізом наукових досліджень, проведеним на базі платформи Scopus за період 2012-2024 років. Згідно з дослідженням С. Василевської та колег, загальна кількість наукових публікацій балтійських вчених у сфері кібербезпеки склала 756 статей. З них на частку естонських дослідників припадає вражаючі 54% (408 документів). Провідними центрами генерації цих знань виступають Талліннський технологічний університет (TalTech) та Тартуський університет. Статистичний тест ANOVA ($p = 0.0137$, $F = 4.84$) підтверджує статистично значущу різницю між Естонією та її сусідами, доводячи, що ранній старт у формуванні політики прямо корелює з довгостроковим зростанням науково-технічного потенціалу[194].

Естонська модель інформаційної безпеки є, мабуть, найбільш концептуально цілісною серед трьох балтійських держав. Її стрижнем є парадокс: країна з населенням близько 1,4 млн осіб стала визнаним у глобальному масштабі лідером у сфері кіберзахисту та цифрового урядування. Цей парадокс пояснюється не розміром, а стратегічним вибором: після набуття незалежності 1991 р. Естонія свідомо обрала «цифрову трансформацію» як основний вектор розвитку, що з часом перетворило її на лабораторію найбільш інноваційних рішень у галузі електронного урядування та інформаційної безпеки. Сьогодні Естонія є єдиною країною у світі, де понад 99% державних послуг доступні в режимі онлайн, а цифрова ідентифікація через e-ID охоплює практично все доросле населення.

Як фіксує М. Москалюк, кіберкризи 2007 р. це масштабні DDoS-атаки на державні установи, банки та медіа, спричинені заворушеннями довкола

[193] Vasilevska, S., Vasilevskis, E., & Vitolina, Z. (2025). Cybersecurity policy analysis and research…
[194] Так само.

перенесення «Бронзового солдата», мали для Естонії значення каталізатора «суттєво прискорили формування спеціалізованих інституцій»[195], через що у 2008 р. у Таллінні розпочав роботу Центр передового досвіду НАТО з кіберзахисту (CCDCOE). Цей центр перетворився на визнаний у масштабах НАТО аналітичний осередок з питань нормативної бази кіберпростору, розробником Таллінського посібника - кодифікації міжнародного права у кіберпросторі. Естонська реакція на кризи 2007 р. є показовою: замість того, щоб обмежитися суто захисними заходами, країна скористалася кризою для здобуття інституційного лідерства в масштабах Альянсу.

Стратегічна логіка естонського підходу будується на кількох взаємопов'язаних принципах. По-перше, це «цифровий суверенітет» - переконання, що у відкритій цифровій економіці незалежність інформаційного простору є не менш важливою, ніж традиційний державний суверенітет. По-друге, «суспільна стійкість» - розуміння того, що технічні засоби захисту є недостатніми без відповідного рівня медіаграмотності та критичного мислення у населення. По-третє, «інституційна відкритість» - практика публічного документування загроз через щорічні доповіді KAPO та Служби зовнішньої розвідки, що перетворює розвідувальні дані на інструмент суспільної мобілізації. Саме ця відкритість відрізняє естонський підхід від традиційної розвідувальної закритості і є однією з ключових особливостей балтійської практики[196].

Інституційна архітектура естонської інформаційної безпеки є найбільш структурованою серед трьох держав. Координаційним вузлом є Відділ стратегічних комунікацій Державної канцелярії. Водночас цей відділ не є єдиним актором: завдання з протидії дезінформації паралельно відображені у чотирьох стратегічних документах - Плані розвитку національної оборони до 2031 р.[197],

---

[195] Москалюк М. Ф. Безпекова політика країн Балтії в умовах російсько-української війни. *Регіональні студії*. 2024. № 37. С. 59–63.
[196] Estonian Internal Security Service (KAPO). Annual Review 2024–2025. Tallinn: KAPO, 2025.
[197] Estonian National Defence Development Plan 2031 / Ministry of Defence of the Republic of Estonia. URL: https://www.kaitseministeerium.ee (дата звернення: 01.04.2026).

Цифровій програмі до 2030 р.[198], Плані розвитку внутрішньої безпеки до 2030 р.[199] та Плані розвитку згуртованої Естонії до 2030 р.[200]. Розподіл між документами є водночас перевагою, оскільки йде охоплення кількох вимірів безпеки, і слабкістю: аналітики фіксують «брак єдиної спільної термінології між ними як перешкоду для повноцінної міжвідомчої координації».

Ключовою ланкою правової бази є Закон про медіапослуги, оновлений 9 березня 2022 р., що транспонував Директиву AVMSD та ввів окрему главу про сприяння медіаграмотності. § 532 закону визначає медіаграмотність як «навички, знання та розуміння, що уможливлюють ефективне та безпечне використання медіа», а § 533 інституційно закріплює відповідальність за неї за Міністерством освіти і науки. У 2025 р. прийнято закон, що забороняє ретрансляцію російських пропагандистських каналів; у 2026 р. схвалено поправки до Закону про медіапослуги, що приводять естонське законодавство у відповідність до Регламенту ЄС про свободу медіа (EMFA)[201]. Принципово важливим є підхід до регулювання дезінформації: Естонія свідомо відмовилась від спеціального кодифікованого закону про дезінформацію, діючи через загальні норми (§ 262 Кримінального кодексу та § 55 Закону про правоохоронну діяльність), що захищає свободу слова, зберігаючи при цьому правовий механізм реагування на найбільш шкідливий контент.

У сфері кіберзахисту Естонія імплементує Директиву NIS2 з найбільшою системністю серед трьох держав, попри певні виклики, пов'язані з розширенням сфери охоплення на постачальників IT-послуг середнього розміру та хмарні компанії, суворіші строки повідомлення про інциденти (24–72 години) та посилений контроль за безпекою ланцюгів постачання[202]. Естонська CERT-EE

---

[198] Digital Agenda 2030 / Ministry of Economic Affairs and Communications of the Republic of Estonia. 2021. URL: https://mkm.ee/en/objectives-activities/digital-agenda-2030 (дата звернення: 01.04.2026).
[199] Internal Security Strategy 2020–2030 / Government of the Republic of Estonia. URL: https://www.siseministeerium.ee/sites/default/files/dokumendid/STAK/siseturvalisuse_arengukava_2020_2030_48lk_final_eng.pdf (дата звернення: 01.04.2026).
[200] Cohesive Estonia Development Plan 2021–2030 / Ministry of the Interior of the Republic of Estonia. URL: https://www.siseministeerium.ee/sidest (дата звернення: 01.04.2026).
[201] The Media Services Bill will reach the Riigikogu…
[202] NIS2 in the Baltics: How Lithuania, Latvia, and Estonia Differ…

(комп'ютерна група реагування на надзвичайні ситуації Естонії) є частиною загальноєвропейської мережі ENISA, що забезпечує швидке реагування на кіберінциденти в масштабах ЄС.

У сфері протидії дезінформації естонська модель вирізняється найбільш системним підходом до вимірювання ефективності заходів. Щорічне опитування Міністерства оборони Естонії засвідчило конкретні результати: частка неестонців, які регулярно переглядали російські телеканали, скоротилася з 62% навесні 2021 р. до 33% навесні 2022 р. і до 24% навесні 2023 р.; аудиторія російських новинних порталів відповідно знизилась із 51% до 32%[203]. Завдяки санкціям ЄС та ініціативі Агентства захисту прав споживачів (TTJA) заблоковано доступ до 389 телеканалів, вебсайтів та акаунтів у соціальних мережах, пов'язаних із Кремлем[204].

Річний огляд KAPO за 2024–2025 рр. фіксує важливу тенденцію: підтримка Кремля в Естонії, яка традиційно концентрується серед старшого покоління, поступово скорочується, що змушує Росію переорієнтовувати операції впливу на молодих російськомовних естонців[205]. Конкретним проявом цієї стратегії є активне залучення молоді до пропагандистських заходів у Росії: олімпіад, змагань, екскурсій, де справжня мета маскується нейтральними культурними або освітніми форматами. Реакцією Кремля на обмеження медіапростору стало системне перенесення пропагандистських операцій у соціальні мережі, зокрема до TikTok, із зростанням застосування deepfake-технологій та ШІ-генерованого контенту[206].

Особливим елементом естонської системи є волонтерська ініціатива «Propastop». Вона здійснює публічний моніторинг пропагандистських каналів і забезпечує зворотний зв'язок, якого бракує централізованим державним структурам[207]. «Propastop» принципово наголошує на обмеженості суто

[203] Propastop. Чи є якась користь від обмеження…
[204] Так само.
[205] Estonian Internal Security Service (KAPO). Annual Review…
[206] Так само.
[207] Propastop. Чи є якась користь від обмеження…

заборонних заходів: «кількість людей в Естонії, які поділяють цінності та погляди інформаційного простору Кремля, все ще велика»[208]. Цей висновок є структурним аргументом на користь поєднання обмежувальних заходів із позитивними стратегіями. Ключовим позитивним заходом є пріоритизація критичного мислення та медіаграмотності в естонській освітній системі: KAPO прямо наголошує, що «критичне мислення залишається єдиним надійним антидотом» проти зростаючих дезінформаційних загроз[209].

Зовнішній вимір естонської інформаційної стратегії реалізується через два взаємопов'язані канали. Перший - активна участь у формуванні нормативної бази НАТО та ЄС: Таллінський посібник, CCDCOE та внесок у формулювання DSA і EMFA позиціонують Естонію як регіонального та загальноальянсового лідера з питань кіберзахисту та протидії дезінформації. Другий - публічна дипломатія через відкриті щорічні доповіді KAPO та Служби зовнішньої розвідки, що публікуються англійською мовою і формують порядок денний для союзників[210]. Показово, що Естонія у 2025 р. вела переговори щодо угоди про захист класифікованої інформації з рядом нових партнерів, а в 2026 р. запровадила поправки до Закону про медіапослуги з огляду на EMFA[211,212].

Специфікою естонської позиції є уникання «надмірного представлення урядових голосів», що відповідає застереженню Чакарса та Екманіс щодо ризиків для медіаплюралізму[213]. Замість прямої пропаганди Естонія робить ставку на якість альтернативного контенту та прозорість медіасистеми. Це підхід, що відповідає стандартам EMFA та є значно стійкішим у довгостроковій перспективі. Ця стратегічна стриманість у поєднанні з технологічним лідерством є, мабуть, найбільш збалансованим з трьох балтійських підходів.

---

[208] Так само.
[209] Estonian Internal Security Service (KAPO). Annual Review…
[210] Так само.
[211] The Media Services Bill will reach the Riigikogu / Estonian Ministry of Culture. 06.02.2026. URL: https://ifacca.org/news/2026/02/06/media-services-bill-will-reach-riigikogu/ (дата звернення: 01.04.2026).
[212] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[213] Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії…

Латвійська модель інформаційної безпеки формується під визначальним впливом специфічного демографічного контексту: частка населення (близько 25–27%) є етнічними росіянами, ще більша переважно вживає російську мову у побуті. Ця демографічна реальність робить Латвію найбільш вразливою серед трьох балтійських держав до кремлівського медіавпливу. Чакарс та Екманіс зазначають, що ступінь залученості Латвії до питань російськомовної аудиторії є вищим, ніж в Естонії та Литві[214], а бюро SAB у своїй доповіді за 2025 р. прямо попереджає, що «наші противники, безумовно, хотіли б виконати значну частину роботи руками латвійців, без їхнього усвідомлення цього»[215].

Для розуміння специфіки латвійської стратегії принципово важливим є також поняття «острівців відчуження». В Латгалії, регіоні з найвищою часткою російськомовного населення, місцеві ради публічно чинили спротив виконанню закону 2022 р. про заборону прославлення тоталітарних режимів, що утворювало саме ті «острівці відчуження», придатні для використання Москвою[216]. SAB систематично відстежує і документує спроби Росії скористатися цими структурними вразливостями для розпалення міжетнічної напруги. Водночас, як констатує звіт SAB за 2025 р., «мовчазний вплив» є потенційно більш небезпечним, ніж відкрита пропаганда: він «поляризує суспільство і послаблює національну безпеку»[217], і саме тому Латвія обрала найбільш радикальний регуляторний шлях.

Латвійський підхід до регулювання медіапростору є найбільш жорстким серед трьох держав. Зміни до Закону про електронні медіа, що набули чинності 24 вересня 2022 р., суттєво розширили повноваження Національної ради з електронних медіа (NEPLP) та встановили нові вимоги щодо розкриття реальних бенефіціарів медіа[218]. Закон запровадив пряму заборону видавати ліцензії на мовлення телепрограмам, виключеним із латвійського переліку ретрансляції,

---

[214] Так само.
[215] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[216] Оксентюк А., Радь П., Клімов Р. та ін. Регіональний аспект союзу РФ і Білорусі: наслідки для сусідів / за ред. Я. Чорногора. Київ : Рада зовнішньої політики «*Українська призма*», 2025.
[217] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[218] Andersone I. New amendments to the Latvian Electronic Mass Media Law enter into force. *IRIS*.

якщо країна їхньої юрисдикції «загрожує територіальній цілісності, суверенітету або національній незалежності іншої держави»[219]. Реальним наслідком стало блокування у червні 2022 р. 80 російських телеканалів.

Окремо важливою є мовна норма: при поширенні програм з мовним треком, що не є офіційною мовою країни ЄС, кабельні оператори зобов'язані забезпечити основний мовний трек латвійською мовою[220]. Цей захід не забороняє контент, але ефективно усуває мовний привілей, який де-факто перетворював латвійський кабельний ефір на канал поширення кремлівських наративів. NEPLP також отримала право виключати медіа зі списку ретрансляції за ненадання або фальсифікацію відомостей про реальних бенефіціарів - захід, що безпосередньо атакує механізми прихованого кремлівського фінансування медіа[221].

Паралельно з обмежувальними заходами розгорталося будівництво позитивної медіаальтернативи. З 2025 р. в Латвії розпочало роботу об'єднане Латвійське громадське медіа (LSM), що поєднало суспільне радіо і телебачення під управлінням Ради з громадських електронних медіа (SEPLP). Метою реструктуризації є підвищення якості контенту для різних мовних груп, зокрема для російськомовної аудиторії, та посилення спроможності протидіяти дезінформації альтернативними якісними продуктами. Критичне застереження дослідників Чакарса та Екманіс щодо ризику «надмірного представлення урядових голосів»[222] є особливо доречним саме стосовно Латвії: в умовах демографічного напруження надмірна державна домінантність у медіапросторі може підштовхнути частину аудиторії до альтернативних джерел.

Бюро захисту Конституції Латвії (SAB) відіграє унікальну роль у балтійському контексті: воно поєднує функції розвідувального органу з активною публічною комунікацією в інтересах суспільної стійкості. Щорічні доповіді SAB, що публікуються латвійською та англійською мовами, є не лише

---

[219] Так само.
[220] Andersone I. New amendments to the Latvian Electronic Mass Media Law enter into force. *IRIS*.
[221] Так само.
[222] Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії…

звітними документами, а й інструментами формування суспільної обізнаності та зовнішньої публічної дипломатії. У Передмові до доповіді за 2025 р. директор SAB Еґілс Звієдріс прямо звертається до громадян: «Я закликаю всіх, споживаючи інформацію, усвідомлювати, що ми перебуваємо під тиском діяльності з інформаційного впливу»[223]. Такий персоналізований заклик через офіційний документ є нетиповим для традиційних спецслужб і відображає глибоке переосмислення ролі розвідки в демократичному суспільстві.

У сфері кіберзахисту SAB зафіксував рекордний рівень кіберзагроз у 2025 р.[224]. Принципово важливим є задокументований зв'язок між DDoS-атаками та конкретними політичними подіями - наприклад, масштабна атака у липні 2025 р. після оголошення латвійської компанії переможцем міжнародного тендеру на безпілотники[225]. Цей зв'язок свідчить про те, що кібератаки є елементом цілеспрямованої кампанії покарання та стримування, а не хаотичними злочинними актами. SAB також задокументував загрозу кіберінцидентів в операційних технологіях на прикладах поза Латвією, зокрема атаки на норвезьку дамбу та Гданську гідроелектростанцію у 2025 р., як попереджувальні кейси для латвійської критичної інфраструктури[226].

Окремим виміром діяльності SAB є моніторинг «правового гібридного інструментарію». Доповідь за 2025 р. документує, що Росія готує позов проти Латвії до Міжнародного суду ООН на підставі нібито порушення ICERD, і вважає цей процес практично завершеним, з очікуваним поданням у 2026 р.. SAB характеризує цей крок як спробу «дискредитувати Латвію на міжнародному рівні та забезпечити довгостроковий міжнародний тиск»[227] і як нову форму гібридної агресії, що вимагає нових форм публічно-дипломатичного реагування.

Зовнішня роль Латвії в архітектурі балтійської та загальноальянсової інформаційної безпеки концентрується навколо Центру передового досвіду

---

[223] Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report…
[224] Так само.
[225] Так само.
[226] Так само.
[227] Так само.

НАТО зі стратегічних комунікацій (StratCom COE), що діє у Ризі з 2014 р.. Цей центр є провідним дослідницьким осередком Альянсу з питань інформаційних операцій та протидії дезінформації і надає аналітичну підтримку як урядам країн-членів, так і командуванню НАТО. Розміщення StratCom COE саме в Латвії є не випадковим: латвійська стратегічна логіка здобуття інституційного лідерства у сфері, де країна стикається з найгострішими практичними викликами, нагадує естонську щодо CCDCOE (Об'єднаний центр передових технологій з кібероборони НАТО). Обидва центри перетворюють специфічну регіональну вразливість на загальноальянсову компетентність.

Литовська стратегія інформаційної безпеки є найбільш комплексно інтегрованою в загальну систему державної оборони серед трьох балтійських держав. Це зумовлено насамперед геополітичним становищем: Литва має спільні кордони з Білоруссю та Калінінградською областю Росії, а так звана «Сувальська щілина», 100-кілометрова смуга польсько-литовського кордону між Калінінградом і Білоруссю, є стратегічно критичним вузлом, захоплення якого відрізало б балтійські країни від решти НАТО. Цей географічний чинник надає особливого значення інформаційним операціям, спрямованим на підрив суспільної підтримки членства в НАТО та союзницьких зобов'язань. Ослаблення суспільної рішучості безпосередньо збільшує стратегічну вразливість країни[228].

Демографічно Литва є найменш вразливою з трьох держав: частка росіян становить лише близько 5–6% населення, а Литва ще у 1991 р. надала громадянство всім постійним жителям без мовного чи етнічного критерію, що суттєво зменшило потенціал для маніпуляцій щодо «дискримінації»[229]. Водночас спільний кордон з Білоруссю є додатковим каналом для операцій впливу: «Національна оцінка загроз 2026», підготовлена литовськими розвідувальними

[228] Москалюк М. Ф. Безпекова політика країн Балтії в умовах російсько-української війни. *Регіональні студії*. 2024. № 37. С. 59–63.
[229] Петрик А. М. «Північний фронт»: Російська пропаганда…

органами AOTD та VSD, документує систематичне використання Білорусі як плацдарму для гібридних операцій проти Литви та інших балтійських держав[230].

Ключовою особливістю литовської моделі є концепція «тотальної оборони», що передбачає залучення всіх ресурсів суспільства, включно з інформаційною стійкістю, до системи національної безпеки. Практичним виразом цього підходу є запровадження обов'язкового курсу громадянської освіти та навичок оборони для учнів 9 класів з 2022 р. - це спільний проєкт Міністерства національної оборони, Міністерства освіти та Союзу стрільців Литви, що передбачав 100-відсоткове охоплення учнів 9 класів вже у 2024–2025 навчальному році[231]. Цей захід є безпосередньою інституціоналізацією стійкості суспільства до інформаційних маніпуляцій як освітнього стандарту.

«Національна оцінка загроз 2026» формулює цей принцип доступно: «до стримування Росії від безрозсудної військової агресії проти нас або інших держав НАТО ми маємо продовжувати розвивати наші оборонні спроможності. Кожен громадянин Литви робить свій внесок у збільшення нашого оборонного потенціалу, розвиваючи здатність виявляти загрози та запобігати їм»[232]. Наголос на «кожному громадянині» є принципово важливим: він відображає не просто риторику, а реальну модель «тотальної оборони», де інформаційна грамотність є таким само складником обороноздатності, як і стрілецька підготовка.

Кількісним підтвердженням загрози є дані з попередніх оцінок: у 2023 р. литовські оборонні відомства виявили понад 3,5 тис. випадків ворожої інформаційної діяльності[233]. Серед домінуючих наративів - звинувачення Литви й НАТО у провокуванні Росії та Білорусі, дискредитація військового потенціалу Альянсу, підрив підтримки України. Ці наративи є не спонтанними, а системними: «Національна оцінка загроз 2026» документує, що вони

[230] Defence Intelligence and Security Service (AOTD); State Security Department (VSD). National Threat Assessment 2026…
[231] Каракуць О. Основні тенденції зовнішньої політики і національної безпеки Литви. Київ: *НІСД*, 2024.
[232] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…
[233] Каракуць О. Основні тенденції зовнішньої політики…

формуються на рівні Адміністрації Президента Росії і поширюються через МЗС, псевдонаукові академічні структури та лояльних литовських громадян[234].

Литовська розвідка задокументувала низку специфічних механізмів проросійської пропаганди, що відрізняються від латвійського та естонського досвіду. Ключовим є використання литовських громадян, а саме прихильників російського режиму, для реалізації ворожої інформаційної політики зсередини[235]. Ці особи, часто переховуючись у Білорусі або Росії від литовського правосуддя, активно співпрацюють із білоруськими та російськими пропагандистськими структурами, виступаючи в інтерв'ю та антилитовських кампаніях. Тенденція до втечі проросійських активістів до Білорусі або Росії спостерігається у всіх балтійських державах[236], але в литовському контексті вона особливо задокументована через ідентифікацію конкретних осіб.

Іншим специфічним каналом є Московський Патріархат. «Національна оцінка загроз 2026» фіксує, що Московський Патріархат здійснює значний вплив через Православну єпархію Вільнюса і Литви, використовуючи її для поширення ідеї «Руського світу»[237]. Попри офіційні декларації єпархії про прагнення до часткової самоврядності, реального вирішення залежності від Москви не відбулося, що зберігає канал потенційного ідеологічного впливу. Важливою особливістю є також задокументоване використання ТікТок для поширення наративів серед молоді: «Росія адаптується до змін у споживанні інформації та активно використовує TikTok для поширення своїх наративів ширшій аудиторії» у форматі розважальних відео та мемів[238].

Третім специфічним механізмом є псевдонаукові академічні структури: Балтійський федеральний університет імені Іммануїла Канта, Фонд підтримки і захисту прав співвітчизників за кордоном (заснований МЗС Росії) та Фонд «Historical Memory». Ці організації проводять конференції та виставки, де

[234] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…
[235] Так само.
[236] Так само.
[237] Так само.
[238] Так само.

проросійські активісти з Литви презентуються як «незалежні експерти», а сфабриковані звинувачення у «русофобії» - як науково обґрунтовані висновки. Реакцією Литви на ці виклики є поєднання законодавчого блокування (LRTK активно блокує незліцензовані сайти, що ретранслюють пропаганду) із судовим переслідуванням проросійських активістів у межах литовського законодавства.

Литва є батьківщиною однієї з найвідоміших у Євросоюзі платформ протидії дезінформації, а саме DebunkEU.org. За аналізом Чакарса та Екманіс, ця ініціатива «поєднала можливості штучного інтелекту та громадянську активність»: алгоритм аналізував контент у соціальних мережах і сигналізував волонтерам, так званим «ельфам», про появу нових дезінформаційних наративів[239]. Ця модель - поєднання ШІ-інструментів із низовою громадянською активністю - стала зразком для інших держав і відображає більш широку тенденцію переходу від суто державного до суспільно-державного реагування на дезінформацію. Принциповою перевагою такого підходу є незалежність волонтерів від урядових інтересів, що підвищує довіру аудиторії до спростувань[240].

«Ельфи» є продовженням глибокої культурної традиції: Чакарс та Екманіс прослідковують від зародження балтійської преси у XIX ст. феномен активних громадян, що бачать свій обов'язок у протидії ворожій пропаганді через формування якісного інформаційного простору. Ця укоріненість медіаактивізму в балтійській традиції пояснює, чому громадянські ініціативи з протидії дезінформації є значно більш розвиненими та сталими в балтійських країнах, ніж у більшості інших держав ЄС. «Національна оцінка загроз 2026» неодноразово апелює до самоорганізації суспільства як необхідного елемента системи захисту[241].

Зовнішня складова литовської інформаційної стратегії є найбільш орієнтованою на формат «Схід-Захід». Литва активно просуває співпрацю з

[239] Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії…
[240] Так само.
[241] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…

Україною, зокрема через формат «Люблінського трикутника» (Польща, Україна, Литва), як стратегічний механізм поширення досвіду протидії дезінформації та взаємного зміцнення інформаційного захисту. Рада зовнішньої політики «Українська призма» рекомендує «розробку спільного підходу у питанні відриву Білорусі від РФ», що в інформаційному вимірі передбачає формування альтернативних інформаційних каналів для білоруського суспільства[242].

«Національна оцінка загроз 2026» прямо наголошує, що саме «послідовний діалог та тісніша співпраця» є антидотом проти спроб Росії «розколоти єдність НАТО методом «розділяй і пануй»»[243]. Це концептуальне положення відображає литовське бачення інформаційної безпеки як системно пов'язаної з колективною безпекою Альянсу: ослаблення будь-якого союзника в інформаційному просторі є ослабленням всього НАТО.

3.2. Спільні елементи та відмінності в інформаційних стратегіях

Системне зіставлення трьох балтійських моделей спирається на концептуальний поділ «твердої» і «м'якої» безпеки: Яковюк та Шестопал констатують, що «питання вищого рівня є однаковими для всіх трьох держав», тоді як у сфері «м'якої» безпеки кожна держава може мати власні пріоритети[244]. Спільними є загальна нормативна база ЄС/НАТО, стратегічне завдання протидії Кремлю та загальна архітектура чотирьох рівнів (державний регулятор - спецслужби - суспільне мовлення - громадянське суспільство); відмінними є конкретні пріоритети, акценти та технологічні рішення.

Першим спільним елементом є чотирирівнева інституційна архітектура: (1) незалежний державний регулятор медіапростору (TTJA/EAK в Естонії, NEPLP в Латвії, LRTK в Литві); (2) спецслужбовий моніторинг і публічне документування загроз (KAPO, SAB, VSD/AOTD); (3) суспільний мовник як виробник якісного альтернативного контенту (ERR, LSM/LTV, LRT); (4) громадянські ініціативи і медіаграмотність як «рівень стійкості». Ця структура

[242] Оксентюк А., Радь П., Клімов Р. та ін. Регіональний аспект…
[243] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…
[244] Яковюк І. В., Шестопал С. С. Правове регулювання політики…

органічно відображає «комплексну модель», де «зовнішня, оборонна та безпекова політика, а також забезпечення єдності та стійкості суспільства були визнані запорукою» досягнення цілей [245].

Другим спільним елементом є орієнтація на НАТО як основний безпековий гарант та інституційна прив'язка ключових центрів компетентності до Альянсу: CCDCOE (Таллінн) та StratCom COE (Рига). Яковюк та Шестопал відзначали, що «країни Балтії не бачать в ЄС надійного гаранта своєї безпеки і оборони»[246]; стратегічне значення зберігає НАТО. Третім спільним елементом є реакція на загрозу ШІ: всі три країни через SAB[247], KAPO[248] та VSD/AOTD[249] фіксують зростання застосування Росією ШІ-генерованого контенту. Четвертим спільним елементом є поєднання обмежувальних і позитивних заходів: жодна з трьох держав не обмежилась лише блокуванням, кожна паралельно розвивала публічний медіаконтент, освітні програми та механізми підтримки громадянської активності[250]. П'ятим спільним елементом є активна участь у формуванні загальноєвропейської нормативної бази: DSA, EMFA, NIS2, GDPR.

Перша і найбільш принципова відмінність стосується жорсткості регуляторного підходу. Латвія обрала найбільш радикальний шлях: масове блокування 80 телеканалів, мовні вимоги для кабельних операторів, широке розкриття медіабенефіціарів[251]. Естонія обрала найбільш виважений підхід: відмова від спеціального антидезінформаційного закону, дія через загальне законодавство, широка система медіаграмотності. Литва займає проміжну позицію: активне блокування через LRTK, але основна ставка - на суспільну стійкість через освітні заходи та громадянські ініціативи[252,253]. Ця відмінність у

[245] Так само.
[246] Так само.
[247] Constitution Protection Bureau of the Republic of Latvia (SAB)…
[248] Estonian Internal Security Service (KAPO). Annual Review…
[249] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…
[250] Propastop. Чи є якась користь від обмеження кремлівських каналів?..
[251] Andersone I. New amendments to the Latvian Electronic Mass Media Law enter into force. IRIS. 2022. 2022-9:1/9. URL: https://merlin.obs.coe.int/iris/2022/9/article9.en.html (дата звернення: 01.04.2026).
[252] Каракуць О. Основні тенденції зовнішньої…
[253] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…

жорсткості безпосередньо відображає різницю у демографічній вразливості: найвразливіша Латвія обирає найжорсткіший підхід.

Друга відмінність - пріоритетність технологічного лідерства. Естонія є незаперечним лідером: CCDCOE, e-ID, е-урядування, Таллінський посібник. Латвія зосереджує лідерство у стратегічних комунікаціях через StratCom COE [8]. Литва є найменш технологічно орієнтованою назовні, натомість найбільш зосередженою на суспільно-освітніх заходах [254,255]. Цей розподіл є функціонально оптимальним: три країни охоплюють три різних виміри інформаційної безпеки, не дублюючи, а доповнюючи одна одну.

Третя відмінність - роль громадянського суспільства. Литва є лідером: DebunkEU та мережа «ельфів»[256]. Естонія поєднує державні та громадянські зусилля через «Propastop»[257]. Латвія є найбільш державно-центричною: SAB і NEPLP відіграють домінуючу роль. Четверта відмінність - ступінь інтеграції інформаційної безпеки в систему тотальної оборони. Литва є безперечним лідером: обов'язковий курс для учнів 9 класів і концепція «кожен громадянин як захисник»[258,259]. В умовах геополітичної вразливості через Сувальський коридор суспільна стійкість є буквально питанням виживання держави[260].

Оцінка ефективності трьох моделей є методологічно складним завданням через відсутність єдиних метрик і багатофакторність процесів. Найбільш конкретні дані наявні щодо Естонії: скорочення аудиторії російських медіа серед неестонців з 62% до 24% між 2021 і 2023 рр.[261]. Оцінки загроз усіх трьох спецслужб свідчать про підтримання «стійкого рівня» загрози, а не її ескалацію, що може вказувати на відносну ефективність вжитих заходів. Системним обмеженням залишається фундаментальна медіаасиметрія: «російська медіа-

[254] Каракуць О. Основні тенденції зовнішньої…
[255] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…
[256] Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії: Довга тінь Росії / пер. І. Ємельянової. Бостон : Academic Studies Press, 2025. 306 с.
[257] Propastop. Чи є якась користь від обмеження кремлівських каналів?..
[258] Каракуць О. Основні тенденції зовнішньої…
[259] Defence Intelligence and Security Service (AOTD); State Security Department (VSD)…
[260] Москалюк М. Ф. Безпекова політика країн Балтії в умовах російсько-української війни. Регіональні студії. 2024. № 37. С. 59–63.
[261] Propastop. Чи є якась користь від обмеження кремлівських каналів?..

індустрія в рази більша, ніж в країнах Балтії разом узятих»[262]. Подолання цього обмеження потребує вдосконалення суспільно-державного партнерства, координації в НАТО та ЄС і розширення співпраці з Україною [4; 5].

Щодо перспектив конвергенції: EMFA, що набрав чинності 8 серпня 2025 р. [10], є найбільш потужним поштовхом до зближення регуляторних підходів, встановлюючи єдиний стандарт медіаплюралізму, прозорості власності та захисту журналістів. Розвиток ШІ-інструментів для виявлення дезінформації є потенційним вектором технологічної конвергенції: спільні платформи аналізу можуть подолати нинішню фрагментованість інструментарію.

Підсумовуючи, можна виокремити три ключових висновки. По-перше, усі три держави функціонують у рамках спільної архітектурної логіки: чотирирівнева інституційна система та спільна нормативна база ЄС/НАТО є продуктом спільних загроз і євроатлантичної орієнтації. По-друге, всередині спільної рамки кожна держава виробила власну характерну конфігурацію: Естонія є цифровим лідером з найбільш системним підходом до вимірювання ефективності; Латвія - найбільш радикальним регулятором, що компенсує демографічну вразливість жорсткістю заходів; Литва - найбільш комплексно інтегрованою моделлю тотальної оборони. По-третє, три моделі є не конкурентними, а взаємодоповнюючими: Естонія охоплює технологічний вимір (CCDCOE), Латвія - стратегічні комунікації (StratCom COE), Литва - суспільну стійкість та низовий активізм (DebunkEU). Така функціональна спеціалізація є оптимальним використанням ресурсів малих держав і прикладом «розподілу праці» у загальноальянсовій системі протидії дезінформації.

[262] Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії…

ВИСНОВКИ

У результаті проведеної комплексної роботи на тему дослідження особливостей інформаційної політики країн Балтії в умовах російсько-української війни (2022-2026 рр.) дозволяє зробити низку ґрунтовних висновків, що відображають трансформацію систем національної безпеки Естонії, Латвії, Литви у відповідь на глобальні гібридні виклики.

Можна стверджувати, що повномасштабна агресія Російської Федерації проти України стала каталізатором остаточної зміни парадигми інформаційної безпеки в Балтійському регіоні. Протягом 2022-2026 років відбувся перехід від вузькотехнічного розуміння кіберзахисту до концепції «когнітивної стійкості» суспільства. Це означає, що об’єктом захисту стала не лише критична інфраструктура чи мережі, а свідомість громадян, їхня здатність розрізняти маніпулятивні наративи та зберігати психологічну стабільність в умовах інформаційного тиску. Інформаційна безпека офіційно визнана фундаментом національної витривалості.

Законодавча база Естонії, Латвії та Литви зазнала найбільш радикальних змін за останні три десятиліття. Уряди цих держав успішно імплементували механізми, які дозволяють балансувати між демократичними цінностями свободи слова та необхідністю захисту національного суверенітету. Зокрема, було впроваджено ліцензування медіаресурсів, які прямо чи опосередковано підтримують агресивні дії третіх країн або поширюють мову ворожнечі або наративи. Такий превентивний підхід дозволив мінімізувати вплив зовнішніх деструктивних факторів на внутрішні політичні процеси.

Було сформовано унікальну систему взаємодії «держава - суспільство - приватний сектор». У країнах Балтії було закріплено роль неурядових організацій та волонтерських рухів (як-от спільноти «кібер-ельфів») як офіційних партнерів у сфері стратегічних комунікацій. Така децентралізована модель захисту виявилася значно ефективнішою за традиційні вертикальні структури, оскільки вона дозволяє виявити та нейтралізувати дезінформаційні

атаки на рівні громад ще до того, як вони набудуть загальнонаціонального масштабу.

Було з'ясовано, що політика жорсткого обмеження російського медіа-контенту у досліджуваний період була не лише виправданою, а й критично необхідною. Вилучення пропагандистських каналів із кабельних мереж та блокування відповідних інтернет-порталів створило «санітарний кордон» навколо інформаційного простору регіону. Досвід останніх років спростував теорію про те, що такі заборони лише посилюють інтерес до забороненого контенту: навпаки, було зафіксовано поступову міграцію аудиторії до національних та європейських джерел інформації, що сприяло деокупації свідомості значної частини населення.

Також, можна зазначити, що медіаграмотність у балтійських країнах трансформувалася з освітнього курсу на стратегічний актив держави. Запровадження комплексних програм навчання для різних вікових груп від дітей до людей похилого віку - сформувало колективний імунітет проти маніпуляцій. Особливий акцент було зроблено на критичному споживанні контенту в соціальних мережах, що дозволило зменшити вразливість суспільства перед алгоритмами штучного інтелекту та вірусними фейками, які розповсюджуються через месенджери.

Порівняльний аналіз стратегій трьох держав дозволив виділити їхні ключові спеціалізації. Естонія продемонструвала світове лідерство у впровадженні цифрових інструментів моніторингу та автоматизованого виявлення бот-мереж. Латвія зосередилася на посиленні правового контролю та захисті державного мовного середовища. Литва ж стала головним хабом стратегічних комунікацій у Східній Європі, активно просуваючи ініціативи щодо санкційного тиску на агресора та координуючи спільні заходи безпеки на рівні НАТО. Разом ці підходи утворюють цілісну регіональну систему безпеки. Балтійський досвід став основою для оновлення стратегічних концепцій НАТО, де інформаційному виміру конфліктів тепер приділяється не менше уваги, ніж військовому.

Було встановлено, що у період 2025-2026 років новим критичним викликом стало використання штучного інтелекту та технологій дипфейків у дезінформаційних кампаніях. Країни Балтії оперативно адаптували свої стратегії, впроваджуючи алгоритми верифікації контенту та створюючи системи швидкого реагування. Це дозволило нейтралізувати спроби дестабілізації під час виборчих процесів та військових навчань, доводячи, що технологічна перевага є невід'ємною частиною сучасної інформаційної політики.

Підсумовуючи, можна стверджувати, що інформаційна політика країн Балтії у 2022-2026 роках є взірцем проактивного захисту демократичного суспільства. Незважаючи на постійне вдосконалення методів агресора, Естонія, Латвія та Литва змогли створити стійку систему, яка не лише відбиває атаки, а й формує власний безпековий порядок денний у світі. Подальший розвиток цієї сфери вимагатиме ще тіснішої міжнародної інтеграції та постійної адаптації до нових технологічних реалій, проте фундамент, закладений у ці роки, є надійним гарантом збереження їхнього інформаційного суверенітету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Бусол О. Ю. Феномен гібридних загроз національній безпеці. *Юридична Україна*. 2020. № 4. С. 5–11. DOI: https://doi.org/10.37749/2308-9636-2020-4(208)-1.

2. Гбур З. В. Актуальні гібридних загрози економічній безпеці України. *Інвестиції: практика та досвід*. 2018. № 7. С. 100.

3. Геращенко А. М., Поліщук І. М. Інформаційна безпека в умовах гібридної війни: виклики та стратегії протидії. *Юридичний науковий електронний журнал*. 2023. № 5. С. 343–346.

4. Гібридні загрози України і суспільна безпека. Досвід ЄС і східного партнерства. Аналітичний документ центру глобалістики «Стратегія XXI». 2018. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf (дата звернення: 01.04.2026).

5. Гоґвуд Б., Ґан Л. Аналіз політики для реального світу / пер. з англ. А. Олійник ; наук. ред. пер. В. Тертичка. Київ : Вид-во Соломії Павличко «Основи», 2004. 396 с.

6. Горбулін В. П., Качинський А. Б. Засади національної безпеки України : підручник. Київ : Інтертехнологія, 2009. 272 с.

7. Демченко В. С. Інформаційна війна як складова гібридної агресії Російської Федерації. *Вісник Прикарпатського університету. Серія : Політологія*. 2023. Вип. 15. С. 27–32.

8. Директива 95/46/ЄС Європейського Парламенту та Ради про захист осіб стосовно обробки персональних даних та про вільне переміщення таких даних від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 01.04.2026).

9. Естонія. Кримінальний кодекс : Закон Естонської Республіки від 06 черв. 2001 р. (зі змінами та допов.). URL: https://www.riigiteataja.ee/akt/123052024017 (дата звернення: 15.05.2026).

10. Естонія. Про медіапослуги (Meediateenuste seadus) : Закон Естонської Республіки від 14 черв. 2022 р. URL: https://www.riigiteataja.ee/en/eli/514062022001/consolide (дата звернення: 01.04.2026).

11. Естонія. Про правоохоронну діяльність (Korrakaitseseadus) : Закон Естонської Республіки від 23 лют. 2011 р. URL: https://www.riigiteataja.ee/akt/123022011 (дата звернення: 15.05.2026).

12. Каракуць О. Основні тенденції зовнішньої політики і національної безпеки Литви. Київ : НІСД, 2024.

13. Клаузевіц К. Про війну / пер. з англ. Дж. Дж. Грехем ; ред. та прим. Ф. Н. Мод. Лондон : Kegan Paul, Trench, Trübner & Co., 1909. URL: https://icct.nl/sites/default/files/import/publication/On-War.pdf (дата звернення: 01.04.2026).

14. Конах В. К., Лазоренко О. А. Загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації. *Стратегічні пріоритети*. 2014. № 2 (31). С. 73–78.

15. Король А. Інформаційні технології в системі міжнародних відносин: проблема впровадження. *Мультиверсум. Філософський альманах*. 2015. Вип. 3–4 (141–142). С. 60–66.

16. Москалюк М. Ф. Безпекова політика країн Балтії в умовах російсько-української війни. *Регіональні студії*. 2024. № 37. С. 59–63.

17. Оксентюк А., Радь П., Клімов Р. та ін. Регіональний аспект союзу РФ і Білорусі: наслідки для сусідів / за ред. Я. Чорногора. Київ : Рада зовнішньої політики «Українська призма», 2025.

18. Петрик А. М. «Північний фронт»: Російська пропаганда проти держав Балтії. Клайпедський університет, 2023. URL: https://www.istpravda.com.ua/articles/2023/10/20/163257/ (дата звернення: 01.04.2026).

19. Пилипчук В., Дзьобань О. Глобальні виклики та загрози національній безпеці в інформаційній сфері. *Вісник Національної академії правових наук України*. 2014. № 3 (78). С. 43–52.

20. Почепцов Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2015. 496 с.

21. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних даних (GDPR) від 27.04.2016. URL: https://gdpr-info.eu/ (дата звернення: 01.04.2026).

22. Резолюція Європейського Парламенту про стратегічні комунікації ЄС для протидії пропаганді третіх сторін від 23.11.2016 (2016/2030 (INI)). URL: https://www.eeas.europa.eu/node/16198_en (дата звернення: 01.04.2026).

23. Руснак І. С. Воєнна безпека України у світлі реформування сектора безпеки і оборони. *Наука і оборона*. 2015. № 2. С. 9–14.

24. Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії: Довга тінь Росії / пер. І. Ємельянової. Бостон : Academic Studies Press, 2025. 306 с.

25. Яковюк І. В., Шестопал С. С. Правове регулювання політики національної безпеки країн Балтії в контексті еволюції стратегічних концепцій НАТО. *Проблеми законності*. 2018. Вип. 143. С. 218–227. DOI: 10.21564/2414-990x.143.148488.

26. 2022 Strengthened Code of Practice on Disinformation : Policy and Legislation. Publication 16 June 2022. URL: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (дата звернення: 01.04.2026).

27. Aaronson M. et al. NATO Countering the Hybrid Threat. *PRISM*. 2011. Vol. 2, No. 4. P. 112–124.

28. Andersone I. New amendments to the Latvian Electronic Mass Media Law enter into force. *IRIS*. 2022. 2022-9:1/9. URL: https://merlin.obs.coe.int/iris/2022/9/article9.en.html (дата звернення: 01.04.2026).

29. Andersson J., Tardy T. Hybrid: What's in a name? European Union Institute for Security Studies. 2015. October. P. 3–4.

30. Bachmann S. D., Gunneriusson H. Hybrid wars: The 21st-century's new threats to global peace and security. *Scientia Militaria: South African Journal of Military Studies*. 2015. Vol. 43. P. 77–98.

31. Bachmann S. D., Gunneriusson H. Terrorism and cyber attacks as hybrid threats: Defining a comprehensive approach for countering 21st century threats to global risk and security. *The Journal on Terrorism and Security Analysis*. 2013. Vol. 9. P. 27–36.

32. Burduli I. Russian Soft Power in the Baltics: Testing NATO Vulnerabilities. *Per Concordiam*. 2019. Vol. 10, No. 2. P. 19–23.

33. Center for Security Studies. Estonia’s National Cybersecurity and Cyberdefense Posture. *Cyber Reports*. 2020.

34. CERT-LV. Latvian cybersecurity and CERT.LV technical activities: Annual report 2023. Information Technology Security Incident Response Institution of the Republic of Latvia. 2023.

35. Churanova O., Romaniuk V. Anti-EU narratives through the Russian-Ukrainian war in the light of StopFake.org's debunks. *Disinformation and fact-checking in contemporary society*. Madrid : Dykinson, 2023. P. 39–61.

36. Cohesive Estonia Development Plan 2021–2030 / Ministry of the Interior of the Republic of Estonia. URL: https://www.siseministeerium.ee/sidest (дата звернення: 01.04.2026).

37. Constitution Protection Bureau of the Republic of Latvia (SAB). Annual Report 2025. Riga : SAB, 2026. 35 p. URL: https://www.sab.gov.lv (дата звернення: 01.04.2026).

38. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Brussels : European Parliament, 2014. 86 p. URL: https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf (дата звернення: 01.04.2026).

39. Defence Intelligence and Security Service (AOTD) ; State Security Department (VSD). National Threat Assessment 2026. Vilnius, 2026. 90 p.

40. Digital Agenda 2030 / Ministry of Economic Affairs and Communications of the Republic of Estonia. 2021. URL: https://mkm.ee/en/objectives-activities/digital-agenda-2030 (дата звернення: 01.04.2026).

41. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022.

42. Estonian Internal Security Service (KAPO). Annual Review 2024–2025. Tallinn : KAPO, 2025.

43. Estonian National Defence Development Plan 2031 / Ministry of Defence of the Republic of Estonia. URL: https://www.kaitseministeerium.ee (дата звернення: 01.04.2026).

44. Gaub F. Hybrid tactics: ISIL & Co. European Union Institute for Security Studies. Issue Alert 47. Paris, 2015. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_47_hybrid_ISIL.pdf (дата звернення: 01.04.2026).

45. Global Cybersecurity Index (GCI) 2024 / International Telecommunication Union. 2024. URL: https://www.itu.int/pub/D-HDB-GCI.01-2024 (дата звернення: 01.04.2026).

46. Hoffman F. Hybrid Warfare and Challenges. *The Routledge Handbook of Civil-Military Relations*. 2012. DOI: 10.4324/9781315814803-35.

47. Horbyk R., Dutsyk D., Shalaiskyi S. Effectiveness of Russian disinformation counteraction in Ukraine in a full-scale war : analytical report / Ukrainian Media and Communication Institute NGO. 2023. 66 p.

48. Internal Security Strategy 2020–2030 / Government of the Republic of Estonia. URL: https://www.siseministeerium.ee/sites/default/files/dokumendid/STAK/siseturvalisuse_arengukava_2020_2030_48lk_final_eng.pdf (дата звернення: 01.04.2026).

49. Klein J. I., Rice C., Levy J. C. U.S. Education Reform and National Security. Independent Task Force Report 68. New York: Council on Foreign Relations Press, 2012. 120 p.

50. Latvian Cybersecurity Strategy 2023–2026: Cabinet Regulation No. 158 / Latvian Cabinet of Ministers. 2023.

51. Lerche Ch., Said A. *Politics Concepts of International in Global Perspective*. Englewood Cliffs: Prentice-Hall, 1979. 178 p.

52. Miklaucic M. NATO countering the hybrid threat. North Atlantic Treaty Organization. URL: https://apps.dtic.mil/sti/tr/pdf/AD1042838.pdf (дата звернення: 01.04.2026).

53. National Cyber Security Strategy 2022 / Ministry of National Defence of the Republic of Lithuania. 2022.

54. National Defence Strategy Estonia. URL: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf (дата звернення: 01.04.2026).

55. Nikers O., Tabuns O. Bureaucratic policy and defense cooperation among the Baltic states. *Security and Defence Quarterly*. 2022. Vol. 37, No. 1. P. 41–54. DOI: https://doi.org/10.35467/sdq/145571.

56. Niruthan N. How Hybrid Warfare Could Change Asia. 2016. June 25. URL: https://thediplomat.com/2016/06/how-hybrid-warfare-could-change-asia/ (дата звернення: 01.04.2026).

57. NIS2 in the Baltics: How Lithuania, Latvia, and Estonia Differ/Baltic Amadeus. 23.09.2025. URL: https://www.balticamadeus.lt (дата звернення: 01.04.2026).

58. Pikner I. Military concepts and hybrid war. *Forum Scientiae Oeconomia*. 2016. Vol. 4. Special Issue No. 1.

59. Propastop. Чи є якась користь від обмеження кремлівських каналів? 27.11.2023. URL: https://www.propastop.org (дата звернення: 01.04.2026).

60. Reichborn-Kjennerud E., Cullen P. What is Hybrid Warfare? *Norwegian Institute of International Affairs (NUPI) Policy Brief*. 2016. No. 1. URL: http://hdl.handle.net/11250/2380867 (дата звернення: 01.04.2026).

61. Report on state defence policy and armed forces development. Rīga : Ministry of Defence of the Republic of Latvia. URL: http://stratobs.eu/docs/data/documents/files/136.pdf (дата звернення: 01.04.2026).

62. Roberts Al. S. Entangling Alliances: Nato's security of information policy and the entrenchment of State Secrecy. *Cornell International Law Journal*. 2002.

Vol. 26 (2). URL: https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1536&context=cilj (дата звернення: 01.04.2026).

63. The Media Services Bill will reach the Riigikogu / Estonian Ministry of Culture. 06.02.2026. URL: https://ifacca.org/news/2026/02/06/media-services-bill-will-reach-riigikogu/ (дата звернення: 01.04.2026).

64. Vasilevska S., Vasilevskis E., Vitolina Z. Cybersecurity policy analysis and research cooperation in the Baltic States. *Research for Rural Development*. 2025. Vol. 40. P. 326–332. DOI: 10.22616/RRD.31.2025.043.

65. Wardle C., Derakshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and policy Making/Council of Europe. 2017. URL: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (дата звернення: 01.04.2026).

ДОДАТКИ

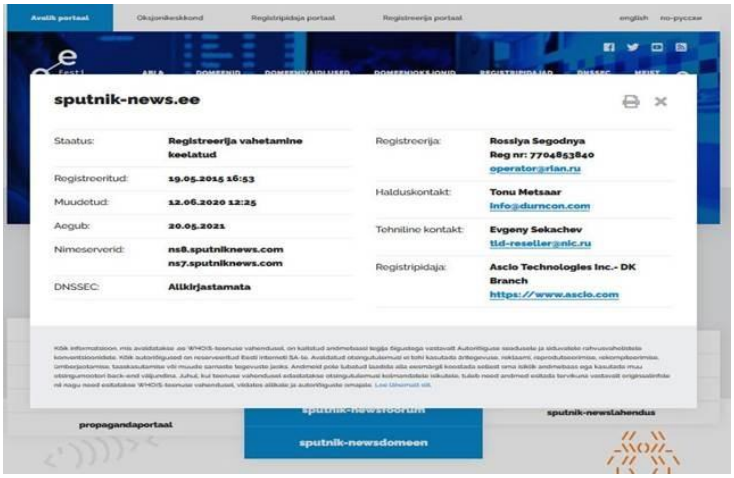


Рис. 2.1 Реєстраційні дані домену sputnik-news.ee *- заблокована реєстрація замінника (*Estonian Internet Foundation, *2020–2021 рр.). Джерело: Estonian Internet Foundation (EIS), est.ee, публічний реєстр доменів .ee*

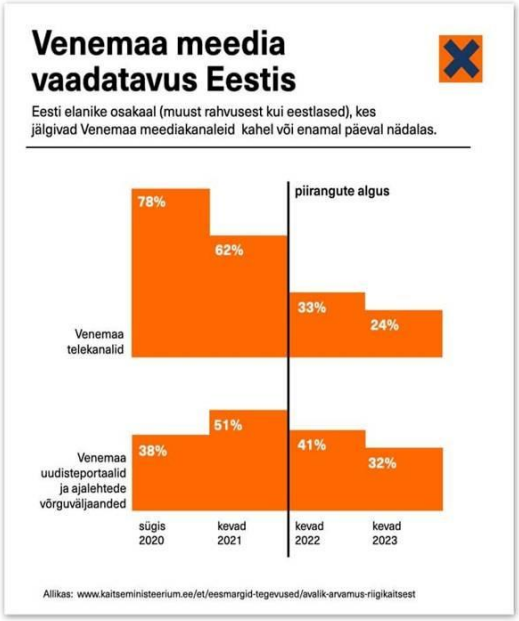
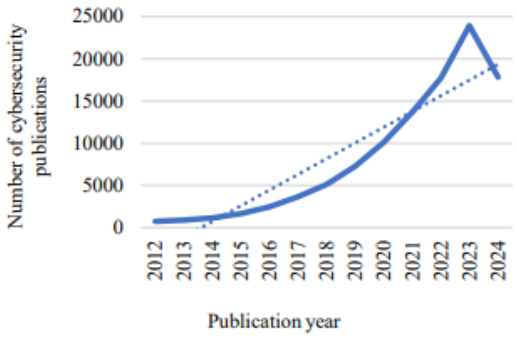


*Рис. 2.2 Динаміка перегляду російських медіаканалів в Естонії (2020–2023 рр.) серед нееестонського населення. Вертикальна лінія позначає момент запровадження обмежень (весна 2022 р.). Джерело: Міністерство оборони Естонії (*Kaitseministeerium*), щорічне опитування громадської думки. URL: www.kaitseministeerium.ee/et/eesmargid-tegevused/avalik-arvamus-riigikaitsest*

Figure 1

Growth in cybersecurity research publications (2012-2024)



Source: Scopus.

Рис. 3.1. Показники Глобального індексу кібербезпеки (GCI) 2024 року.