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:
ІНФОРМАЦІЙНА БЕЗПЕКА КРАЇН БАЛТІЇ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Студентки 4 курсу
денної форми навчання
Куріщенко Аліни
Євгенівни

Науковий керівник:
к. н. з держ. упр.
доцент кафедри
міжнародних відносин
Пістракевич О.В.

Київ – 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БРЕ – Бюро розвитку електрозв'язку

ГІК – Глобальний індекс кібербезпеки

ГУР МО – Головне управління розвідки Міністерства оборони України

КаПо – Департамент поліції Безпеки Естонії (*з ест.* Kaitsepolitseiamet)

МСЕ – Міжнародний союз електрозв'язку

МСІ – Міністерство зв’язку та інформатики

НІСО – Національна стратегія розвитку інформаційного суспільства

УКМЦ – Український кризовий медіа-центр

BECID – Baltic Engagement Centre for Combating Information Disorders

BEREC – Орган європейських регуляторів електронних комунікацій (*з англ.* Body of European Regulators for Electronic Communications)

CEF Digital – Програма “Connecting Europe Facility”

CERT – Центр реагування на комп’ютерні інциденти

CERT-EE – Центр реагування на комп’ютерні інциденти Естонії

CERT-LT – Національна команда комп'ютерної надзвичайної допомоги Литви

CERT.LV – Центр реагування на комп’ютерні інциденти Латвії

DDoS – Distributed Denial-of-Service attack

EDF – Європейський оборонний фонд (*з англ.* European Defence Fund)

EDIDP – Єврокомісія впровадила Європейську програму розвитку оборонної промисловості (*з англ.* The European Defence Industrial Development Programme)

E-ITS – Електронна інформаційно-технічна система (*з англ.* Electronic Intelligent Transport Systems)

EISA – Управління інформаційних систем Естонії

ENISA – Агенція Європейського Союзу (*з англ.* European Union Agency for Network and Information Security Агенція Європейського Союзу)

EuroQCI – Європейської квантової комунікаційної інфраструктури

GNSS – Global Navigation Satellite System

GOVSATCOM – The European Union Governmental Satellite Communications

Hybrid CoE – Європейський центр досвіду протидії гібридним загрозам

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

MFA – Multi-Factor Authentication

OECD – Організація економічного співробітництва та розвитку (*з англ*. Organisation for Economic Co-operation and Development)

PADR – Підготовчі дії з оборонних досліджень (*з англ.* Preparatory Action in Research Defence)

RIA – Riigi Infosüsteemi Amet

SAB – Бюро із захисту Конституції Латвії (*з лат.* Satversmes aizsardzības birojs)

TTJA – Consumer Protection and Technical Regulatory Authority of Estonia

VDD – Служба державної безпеки Латвії (*з лат.* Valsts drošības dienests)

ВСТУП

Актуальність теми. Російсько-українська війна стала каталізатором нових викликів для міжнародної безпеки, зокрема для країн Балтії. Агресивна політика Росії, що виходить за межі інформаційного простору, створює безпрецедентні загрози для суверенітету та демократичних цінностей трьох держав. Саме тому дослідження інформаційної безпеки країн Балтії набуває особливої актуальності та важливості, де країни Балтії демонструють високий рівень готовності до протистояння цим викликам, активно розвиваючи системи кіберзахисту, створюючи новітні механізми для боротьби з дезінформацією та співпрацюючи з міжнародними партнерами для зміцнення обороноздатності в інформаційній сфері. Враховуючи зростання кіберзагроз, розв'язання питань інформаційної безпеки є критично важливим для забезпечення національних інтересів, економічної стійкості та суверенітету балтійських країн.

Насамперед, це геополітичне розташування та історичний досвід. Країни Балтії географічно розташовані на передовій протистояння з Росією, а їхній історичний досвід радянської окупації робить їх вразливими до гібридних атак. Розуміння цих особливостей є ключовим для розробки ефективних стратегій забезпечення інформаційної безпеки.

Російська гібридна війна є також немало важливим фактором, з тієї причини, що Російська Федерація активно використовує інформаційну війну як інструмент досягнення своїх геополітичних цілей. Дезінформація, пропаганда, кібератаки та інші методи інформаційного впливу спрямовані на дестабілізацію суспільства, підрив довіри до державних інститутів та маніпулювання громадською думкою. До того ще глобальні наслідки, коли успішна інформаційна атака на країни Балтії може мати серйозні наслідки для

всієї Європи та світу, підриваючи довіру до демократичних інститутів та міжнародного порядку.

Незважаючи на значний тиск, країни Балтії демонструють помітні успіхи у розбудові стійких систем інформаційної безпеки та ефективній протидії гібридним загрозам. Аналіз їхніх стратегій, політик та конкретних інструментів може стати цінним для інших країн, які стикаються з подібними викликами.

Об'єктом дослідження є політика забезпечення інформаційної безпеки країн Балтії (Литви, Латвії та Естонії).

Предметом дослідження є механізми, стратегії та інструменти протидії інформаційним загрозам у країнах Балтії в умовах російсько-української війни.

Мета роботи – проаналізувати підходи країн Балтії до забезпечення інформаційної безпеки в умовах російсько-української війни, визначити ефективні механізми протидії сучасним інформаційним викликам і загрозам, що постають перед Естонією, Латвією та Литвою.

З метою досягнення поставленої цілі, у роботі були визначені такі завдання:

– дослідити становлення системи інформаційної безпеки країн Балтії;

– охарактеризувати державне регулювання та нормативно-правове забезпечення інформаційної безпеки балтійських країн;

– проаналізувати загрози інформаційній безпеці країн Балтії та дослідити реакцію країн Балтії на нові виклики після початку російсько-української війни;

– оглянути вплив російсько-української війни на суспільну думку в балтійських країнах (за результатами опитування);

– дослідити стратегії та подальші плани країн Балтії для покращення ситуації в інформаційному середовищі.

Теоретичне та практичне значення роботи полягає в тому, що отримані в ході дослідження результати становлять теоретичну базу для аналізу проблем інформаційної безпеки країн Балтії на сучасному етапі та можуть бути використані в подальших наукових розробках цієї тематики.

Апробація роботи відбулась під час V студентської наукової конференції «Актуальні проблеми міжнародних відносин» 22 травня 2025 року. Темою виступу була «Співпраця країн Балтії та України у сфері інформаційної безпеки».

Структура роботи. Бакалаврська робота складається із вступу, трьох розділів, які розбиті на вісім підрозділів, висновків та списку використаних джерел та літератури у кількості 72. Загальний обсяг роботи складає 88 сторінок.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Стан наукової розробки проблеми та джерельна база дослідження

У нинішню епоху цифрових технологій питання інформаційної безпеки набувають особливої значущості та комплексності. У зв'язку зі збільшенням кількості та рівня складності кібернетичних загроз, безперервним розвитком технологій та зростаючою залежністю суспільства від інформаційних систем, виникає необхідність у постійному розвитку та оптимізації заходів інформаційної безпеки.

Цей огляд представляє аналіз основних висновків та методології проведеного дослідження щодо інформаційної безпеки Балтійських країн в умовах російсько-української війни. Закладається міцна теоретична та фактична основа для подальшого дослідження. Методологія, що базується на аналізі офіційних документів та якісному описі ситуації, аналізує стан інформаційної безпеки як до початку російсько-української війни так і після повномасштабного вторгнення.

Класифікуючи використані джерела наукової та експертної літератури, такі як: наукові статті, монографії, підручники, матеріали конференцій, законодавчі акти, статистичні дані, експертні інтерв'ю, звіти організацій, веб-сайти, можна зазначити, що вони містять результати наукових досліджень, статистичні дані та аналіз конкретних випадків, що забезпечує доказову базу.

Стан наукової розробки щодо інформаційної безпеки країн Балтії в умовах російсько-української війни є динамічним і постійно розвивається, оскільки ситуація залишається напруженою. Однак, на основі загальнодоступної інформації та аналізу тенденцій, можна виділити, що загроза є актуальною для

Латвії, Литви та Естонії з боку Росії, розвивається активізація російських та проросійських кіберугруповань, саме тому відбувається міжнародна співпраця для посилення національних систем кібербезпеки, приймаються нові закони та вносяться зміни до існуючих, спрямовані на посилення відповідальності за кіберзлочини та регулювання інформаційного простору.

Проблеми безпеки країн Балтії в контексті російської агресії стали об'єктом комплексних досліджень представників різних наукових дисциплін, зважаючи на безперервний розвиток інформаційних технологій та виникнення нових загроз, наукова спільнота активно розробляє інноваційні підходи та рішення для ефективного контролю й захисту інформації в сучасному цифровому просторі.

Зокрема у статті українських вчених О. Івасечко та О. Коваля «Загрози та виклики для країн Балтії на сучасному етапі євроінтеграції»[1], які зробили значний внесок у дослідження безпекових викликів для країн Балтії та проаналізували наслідки російської агресивної політики. Було зроблено висновок, що Росія не чекає слушного моменту, а в сучасних умовах вдається до окремих елементів «гібридної війни» і звинувачує в цьому Латвію, Литву та Естонію у «порушенні прав російськомовного населення», а також використовуються різноманітні методи для досягнення цілей РФ, включаючи підтримку проросійських партій, підготовку провокаторів з числа молодих прихильників імперської ідеології, проведення розвідувальних та вербувальних операцій.

Стаття М. Гладиша та О. Краєвської «Балтійський вимір Європейської політики безпеки та оборони» зосереджена на загальному аналізі європейської політики безпеки і оборони в Балтійському регіоні. У ній була висвітлена

[1]Івасечко О. Я., Коваль О. В. Загрози та виклики для країн Балтії на сучасному етапі євроінтеграції. 2016. С. 248–255.

потенційна російська агресія, яка активно просувається через російські ЗМІ, що часто подається як реакція на утиск прав російськомовного населення в балтійських країнах та необхідність відновлення "геополітичної рівноваги" шляхом повернення цих країн до сфери впливу Росії [2].

В опублікованих матеріалах І. Туряниці «Пріоритети оборонної політики та національної безпеки Литовської Республіки на сучасному етапі[3]», а також О. Давимука та В. Кравченко «Особливості безпекової співпраці України та Литви в умовах протидії російській загрозі»[4] було детально досліджено оборонну політику Литви та її співпрацю з Україною. Визначаються сфери та головні пріоритети розвитку оборонної політики Литви в контексті її європейської та євроатлантичної інтеграції (членства в ЄС та НАТО), а також був зроблений аналіз інформаційної складової російсько-української війни, зокрема атаки на безпековий сектор України та пошук результативних засобів протидії інформаційним впливам.

Згідно з дослідженнями Звоздецької О.Я. «Кібербезпека країн Балтії: сучасні виклики та загрози», Естонія поставила собі за мету побудувати багаторівневу систему захисту від інформаційних загроз та створити міцне правове поле для регулювання питань кібербезпеки. Найбільш уваги в багаторівневій системі безпеки приділяється захисту критично важливих інформаційних ресурсів. Стратегічне планування є ключовим елементом, який об’єднує всі компоненти системи кібербезпеки та сприяє ефективному

[2]Гладиш М., Краєвська О. Балтійський вимір Європейської політики безпеки та оборони. *Грані.* 2015. № 4 (120). С. 80–85.
[3] Туряниця І. Пріоритети оборонної політики та національної безпеки Литовської Республіки на сучасному етапі. *Наукові зошити історичного факультету Львівського університету.* 2017. № 18. С. 323–333.
[4] Давимука О. О., Кравченко В. В. Особливості безпекової співпраці України та Литви в умовах протидії російській загрозі. *Стратегічні пріоритети.* № 3 – 4 (51). 2019. С. 70–75.

використанню інформаційних технологій для розробки інноваційних рішень задля гарантування інформаційної безпеки [5].

Дисертація В. Завадського «Європейська інтеграція країн Балтії (1991–2004 рр.)» є комплексним дослідженням шляху країн Балтії до членства в Європейському Союзі, розглядаючи політичні, економічні та соціальні аспекти цього процесу. Доведено, що при прийнятті країн Балтії до ЄС керівництво організації керувалося переважно політичними мотивами, які також відігравали важливу роль і для самих балтійських держав, поряд з економічною зацікавленістю.Розглянуто діяльність цих республік в організаціях регіонального та міжнародного співробітництва (Балтійській Асамблеї, Раді держав Балтійського моря, Північній Раді, ОБСЄ, Раді Європи) як важливу передумову євроінтеграції [6].

У своїй науковій праці М. Замікула «Країни Балтії на початку 1990-х років: передумови євроатлантичної інтеграції» досліджує можливі сценарії формування зовнішньої політики, політичні та соціальні фактори, що зумовили вибір європейського/євроатлантичного напряму як ключового у відносинах із сусідніми державами та на міжнародній арені балтійських країн[7].

Таким чином, сучасні наукові дослідження в галузі інформаційної безпеки є міцною та прогресивною сферою, що безперервно прогресує, відповідаючи на нові виклики. Вчені досягли значних успіхів у вивченні складних взаємозв'язків між технологіями, суспільством і політикою з метою глибшого

---

[5] Звоздецька О. Кібербезпека країн Балтії: сучасні виклики та загрози. Медіафорум : аналітика, прогнози, інформаційний менеджмент: збірка наукових праць. Чернівці: Чернівецький національний університет, 2017. Том 5. С. 20–34.

[6] Завадський В.М. Європейська інтеграція країн Балтії (1991-2004 рр.) у вітчизняній та зарубіжній історіографії. *Вісник Східноукраїнського національного університету ім. В. Даля*. гол. ред. Голубенко О. Л. Луганськ: Вид. СНУ ім. В. Даля, 2007. № 2. С. 65–71.

[7] Замікула М.О. Країни Балтії на початку 1990-х років: передумови євроатлантичної інтеграції. *Наукові праці Чорноморського державного університету імені Петра Могили. Серія «Історія»*. 2010. Т. 129. Вип. 116. С. 91–94.

розуміння проблем інформаційної безпеки Дослідження інформаційної безпеки спирається на різноманітну джерельну базу, що охоплює наукові статті у фахових виданнях, матеріали наукових конференцій, офіційні урядові документи та нормативно-правові акти. Попри значні досягнення, стрімкий розвиток інформаційних технологій та поширення кіберзагроз зумовлюють необхідність безперервних наукових пошуків для реагування на нові виклики та створення новаторських методів захисту інформаційних ресурсів у світі, що стає дедалі більш взаємозалежним.

1.2. Понятійно-категоріальний апарат та методи дослідження

Усвідомлення сутності понятійно-категоріального апарату та застосування дієвих методів дослідження є ключовими передумовами для вивчення інформаційної безпеки. Цей набір понять та категорій є своєрідним орієнтиром для дослідження різноманітних аспектів безпеки, включаючи приватність, доступність, контроль ризиків та аналіз загроз.

На сьогоднішній день існує багато різних інтерпретацій поняття «інформаційна безпека держави». За твердженням Фісуна Ю., інформаційна безпека – стан захищеності інформаційного середовища, який відповідає інтересам держави, який забезпечує формування, використання і можливості розвитку незалежно від впливу внутрішніх і зовнішніх інформаційний загроз [8].

В цілому, інформаційна безпека держави – це стан захищеності життєво важливих інтересів держави, суспільства та особистості в інформаційному просторі, тобто в сфері діяльності, в якій інформаційні комунікації відіграють провідну роль, від потенційних та реальних загроз. Він охоплює широкий

[8] Рижук О. Аналіз підходів щодо визначення поняття «інформаційна безпека держави» в умовах глобалізації. *Міжнародні відносини. Серія "Політичні науки"* № 13. 2017. С. 123–132.

спектр заходів, спрямованих на забезпечення, а саме конфіденційність, цілісність інформації та доступність відомостей.

Понятійно-категоріальний апарат інформаційної безпеки охоплює визначення ключових понять, таких як незахищеність, загрози, запобіжні заходи та заходи безпеки, а також систематизацію різних типів інцидентів безпеки, методів проникнення, запобіжних заходів та політик безпеки.

Стосовно аспектів інформаційної безпеки будь-якої країни, можна підкреслити захист критичної інформаційної інфраструктури, що включає в себе захист державних інформаційних систем, мереж, баз даних, а також об'єктів енергетики, транспорту, зв'язку та інших важливих галузей.

Протидія інформаційним загрозам – боротьба з дезінформацією, пропагандою, кібершпигунством, кібератаками та іншими формами інформаційного впливу.

Забезпечення інформаційного суверенітету – контроль над інформаційними ресурсами та технологіями, а також захист національного інформаційного простору від зовнішнього впливу.

Захист персональних даних – забезпечення конфіденційності та безпеки персональних даних громадян, які обробляються державними органами та іншими організаціями.

А також формування інформаційної культури суспільства, що передбачає підвищення рівня обізнаності громадян про інформаційні загрози та способи захисту від них.

Інформаційна безпека Балтійських країн забезпечується комплексом заходів, в яких беруть участь різні суб'єкти на національному та міжнародному рівнях. Першочергові з них:

1. Державні органи, до яких відносяться: Національні служби безпеки, що займаються контррозвідкою, захистом критичної інфраструктури та боротьбою

з кіберзагрозами; Міністерства оборони, які відповідають за кіберзахист військових інформаційних систем та проводять операції інформаційно-психологічного впливу; Державні центри кібербезпеки; Міністерства внутрішніх справ, а також Міністерства закордонних справ, які займаються міжнародним співробітництвом у сфері інформаційної безпеки.

2. Забезпечують кібербезпеку військових мереж Збройні Сили, що беруть участь у спільних навчаннях з партнерами по НАТО.

3. Приватний сектор – компанії, що надають послуги у сфері інформаційних технологій; оператори зв'язку; банки та інші фінансові установи.

4. Міжнародні організації: НАТО, Європейський Союз, Центр передового досвіду НАТО з кібероборони (CCDCOE, Естонія м.Таллінн).

Для запобігання інформаційній небезпеці через постійні розробки нових методів атак, була започаткована така галузь як кібербезпека. Кібербезпека — це комплекс заходів, спрямованих на захист комп'ютерних систем, мереж, програмного забезпечення та даних від цифрових атак, пошкоджень або несанкціонованого доступу. Це багатогранна галузь, що охоплює різні аспекти захисту інформації в цифровому просторі.

У зв’язку з цим, дезінформація є також важливим елементом, що зв’язаний в контексті інформаційної безпеки серед країн для поширення неправдивої інформації та введення в оману. Можна зазначити, що дезінформація – це навмисне поширення неправдивої або спотвореної інформації з метою введення в оману, маніпулювання громадською думкою або завдання шкоди. Це явище має давню історію, але в епоху цифрових технологій набуло нових масштабів і форм.

Важливо розуміти, що вплив дезінформації є багатогранним і може мати далекосяжні наслідки. Це можуть бути підрив довіри до ЗМІ, державних

інституцій та експертів, використання дезінформації для маніпулювання виборами, розпалювання конфліктів та дестабілізації суспільства, а також поглиблення соціальних розколів, розпалювання ненависті та створення атмосфери недовіри. Одним з головних інструментів ворога є саме дезінформація, де кампанії країни ворога використовують різноманітні методи та комбінації для досягнення своїх цілей.

Стосовно елементів інформаційної безпеки, можна зазначити конфіденційність (забезпечення доступу до інформації лише авторизованим особам та шифрування даних, контроль доступу та інші методи захисту від несанкціонованого розкриття), цілісність (забезпечення точності та повноти інформації, захист від несанкціонованої зміни або пошкодження даних, та використання контрольних сум, цифрових підписів та інших методів для перевірки цілісності). Доступність – забезпечення доступу до інформації авторизованим користувачам у потрібний час. Автентифікація – перевірка особи користувача, що намагається отримати доступ до інформації, та використання паролів, біометричних даних, смарт-карт та інших методів автентифікації. До цього ж входить авторизація, для визначення прав доступу користувача до інформації. Не відмовність, як забезпечення можливості підтвердження того, що певна дія була виконана. Фізична безпека, безпека персоналу, безпека мереж та безпека програмного забезпечення.

У сфері інформаційної безпеки застосовуються різноманітні методи дослідження, спрямовані на глибоке розуміння, ретельний аналіз та вдосконалення захисту інформаційних систем, мереж і даних. Огляд наявної літератури є важливим початковим етапом у дослідженні інформаційної безпеки. Цей підхід включає аналіз наукових статей, матеріалів конференцій, законодавств, нормативно-правових актів та інших релевантних джерел для оцінки поточного стану знань та недостатньо досліджених аспектів.

Детальні дослідження передбачають глибоке вивчення певної теми або явища з метою отримання конкретних, точних і всебічних даних. Було застосовано даний метод для аналізу загроз та викликів у сфері інформаційної безпеки балтійських країн, оскільки він може забезпечити важливі відомості про проблеми в цій галузі, та дає змогу отримати нові знання, підтвердити чи спростувати існуючі теорії або зробити важливі висновки щодо цієї теми.

Прогностичний аналіз має на меті передбачити можливі сценарії розвитку ситуації в сфері кібербезпеки та інформаційної війни в цих країнах з урахуванням зовнішніх і внутрішніх факторів. Даний метод дослідження було використано для оцінки потенціалу для поширення пропаганди та дезінформації, яка може підривати політичну стабільність і національну безпеку цих країн, а також аналізу можливих впливів інформаційних війн на суспільну думку, політичну ситуацію та економіку.

Розвідувальний аналіз передбачає збір, аналіз та оцінку даних з різних джерел, щоб зрозуміти поточний стан загроз, а також ймовірні майбутні загрози для інформаційної безпеки Балтії. Оскільки країни Балтії є частиною НАТО і Європейського Союзу, а Росія активно веде інформаційні війни, розвідувальний аналіз має важливе значення для забезпечення стабільності та захисту від кібератак і інформаційних операцій.

Значна кількість дослідницьких робіт залучає прогностичні та глибокі методи аналізу, щоб на основі аналізу історичних та поточних даних передбачити, що може статися в майбутньому. Це дозволяє дослідникам виявляти потенційні тенденції, ризики та можливості; дають змогу виявляти складні закономірності та взаємозв'язки у великих обсягах даних, що призводить до більш точних прогнозів.

Об'єднання різних методів дослідження дає змогу посилити їхні сильні якості та компенсувати слабкі сторони, як це було зроблено в дослідженні

інформаційної безпеки балтійських країн в умовах російсько-української війни.

Виходячи з цього, понятійно-категоріальний апарат і методологія дослідження формують базис для досліджень у галузі інформаційної безпеки, гарантуючи системний підхід до сприйняття, дослідження та врегулювання проблем, що стосуються захисту цифрових активів і систем.

Систематизована класифікація об’єктів, яку пропонує понятійно-категоріальний апарат, слугує для впорядкування ключових концепцій, засад і моделей у цій галузі, що сприяє прозорій комунікації та розповсюдженню знань серед дослідницької спільноти, практикуючих фахівців та стейкхолдерів.

Разом з тим, широкий спектр дослідницьких підходів, що охоплює аналіз літератури, опитування та прогнози дозволяє досліджувати, оцінювати та розробляти новаторські способи боротьби з новими загрозами та слабкими місцями.

Резюмуючи, можна констатувати, що наукова розробка проблематики інформаційних систем є динамічною та еволюціонуючою сферою. В умовах швидкого технологічного прогресу та всеосяжного проникнення цифрових систем у сучасне життя, необхідність у дієвих засобах інформаційної безпеки набуває особливої «гостроти».

У цій галузі наукові співробітники та дослідники досягли вагомих результатів у вивченні багатоаспектності проблем міжнародної інформаційної безпеки, починаючи з ідентифікації вразливостей у програмних продуктах та мережевій інфраструктурі й закінчуючи дослідженням соціально-технічних чинників, які впливають на ситуацію на міжнародній арені та національній безпеці балтійських країн.

Широке коло наукових праць, галузевих звітів, тематичних та емпіричних досліджень складають джерельну базу цієї роботи, надаючи різнопланові розуміння та точки зору на складну політичну ситуацію між Росією та Україною, що зачіпає країни Балтійського регіону.

Понятійно-категоріальний апарат є базовою основою для систематизації та об'єднання ключових уявлень, ідей, припущень і концепцій у сфері дослідження інформаційних систем. Він забезпечує впорядковану класифікацію для категоризації різноманітних тем, починаючи від контролю доступу і завершуючи управлінням ризиками та дотриманням нормативних вимог. Забезпечуючи концептуальну базу, понятійно-категоріальний апарат сприяє міжнародній співпраці та обміну знаннями.Окрім цього, він сприяє глибшому розумінню базових принципів і динаміки, які визначають явища інформаційної безпеки, що, у свою чергу, впливає на формулювання дослідницьких питань, гіпотез та алгоритмів.

Таким чином, дослідницька база у сукупності з розвиненим понятійно-категоріальним апаратом та різноманітними методами дослідження створює надійний фундамент для розширення знань і вдосконалення практичної діяльності в сфері інформаційної безпеки.

РОЗДІЛ 2

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРАЇН БАЛТІЇ

2.1. Становлення інформаційної безпеки країн Балтії

Повертаючись до історії та зазначаючи загрози, перед якими стоять країни Балтії щодо їх інформаційній безпеки, розпад Радянського Союзу створив нові геополітичні реалії, змусивши колишні радянські республіки шукати своє місце у світі. Серед них особливо відзначилися країни Балтії, які спираючись на історичний досвід державності та прагнучи забезпечити свою безпеку, швидко обрали курс на інтеграцію до Європейського Союзу та НАТО. Цей вибір був обумовлений низкою факторів, зокрема успішним досвідом міжвоєнного періоду, коли балтійські держави вже довели свою здатність будувати суверенні держави.

Історично склалося так, що країни Балтії завжди відчували культурну та цивілізаційну спорідненість із Західною Європою. Однак, загроза з боку Росії, яка прагнула відновити свій вплив у регіоні, змусила країни Балтії прискорити процес інтеграції в євроатлантичні структури. Саме питання безпеки стало вирішальним фактором, який спонукав їх до вступу до НАТО. При цьому, членство в Альянсі розглядалося як необхідний крок на шляху до Європейського Союзу, оскільки гарантувало колективну безпеку і створювало сприятливі умови для економічного та політичного розвитку.

Рішуче прагнення Литви, Латвії та Естонії до інтеграції із Західною Європою зумовлене, зокрема, двома додатковими міркуваннями. Перше з них – це логіка безпеки та політичної стабільності, яка забезпечується членством у НАТО як відповідь на потенційну російську «загрозу». Другим важливим чинником є логіка «ідентичності»: країни Балтії надзвичайно цінують свою національну самобутність, яка зазнала утисків у період

Радянського Союзу, і тому інтеграція до Європейського Союзу та Балтійського регіону підкреслює їхню приналежність до «західноєвропейської» цивілізації[9].

Історичний шлях країн Балтії тісно пов'язаний з постійним іноземним втручанням, позначений численними руйнівними війнами, що протягом століть ініціювалися сусідніми державами, що й сьогодні змушує корінних жителів цих земель мати обґрунтовані побоювання щодо свого майбутнього. Споконвіку балтійські народи, розташовані на межі між Європою та Росією, між скандинавським та слов'янським світами, відчували на собі вплив іноземного втручання, інформаційних та націоналістичних настроїв.

Для розуміння того, як три балтійські країни з загальною кількістю населення трохи більше шести мільйонів впливають на політику великих держав та їхні інтереси, варто згадати деяких відомих політиків та аналітиків: Карла Більдта та Джорджа Кеннана. У 1994 році, у своїй статті для журналу "Foreign Affairs", тодішній прем'єр-міністр Швеції Карл Більдт зазначив, що країни Балтії стануть індикатором майбутнього курсу Росії: «Країни Балтії стануть лакмусовим папірцем нового напрямку розвитку [Росії]» [10].

Після відновлення незалежності на початку 1990-х років, країни Балтії зіткнулися з викликами побудови нових демократичних інституцій та інтеграції до західних структур. Вже тоді стало очевидно, що інформаційний простір може бути полем боротьби. Ключовим моментом, який каталізував розвиток систем кібербезпеки, стала кібератака на Естонію у 2007 році. Ця атака, спрямована на державні установи, банки та ЗМІ, була першою в історії кібервійною проти суверенної держави, що стала «дзвінком» для всіх країн

[9] The European Union and the Baltic States: Visions, Interests and Strategies for the Baltic Sea Region. Ed. by Jopp M. and Arnswald S. Helsinki : *The Finnish Institute of International Affairs*, 1998. 269 p.
[10] Bildt, C. (1994, Sept. – Oct). *The Baltic litmus test. Foreign Affairs*, p. 73(5), 72 – 85.

Балтії та світу, підкресливши, що кіберпростір є п'ятим доменом війни, поряд із сушею, морем, повітрям та космосом.

Таким чином, інформаційне середовище країн Балтії є динамічним та складним з ранньої історії. Історичні фактори, такі як радянська окупація, геополітичне розташування на східному кордоні ЄС, робить країни Балтії вразливими до російської пропаганди та інформаційних атак, а глобальні тренди формують його особливості. Для забезпечення інформаційної безпеки та стійкості суспільства країни Балтії ще з віддаленого історичного періоду постійно працювали над підвищенням медіаграмотності населення, підтримкою незалежних медіа та міжнародним співробітництвом. В цілому країни Балтії успішно реалізували стратегію інтеграції до Європейського Союзу, що є позитивним як з точки зору досягнутого результату, так і з позиції захисту їхніх національних інтересів, включаючи інформаційного. Процес європейської інтеграції сприяв позитивним внутрішнім змінам у різних сферах суспільного життя балтійських країн.

2.2. Державне регулювання сфери інформаційної безпеки країн Балтії

В умовах формування глобального інформаційного простору держави, основна проблема інформаційної безпеки полягає в стрімкому розвитку та впровадженні новітніх інформаційних, телекомунікаційних і кібернетичних технологій. Інформаційна безпека країн Балтії (Естонії, Латвії та Литви) є надзвичайно важливим питанням з огляду на їхнє географічне розташування та історичний досвід. Балтійські країни активно працювали над зміцненням своєї інформаційної безпеки, враховуючи загрози, що походять від Російської Федерації та інших джерел. Говорячи про зміст інформаційної безпеки балтійських країн, можна зазначити національні стратегії кібербезпеки, де

кожна країна має свої власні концепції, які визначають пріоритети та напрямки діяльності у цій сфері.

Важливо зазначити, що країни Балтії надавали особливого значення загрозам кібербезпеки та інформаційному впливу з боку Російської Федерації ще до початку повномасштабної війни, та ще з минулих років до російсько-української війни, ідучи до сьогодення, ця діяльність [інформаційна безпека країн Балтії] здійснюється у відповідності до законодавства і підлягає постійному контролю спецслужб. Відповідно до законодавства балтійських країн, щорічно готуються та оприлюднюються національні звіти про загрози безпеці, зібраних Департаментом державної безпеки та військовою розвідкою, в яких значне місце відводиться питанням національної та інформаційної безпеки. В цілому, кожна з країн Балтії має власну стратегію та інституції, відповідальні за забезпечення інформаційної безпеки.

Ще на ранніх етапах розвитку кібербезпеки, Естонія прийняла першопрохідницьке рішення, розробивши та затвердивши власну Національну стратегію, яка відповідає міжнародним нормам. Для зміцнення кібербезпеки у 2006 році в Естонії було створено CERT Estonia (далі – CERT-EE), а 2008 року країна стала платформою для міжнародної співпраці у сфері кібербезпеки завдяки відкриттю центру НАТО в Таллінні.

Розташований в Естонії, Центр передового досвіду НАТО з кіберзахисту, створений у 2008 році, є міжнародною військовою організацією, яка об'єднує зусилля країн-членів Альянсу та партнерів для підвищення рівня їхньої інформаційної безпеки та протидії зростаючим кіберзагрозам. Естонія також має Агентство з питань кібербезпеки (далі – RIA), яке відповідає за координацію та реалізацію державної політики у сфері кібербезпеки.

Обов'язки з координації державної політики в галузі кібербезпеки в Естонії до 2011 року виконувало Міністерство оборони (далі – МО), але після

2011 року відповідальність за розробку та впровадження державної політики у сфері кібербезпеки в Естонії перейшла від МО до Міністерства з економічних питань та комунікацій (далі – МЕК). Кібернетична оборона є невід'ємною частиною загальної системи національної безпеки, а МО відповідає за координацію всіх зусиль у цій сфері. Безпосередньо МЕК, а саме його підрозділи, такі як Департамент державних інформаційних систем та Естонський центр інформатики, несуть відповідальність за розробку та впровадження політики інформаційної безпеки[11].

У червні 2011 року Естонський центр інформатики реформували, надавши йому статус Управління інформаційних систем Естонії (EISA) з розширеними повноваженнями. Управління інформаційних систем Естонії складається з кількох підрозділів, кожен з яких спеціалізується на певних аспектах кібербезпеки, забезпечуючи таким чином комплексну охорону державного кіберпростору, наприклад: Департамент із захисту критичних інформаційних інфраструктур (Critical Information Infrastructure Protection (CIIP), Центр обміну документами (Document about exchange centre (DEC), Інфраструктура відкритих ключів (Public Key Infrastructure (PKI), IT-інфраструктура (IT-infrastructure). Інфраструктура відкритих ключів забезпечує безпечну ідентифікацію та підписи, а стійка IT-інфраструктура гарантує безперебійну роботу державних інформаційних послуг навіть за умов форс-мажору.

Створена при Комітеті з питань безпеки Уряду Естонії, Рада з кібербезпеки є міжвідомчим органом, який забезпечує стратегічне керівництво та координацію у сфері кібербезпеки, сприяючи об'єднанню зусиль різних державних органів для ефективного протистояння кіберзагрозам.

---

[11]National Security Concept of Estonia. 2010. Pp. 7–8. URL: https://www.files.ethz.ch/isn/156839/Estonia%20-%20National%20security%20concept%20of%20estonia%202010.pdf (date of access: 06.04.2025).

У 2014 р. був підписаний новий документ «Стратегія кібербезпеки на 2014-2017 рр.» (Cyber Security Strategy, 2014), офіційно визнавши кіберпростір операційним середовищем, НАТО підкреслило, що кіберзагрози становлять таку ж серйозну загрозу безпеці, як і традиційні військові загрози, і закликало до колективних дій для протидії їм. Пізніше, у 2015 році Європейська комісія ініціювала низку великих, позначених грифом секретності програм, призначених для компаній з Євросоюзу та країн-партнерів. Створення системи безпеки для таких конфіденційних проєктів було непростим завданням. Масштабні програми ЄС отримали вигоду від уніфікованої системи безпеки Комісії, що спростило адміністрування та підвищило ефективність підготовки та контролю проєктів. Секретність не стримувала компанії, адже Національний орган безпеки Служби зовнішньої розвідки Естонії надавав роз'яснення щодо захисту та створював просту й зрозумілу структуру безпеки для всіх учасників. З 2015 року за ініціативою Комісії було запущено низку секретних програм, спрямованих на інновації та розвиток в оборонній промисловості, серед яких: Підготовчі дії з оборонних досліджень (PADR) у 2017-2019 роках, Європейська програма розвитку оборонної промисловості (EDIDP) у 2019 – 2021 роках та Європейський оборонний фонд (EDF), що діє з 2021 року.

Згодом у 2017 році в Таллінні відкрився Об’єднаний центр передових технологій НАТО (NATO Cooperative Cyber Defence Centre of Excellence), який став флагманом європейської кібербезпеки, об’єднавши зусилля країн-членів Альянсу в боротьбі з кіберзагрозами та сприяючи розробці новітніх технологій у інформаційній галузі.

Таким чином, підґрунтям регулювання інформаційної безпеки Естонської Республіки здійснюється Національною стратегією, Департаментом

державних інформаційних систем, Ради з кібербезпеки, Міністерством оборони та Естонським центром інформатики.

Беручи наступну Балтійську країну – Латвію, то вона завжди прагнула зміцнити свою безпеку шляхом оновлення законодавства та вдосконалення інструментів протидії загрозам. Латвія розробила нову Концепцію національної безпеки, яка передбачає комплекс заходів для протидії сучасним викликам, зокрема, у сферах інформаційної безпеки, захисту державної мови та енергетичної незалежності.

Політика Латвії у сфері кібербезпеки базується на таких фундаментальних документах, як Концепція національної безпеки 2011 року, CERT.LV, який є національним центром реагування на інциденти інформаційної безпеки та Стратегія кібербезпеки 2014–2018 років[12]. Заходи, передбачені Стратегією кібербезпеки Латвії на 2014–2018 роки, виявилися настільки ефективними, що деякі з них, зокрема, моніторинг критичної інфраструктури, були продовжені до 2022 року.

Основною метою Стратегії є створення ефективної системи кібербезпеки шляхом розробки відповідного законодавства, аналізу ризиків та визначення пріоритетних напрямків розвитку, що дозволить забезпечити захищеність інформаційних систем у всіх секторах економіки та суспільства. Політика кібербезпеки спрямована на посилення стійкості держави до кібератак шляхом вдосконалення технологічних засобів захисту, підвищення кваліфікації фахівців та проведення масштабних інформаційних кампаній з метою підвищення обізнаності громадян про загрози в кіберпросторі. За словами Ковальова А. А. – російського журналіста та перекладача, для досягнення мети

[12]Cyber Security Strategy of Latvia 2014–2018. P. 5. URL: https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas_strategija%20EN%20%281%29.pdf (date of access: 07.04.2025).

підвищення рівня кібербезпеки політика пропонує комплексний підхід, який включає в себе п'ять взаємопов'язаних напрямів: посилення захисту інформаційних систем, управління кіберризиками, підвищення стійкості ІКТ-інфраструктури тощо. Політика спрямована на створення умов для рівного доступу всіх громадян до державних та комерційних електронних послуг, підвищення рівня кібергігієни населення шляхом проведення інформаційних кампаній, стимулювання наукових досліджень у галузі кібербезпеки, активної участі у міжнародних ініціативах та зміцнення правових засад кіберпростору шляхом вдосконалення законодавства та посилення боротьби з кіберзлочинністю[13].

У Латвії, до того ж, існує чітко визначена процедура щорічної публікації звітів про стан національної безпеки, відповідальна за яку Служба державної безпеки Латвії (далі – СДБЛ, *з лат.* VDD)[14]. Окрім СДБЛ, в Латвії функціонує Бюро із захисту Конституції (далі –SAB)[15], яке також здійснює оцінку загроз національній безпеці та публікує власний щорічний звіт, у якому особлива увага приділяється російській загрозі.

У липні 2018 року на Брюссельському саміті, рішення, що були прийняті на самітах в Уельсі та Варшаві у 2016 році[16], були підтверджені, та було вирішено зміцнити безпеку східного флангу НАТО. Посилення присутності Альянсу в країнах Балтії та Польщі стало важливим доповненням до Стратегії

---

[13]Ковальов А. А., Балашов А. І. Міжнародно-правові аспекти політики кібербезпеки деяких європейських країн колишнього радянського блоку. *Вісник Поволзького інституту управління.* 2018. №5 (18). З. 105–114.

[14] Valsts Drosibas Dienests. Pārskats par VDD darbību 2024. gadā. URL: https://vdd.gov.lv/ (дата звернення: 04.04.2025).

[15] Latvijas Republika Satversmes Aizsardzibas Birojs. 2023. URL: sab.gov.lv/files/uploads/2024/02/SAB-2023.gada-parskats_LV.pdf (date of access: 07.04.2025).

[16] North Atlantic Treaty Organisation. Brussels Summit Declaration. 11 – 12 July. 2018. URL: https://www.nato.int/cps/en/natohq/official_texts_156624.htm (date of access: 07.04.2025).

стримування, де було зазначено, що необхідним є вживання додаткових заходів для посилення стримування, що включають елементи посилення повітряних і морських сил, інформаційних, а також сил швидкого реагування НАТО.

Латвійський політичний діяч Раймондс Вейоніс заявив, що для протидії гібридним загрозам, особливо в інформаційному просторі, необхідно зміцнювати стійкість держав-членів НАТО. Ризики, пов'язані з когнітивними атаками, ймовірно, збільшаться з розвитком штучного інтелекту та методів збирання великих даних, саме тому він наголосив на необхідності інвестицій демократичних країн у протидію цим новим викликам для зниження потенційних ризиків та підвищення когнітивної стійкості.

На завершення своєї промови, Раймондс Вейоніс зазначив, що Латвія має максимально підвищити рівень обізнаності своїх громадян, і особливо політичних лідерів, щодо ризиків цифрової безпеки. Ця робота повинна починатися з трансформації латвійських освітніх систем і має бути спрямована на загальне підвищення здатності суспільств критично мислити. Інакше, якщо Латвія не відреагує на ці нові виклики, на неї чекають серйозні наслідки в Балтійських країнах, міжнародних організаціях та демократичних системах.

За словами президента Латвії, країни-члени Альянсу з кожним роком краще розуміють широкий спектр погроз та приймають необхідні рішення. Центр передового досвіду стратегічних комунікацій НАТО в Ризі за короткий час завоював міжнародне визнання, проводячи важливу роботу з виявлення загроз в інформаційному просторі та розробці заходів у відповідь. Дослідження Центру передового досвіду стратегічних комунікацій НАТО також у 2019 році, такі як «Реагування на виклики когнітивної безпеки» та «Чорний ринок маніпуляцій у соціальних мережах», демонструють дедалі більшу вразливість суспільства до когнітивних атак, які використовують великі обсяги персональних даних. Але важливо далі розвивати як міжнародне

співробітництво, так і зміцнювати національну стійкість та координувати роботу різних структур.

Остання з країн Балтії – Литовська Республіка, мала ще до початку повномасштабного вторгнення Національний центр кібербезпеки, який відповідає за координацію діяльності з питань кібербезпеки, регулює свою інформаційну безпеку за допомогою Програми розвитку електронної інформаційної безпеки 2011-2019 років (далі – ПРЕІБ)[17], затвердженої у 2011 році, та Закону «Про Кібербезпеку»[18], прийнятого у 2014 році. ПРЕІБ спрямована на визначення цілей та завдань для розвитку електронної інформації, щоб забезпечити конфіденційність, цілісність та доступність електронних даних та послуг у кіберпросторі, а також захистити електронні комунікаційні мережі, інформаційні системи та критично важливу інформаційну інфраструктуру від інцидентів та кібератак. Головними цілями Програми було заявлено посилення захисту державних інформаційних ресурсів, а також гарантія ефективного функціонування критично важливої інформаційної інфраструктури[19].

Виокремлюючи та аналізуючи по законах, можна зазначити мету агресивних інформаційних атак – створення атмосфери страху в балтійському суспільстві. Інформаційна війна виступає одним з інструментів протиборства авторитарних режимів і західного світу. Росія регулярно організовує комплексні інформаційні кампанії, які поєднують психологічний тиск та інформаційно-кібернетичні операції, спрямовані на зміну мислення, установок і поведінки цільової аудиторії шляхом розповсюдження дезінформації та

[17]Del Elektronines Informacijos Saugos (Kibernetinio Saugumo) Plėtros 2011-2019 METais Programos Patvirtinimo. Nr. 796. 2011–2019.

[18] Lietuvos Respublikos. *Kibernetinio Saugumo Įstatymas*. Nr. XII-1428. 2014.

[19]Звоздецька О. Кібербезпека країн Балтії: сучасні виклики та загрози. *Медіафорум : аналітика, прогнози, інформаційний менеджмент: збірка наукових праць.* Чернівці: Чернівецький національний університет, 2017. Том 5. С. 20-34.

використання кібер- або фізичних засобів впливу. Навіть до початку повномасштабного вторгнення спостерігалося значне зростання як кількості, так і складності інформаційних атак. Литва, Латвія, Естонія та Польща стали об'єктами інформаційних операцій, що вирізнялися безпрецедентним характером та масштабом, і навіть включали фізичні дії для посилення їхнього впливу.

Таким чином, законодавчо закріплена практика щорічної публікації звітів про загрози національній безпеці у країнах Балтії та Національні стратегії мають виключно важливе значення для забезпечення ефективного протистояння викликам і загрозам. Системами забезпечення захисту критичної інфраструктури в інформаційному просторі є законодавчі зміни, які виступають головним пріоритетом для трьох країн, що активно працюють над гарантуванням безпеки, розуміючи, що це ключова умова для їхньої національної безпеки. Створюється база даних, що систематизує всі види загроз, особливо акцентуючи увагу на інформаційних, відстежує зміни в цих загрозах та ідентифікує нові, при цьому всі загрози називаються своїми іменами, включаючи осіб та медіа, що становлять загрозу національній та інформаційній безпеці.

2.3. Нормативно-правове забезпечення інформаційної безпеки країн Балтії

Покладаючись лише на власний культурний досвід, балтійським землям неможливо уникнути упереджень у прогнозуванні майбутнього та оцінці загроз. Обмеженість перспективи, зумовлена знаходженням у звичному соціокультурному середовищі, може спотворити наше розуміння реальних процесів. Тому для отримання більш об’єктивної оцінки ситуації необхідно

залучати до дослідження експертів з інших культурних і політичних контекстів.

Безпекова ситуація в країнах Балтії тісно переплітається з міжнародними подіями, причому ключові загрози безпеці мають транснаціональний характер. Це зумовлює потребу в забезпеченні стабільності безпеки як на регіональному, так і на глобальному рівнях. Так, у «Рамковій програмі політики безпеки» (далі – РППБ) від 2017 року зазначається, що прямі загрози для держави визначаються станом безпеки в євроатлантичному регіоні та характером відносин між країнами безпосереднього сусідства. У Спільній партійній угоді Естонії 2017 року також наголошується на асиметричних загрозах, що не мають національних меж і джерело яких складно встановити, проте їхній вплив є порівнянним з традиційними загрозами безпеці. Західні країни постійно стикаються з терористичною загрозою, що походить з держав Близького Сходу та Північної Африки, де відбуваються зміни політичних режимів. Згідно з наявними документами, цей фактор має значний вплив на безпекову ситуацію в усьому Балтійському регіоні.

У глобальному масштабі Росія виявила свою силу в цифровій сфері. Після російських кібератак на Естонію під час квітневих заворушень 2007 року всі країни Балтії визнали кіберзагрози як важливий фактор, що впливає на їхню безпеку, та відобразили це у своїх офіційних документах.

У документах усіх країн Балтії глобальні кризи та нерівномірний соціальний розвиток визначено як загрози безпеці. Протягом останнього десятиліття головна зовнішня загроза для Балтійського регіону походить від Росії, яка використовує широкий спектр інструментів, включаючи військові, політичні, дипломатичні, інформаційні та економічні, для реалізації власних інтересів. Крім нарощування власної військової потужності, Росія також посилила свою військову присутність у Балтійському морі та поблизу кордонів

країн Балтії. Її агресивна та провокаційна поведінка проявляється, зокрема, у порушеннях повітряного простору, проведенні наступальних військових навчань та навіть у ядерних погрозах. Росія становить загрозу для всього євроатлантичного регіону, володіючи потенціалом і демонструючи готовність застосовувати різноманітні засоби впливу, включаючи військові, економічні, енергетичні, інформаційні та інші невійськові інструменти. (Основи політики безпеки, 2017 [20]; Стратегія національної безпеки, 2017)[21].

Пізніше, на сайті Державного органу з інформаційних систем Естонії[22] було зазначено, що атаки програм-вимагачів все частіше супроводжуються загрозою не лише шифрування, але й викрадення та оприлюднення даних. Тому всі організації мають усвідомлювати, що у випадку такої атаки інформація на їхніх пристроях буде не лише недоступною через шифрування, але й, з огляду на зростаючу тенденцію, може бути вкрадена та розголошена. Отже, одних лише резервних копій даних недостатньо для ефективного протистояння атакам програм-вимагачів.

Як приклад, у 2020 році CERT-EE зафіксував випадок масштабної атаки програми-вимагача на великий медичний заклад. Внаслідок інциденту дані були не лише зашифровані, а й викрадені. Після відмови жертви сплатити викуп за ключ дешифрування, зловмисники заявили про намір оприлюднити вкрадену інформацію. CERT-EE підтверджує факт розголошення даних, що

---

[20]"Eesti julgeolekupoliitika alused". 2017. P. 3–6, 16–17 URL: https://www.riigiteataja.ee/aktilisa/3060/6201/7002/395XIII_RK_o_Lisa.pdf# (date of access: 13.04.2025).

[21]Nacionalinio Saugumo Strategija. 2017. P. 5–7. URL: https://kam.lt/wp-content/uploads/2022/03/2017-nacionalinio-saugumo-strategija.pdf (date of access: 13.04.2025).

[22] Riigi Infosüsteemi Amet. *Lunavara Rünnakutega kaasneb üha sagedamini andmevarguse ja lekke risk.* Juuni 2020. URL: https://www.ria.ee/sites/default/files/documents/2022-11/Lunavararunnakutega-kaasneb-uha-sagedamini-andmevarguse-ja-lekke-risk.pdf (date of access: 13.04.2025).

свідчить про їхнє попереднє викрадення. Оприлюднена інформація містила імена та прізвища пацієнтів, дати їх народження, стать, громадянство, професію, поштову адресу та номер телефону. Крім того, у витоку були присутні ім'я та номер телефону лікаря, записи про алергії, результати аналізів і відомості про лікування. Сума викупу, яку вимагали зловмисники, становила мільйони євро. Враховуючи чинність Загальний регламент із захисту даних (General Data Protection Regulation, далі – GDPR), де передбачені штрафи до 20 мільйонів євро або до 4% світового обороту, ймовірно, що загроза розкриття персональних даних у подібних атаках зростатиме.

Парламент Латвії, враховуючи безпекові виклики для Балтійських республік ще до початку повномасштабного вторгнення, у 2016 році прийняв ряд законодавчих змін, спрямованих на зміцнення національної безпеки. Підкреслено, що в критичній ситуації, як-от іноземне вторгнення, військові підрозділи повинні діяти негайно та самостійно, не чекаючи наказів від вищого командування.

Латвійські офіційні документи (Концепція національної безпеки 2008 [23] та 2019 років) визначають, що належний рівень безпеки держави досягається завдяки стабільному внутрішньополітичному клімату, сприятливій соціально-економічній кон'юнктурі, належному розвитку оборонних спроможностей, сучасній системі управління кризами, вдосконаленій цивільній обороні, підтримці громадськістю політики безпеки, дотриманню міжнародних стандартів та зобов'язань, а також послідовній трансатлантичній співпраці в політичній, економічній, безпековій та оборонній сферах. Щодо загроз національній безпеці Латвії, то вони пов'язані з: розвитком ситуації у сфері міжнародної безпеки; військових дій Росії поблизу кордонів Латвії та

[23]National Security Concept. Nr.165. 2008. National Security Concept. 2019. URL: https://www.vestnesis.lv/ta/id/182987 (date of access: 13.04.2025).

шкідливої кібердіяльності та тенденції міжнародного тероризму. Крім того, у Концепції зазначено, що загрози становлять спроби окремих зарубіжних країн вплинути на латвійську державу, суспільство та її цінності, на колишній прозахідний зовнішньополітичний курс країни, а також на внутрішньополітичну стабільність політичними, гуманітарними, економічними, а найголовніше - інформаційними засобами. Для реалізації базових державних функцій необхідні рішення, що забезпечують державний контроль над критичною ІТ-інфраструктурою. До ключових заходів із запобігання кіберзагрозам належать: впровадження дієвої політики кібербезпеки; нарощування потенціалу виявлення та реагування на загрози; зміцнення безпеки критичної ІТ-інфраструктури; оцінка ризиків, пов'язаних з інфраструктурними об'єктами та послугами; а також поглиблення міжвідомчої та міжнародної співпраці.

Починаючи з 2015 року, коли Сейм затвердив попередню Концепцію у 2008 році, міжнародна безпекова обстановка не покращилася. На тлі вже існуючих конфліктів та суперечностей з'явилися нові ризики та загрози. Діапазон загроз національній безпеці суттєво збільшився через посилення гібридних загроз, серед яких особливе місце займають ризики кібербезпеки. Гібридні загрози проявляються різноманітно і можуть охоплювати як військові інструменти та залякування їхнім застосуванням, так і широкий спектр невійськових методів, починаючи від діяльності розвідувальних та безпекових служб, кібератак, масштабних інформаційних кампаній і розповсюдження неправдивої інформації, використання внутрішніх суперечностей та конфліктного потенціалу в суспільстві, і закінчуючи економічним тиском та терористичними актами. Гібридні загрози діють узгоджено, підсилюючи одна одну, і їхньою характерною рисою є максимальне приховування будь-якого зв'язку з організаторами відповідних дій. Так само, у багатьох випадках можна лише

підозрювати виконавців, але точно встановити та довести їхню причетність вкрай складно. Очікується подальше зростання гібридних загроз, включаючи кібернетичні ризики, що особливо актуально з огляду на розвиток інформаційних технологій. Через це ЄС та НАТО започаткували у 2017 році Європейський центр передового досвіду протидії гібридним загрозам (Hybrid CoE). Заснований за ініціативою Фінляндії, Центр був зосереджений на питаннях безпеки в Європі, сприяючи поглибленню співробітництва між Європейським Союзом та НАТО відповідно до Спільної декларації про протидію гібридним загрозам, ухваленої у квітні 2016 року.

Беручи за увагу третю Балтійську країну – Литву, згідно з Литовською Стратегією національної безпеки[24], прийнятою у 2017 році, головною загрозою є агресія Росії, яка ігнорує загальновизнані міжнародні правила та принципи мирного співіснування.

Повертаючись у раніші часи, в 2013 році у Литовській Республіці спостерігалося зростання кількості кіберінцидентів, спрямованих проти інформаційних систем та мереж державних установ ADA, комп'ютерів приватних компаній і окремих осіб. При цьому, порівняно з 2012 роком, технології атак, методи та способи несанкціонованого проникнення стали значно складнішими. Кібератаки на інформаційні системи та мережі ADA литовських державних установ, приватних компаній і фізичних осіб здійснюються різними зловмисниками з різними мотивами, яких умовно можна поділити на дві категорії. Перша група включає державних або спонсорованих державою, фінансованих державою кіберзлочинців, що діють за вказівками державних, розвідувальних та безпекових служб, володіють

[24] National Security Strategy of the Republic of Lithuania 2017. *Cooperative Cyber Defence Centre of Excellence.* URL: https://www.newstrategycenter.ro/wp-content/uploads/2019/07/2017-nacsaugstrategijaen.pdf (date of access: 14.04.2025).

значними ресурсами та можливостями, а також мають чітко визначені цілі для здійснення діяльності в кіберпросторі. Другу групу складають кіберзлочинці, які діють незалежно, без державних вказівок чи наказів від спецслужб, і мають на меті отримання особистої фінансової або іншої вигоди в кіберпросторі. За даними Другого слідчого відділу Литви (The Second Investigation Department, далі – AOTD), найбільша кількість кіберінцидентів, спрямованих проти систем ADA та мереж литовських державних установ, припала на 2013 рік. Ці кібератаки були здійснені розвідувальними або безпековими службами іноземних держав чи пов'язаними з ними, контрольованими або підтримуваними ними організаціями. Найбільші кібернетичні можливості, спрямовані на збір інформації, порушення роботи систем та мереж ADA, їхнє захоплення або вплив, демонструють російські розвідувальні та безпекові служби, особливо структурні підрозділи Федеральної служби безпеки (далі – ФСБ).

У 2013 році в кіберпросторі також спостерігалася активізація контррозвідувальної діяльності. Протягом першого півріччя було задокументовано кіберінциденти, пов'язані з поширенням шпигунського програмного забезпечення. У системах ADA та мережах численних державних установ було виявлено шпигунську активність або її сліди. Виявлене відомством шкідливе програмне забезпечення та його нові модифікації призначені для збору даних з комп'ютера, віддаленого керування зараженим пристроєм, моніторингу мережі, виявлення облікових записів і паролів у мережі, а також для запису відео та аудіо. Встановлено, що шпигунське програмне забезпечення було інстальовано на комп'ютерах, що обробляли інформацію, пов'язану з внутрішньою та зовнішньою політикою Литви, внутрішньою безпекою, енергетичними проєктами, питаннями Європейського Союзу та головуванням Литви в Раді ЄС. Слід зазначити, що міжнародні

компанії, що працюють у сфері інформаційних технологій, у 2014 році виявили шпигунські програми (Snake rootkit, Turla, Uroburos), які використовувалися щонайменше з 2012 року. Найновіші версії цих шпигунських програм були зафіксовані AOTD. Додаток до звіту містить оновлену інформацію, що стосується версії шпигунського програмного забезпечення, яка була оприлюднена у звіті за 2012 рік. Це технічний аналіз шпигунського програмного забезпечення, який надає IT-спеціалістам компаній чи установ, а також приватним користувачам можливість перевірити комп'ютерні мережі їхніх організацій та персональні комп'ютери на наявність відповідних загроз. У 2013 році також було зафіксовано систематичне та інтенсивне сканування інтернет-мереж державних установ з метою розвідки. Головною метою цих дій був збір інформації про вразливості комп'ютерів або мереж, які могли б бути використані для несанкціонованого доступу, захоплення або іншої експлуатації.

У 2013 році кіберзловмисники не лише активно займалися шпигунством, але й втручалися в роботу інформаційних систем державних установ Литви. Це могло завдати шкоди національній безпеці та обороноздатності Литви. За наявною інформацією, у другій половині 2013 року відбувалися періодичні атаки на державні установи Литви. У 2013 році, окрім атак типу «відмова в обслуговуванні» (DDoS), спостерігалося зростання кількості заражених литовських веб-сайтів, ймовірно, внаслідок цілеспрямованих кібератак. Через це системи безпеки багатьох державних веб-сайтів були тимчасово недієздатними. Окрім того, внаслідок прямих кібератак спостерігалися збої в роботі різних інформаційних систем окремих державних установ. Зростання числа кібератак у другій половині 2013 року, порівняно з першою, ймовірно, було пов'язане з головуванням Литви в Раді ЄС, а також з осінніми російсько-білоруськими військовими навчаннями «Захід-2013» та

навчаннями НАТО «Steadfast Jazz 2013». Не виключено, що технічні несправності інформаційних систем, заражені веб-сайти та тимчасова непрацездатність систем безпеки литовських веб-ресурсів, а також інші інциденти можуть бути наслідком можливих кібератак на ці системи, причому цілі цих атак могли бути подвійними. Насамперед, кібератаки можна розглядати як цілеспрямовані дії, тобто атаки тривають до моменту успішного проникнення в атаковану систему (або системи), незалежно від повідомлень систем безпеки про відбиті спроби. З іншого боку, згадані атаки та інциденти також можуть розглядатися як широкомасштабна розвідувальна операція або підготовчий етап до фази проникнення. Мета таких дій може полягати не в завданні безпосередньої шкоди окремим системам чи пристроям, а в зборі інформації, яка в майбутньому може бути використана для проведення масштабної кібератаки. Слід зауважити, що у 2013 році, за винятком атаки на інтернет-портал Delfi, масштабних кібератак у Литві не відбулося. Однак, за інформацією, наявною в AOTD, щонайменше двічі планувалися атаки подібного характеру.

Особливо турбує мілітаризація Калінінградської області, яка безпосередньо межує з Литвою, що має стратегічне значення для Росії, забезпечує доступ до Балтійського моря, та дозволяє Росії проєктувати військову силу в регіоні. Російська сторона активно використовує Калінінград для проведення інформаційних операцій, спрямованих на дезінформацію та пропаганду, для того щоб зробити розкол серед населення[25]. До того ж акцентується увага на тому, що Росія може одночасно використовувати військові та гібридні тактики ведення війни проти Заходу, використовуючи «сірі зони» між війною та миром,

[25] Білоножко С. Західний вектор зовнішньої політики країн Балтії: шлях від незалежності до євроінтеграції. *Наукові праці історичного факультету Запорізького національного університету.* 2015. № 44 (2). С. 134.

проводячи приховані інформаційні операції, які важко прописати конкретному актору, що створює довгострокові наслідки для безпеки регіону.

У 2016 році Російська Федерація надавала підтримку поширенню книги Галини Сапожнікової, яка містила дезінформацію про роль Литовської Республіки у розпаді СРСР «The Lithuanian Conspiracy and the Soviet Collapse. Investigation into a Political Demolition». Незважаючи на це, книга була презентована в Італії, тоді як на території Литви авторці було заборонено в'їзд (персона non grata).

Що зазначалося ще раніше, це те, що у своєму річному посланні до Сейму Литви у 2014 році Президент Даля Грибаускайте зазначила, що російська анексія Криму радикально змінила геополітичну ситуацію в Європі, поставивши під сумнів фундаментальні принципи міжнародного права та безпеки: «останніми днями слова Свобода, Незалежність, Суверенітет, територіальна цілісність і Мир набули нового значення. Понад півстоліття Європа, що жила у мирі – і за це отримала Нобелівську премію, – знову зіткнулася з агресією. Війна і окупація стали вже не історичними термінами в підручниках, а реальною загрозою на європейському континенті. Переживаючи події, які відбуваються в Україні, ми знову переконалися, наскільки тендітна свобода….», тому «урок України – зобов'язання для всіх – з усієї сили вберегти свою свободу»[26].

Було встановлено, що країна серед балтійських, зокрема Литва, має подібне до України стратегічне бачення російської загрози, яка спричиняє значні зміни в системі євроатлантичної безпеки. Саме тому, Литва є важливим партнером України в забезпеченні національної та інформаційної безпеки,

[26] Нападиста В. "Україна в контексті викликів та загроз: погляд з країн Балтії". *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України.* С. 243-268.

оскільки вона послідовно підтримує євроатлантичні прагнення України та має спільні інтереси у протистоянні викликам безпеки, а також через її статус постраданської країни та членство в НАТО, має вразливість до методів гібридного та конвенційного впливу, які використовує Москва. Це пояснюється тим, що Литва є схильною до гібридних і конвенційних загроз, які виходять від Російської Федерації [27].

Паралельно з військовою загрозою, Литва стикається з проблемами ідеологічного впливу Росії та вербування молоді, особливо російськомовних меншин, російськими спецслужбами, що становить пряму загрозу національній безпеці, оскільки ці особи можуть бути використані для шпигунства, диверсій або поширення дезінформації.

Основними документами, що регулюють інформаційну безпеку в Литві, є: «Програма розвитку електронної інформаційної безпеки (кібербезпека), 2011-2019 pp.» (Resolution no 796 of 29 June 2011. On the Approval of The Programme for the Development of Electronic Information Security (Cyber Security 2011–2019), затверджений Урядом Литви 29 червня 2011 року, є основою для забезпечення безпеки кіберпростору країни, а також Закон «Про Кібербезпеку» (National legislation Cybersecurity Act (2014)) прийнятий у 2014 р., згідно з яким кібербезпека визначається як комплекс правових, організаційних та технічних заходів, спрямованих на запобігання, виявлення, аналіз та реагування на інформаційні загрози, а також відновлення працездатності систем управління електронних мереж зв'язку, інформаційних систем або промислових процесів у разі кібератак.

Говорячи про органи Литовської Республіки, що контролюють політику кібербезпеки, то, наприклад, відповідно до законодавства Литовської

[27] Jakniunaite, D. 2016. Changes in Security Policy and Perceptions of the Baltic States 2014–2016. *Journal on Baltic Security.* Vol. 2. No. 2. Pp. 6–35.

Республіки, організація, контроль та координація політики кібербезпеки покладені на Міністерство національної оборони. Центр кібербезпеки відіграє важливу роль у створенні законодавчої бази, яка забезпечить належне виконання функцій організаціями, що займаються захистом кіберпростору.

Відповідальність за впровадження політики кібербезпеки покладена на низку державних органів, серед яких Національний центр кібербезпеки, Державна інспекція захисту даних та Литовська поліція.

Уряд Литовської Республіки має значні повноваження у сфері кібербезпеки, затверджуючи ключові документи та процеси, що стосуються захисту цифрового простору країни. Зокрема, Уряд визначає Національну стратегію кібербезпеки, яка є дорожньою картою для всіх подальших дій, формує склад Ради з питань кібербезпеки, що свідчить про його роль у координації та управлінні, а також затверджує методику та перелік критичної інформаційної інфраструктури, включно з її керівниками, забезпечуючи захист найважливіших систем країни.

До повноважень Уряду також входить встановлення організаційних та технічних вимог до кібербезпеки для всіх відповідних суб'єктів, а поряд з цим – затвердження Національного плану управління кібербезпекою та контроль управління кризами у сфері кібербезпеки, підкреслюючи ключову роль у реагуванні на надзвичайні ситуації.

Міністерство національної оборони (далі – МНО) виступає головним координатором у процесі формування стратегічних документів у сфері інформаційної безпеки та встановлює норми та правила для учасників ринку безпеки даних; створює детальний план того, як діяти у разі кібератаки; визначає, які інформаційні системи є найважливішими і потребують особливого захисту; здійснює ідентифікацію критичної інформаційної інфраструктури, визначаючи її суб’єктів; затверджує типовий план управління

кіберінцидентами для таких об’єктів; затверджує план кіберзахисту критичної інформаційної інфраструктури; визначає порядок реагування на кіберінциденти в системах зв’язку та інформації суб’єктів кібербезпеки, а також затверджує план імплементації заходів технічної кібербезпеки та встановлює порядок управління інформаційними ресурсами й критичною інформаційною інфраструктурою.

МНО наділене повноваженнями розробляти та координувати реалізацію політики кібербезпеки Литовської Республіки. Ці функції покладено на новостворений департамент кібербезпеки та інформаційних технологій.

Стосовно суб’єктів кібербезпеки, то відповідно до законодавства, на суб’єктів кібербезпеки покладаються певні обов’язки, проте ці вимоги не поширюються на малі та дуже малі підприємства, визначені Законом про розвиток малого та середнього бізнесу. Серед суб’єктів варто виокремити:

1) суб’єкт господарювання, який здійснює управління та контроль державних інформаційних ресурсів;

2) спеціаліст з управління критичною інформаційною інфраструктурою;

3) фахівець, який відповідає за планування, організацію та контроль за захистом інформаційних систем, що мають критичне значення для функціонування держави або суспільства;

4) компанія, що забезпечує доступ до мережі для широкого кола користувачів;

5) постачальники цифрових послуг.

Литва демонструє непогані результати у боротьбі з пропагандою та інформаційними погрозами. Згідно з опитуванням, проведеним дослідницькою компанією Spinter у травні 2018 року, близько половини мешканців Литви (49%) помічають пропаганду у ЗМІ, а 38% опитаних стверджують, що можуть відрізнити неправдиву інформацію.

Отже, російські спецслужби ще до початку повномасштабного вторгнення значно активізували свою діяльність у балтійському регіоні. Вони використовували широкий спектр методів, включаючи вербування агентів з числа місцевого населення, таких як підприємці, журналісти, науковці та дипломати, з метою збору розвідувальної інформації та здійснення впливу на політичні процеси в країнах Балтії. Уряд Росії залучає мешканців регіону до збройних конфліктів на Донбасі, як це було продемонстровано на прикладі громадян Естонії та Латвії, яких звинуватили у тероризмі на боці сепаратистів.

Країни Балтії розробили комплексні та всеохоплюючі стратегії для забезпечення кібербезпеки. Стратегії забезпечують комплексний підхід до інформаційної безпеки, охоплюючи економічний, соціальний, правовий та військовий виміри. За підтримки НАТО країни Балтії прагнуть гармонізувати національне законодавство у сфері кібербезпеки, щоб створити спільну міжнародно-правову основу для запобігання конфліктам, що можуть виникнути через використання інформаційно-комунікаційних технологій. Вони усвідомлюють тісний зв'язок між кібербезпекою та національною безпекою, розуміючи, що кібернетичні загрози, такі як атаки на інформаційно-комунікаційні системи або критичну інфраструктуру, можуть підірвати національну безпеку та економічну стабільність держави.

Всі три держави активно працюють над захистом свого кіберпростору, розглядаючи його як частину національної безпеки, та надають пріоритет захисту критичної інфраструктури як ключовому елементу національної безпеки. Саме такий підхід зумовлює застосування силових методів для забезпечення кібербезпеки, оскільки вони вважаються найбільш ефективними. Необхідно підкреслити, що країни у своїх стратегіях кібербезпеки окремо визначають внутрішні та зовнішні джерела кіберзагроз, наголошуючи на їх різному характері. Усі країни розробляють власні стратегії кібербезпеки, які,

як правило, передбачають посилення військового компонента в сфері кіберзахисту. Ця тенденція виводить питання кібербезпеки на рівень національної безпеки та зосереджується насамперед на захисті державних інформаційно-комунікаційних ресурсів. У зв'язку з цим, саме силові відомства несуть основну відповідальність за нейтралізацію кібернетичних загроз.

РОЗДІЛ 3
ВПЛИВ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ КРАЇН БАЛТІЇ

3.1. Загрози інформаційній безпеці країн Балтії після повномасштабного вторгнення Росії в Україну

Після того, як Російська Федерація розв'язала повномасштабну війну проти України, інформаційна безпека країн Балтії та всієї світової спільноти зіткнулася з безпрецедентними викликами та загрозами. У контексті розгортання війни на різних рівнях – від традиційних бойових дій до гібридних стратегій – цифровий простір перетворився на арену боротьби за вплив, маніпулювання інформацією та дестабілізацію. Росія прагне дискредитувати балтійські країни, дедалі частіше звинувачуючи їх у переписуванні історії, пропагуванні нацизму та поширенні русофобії.

Починаючи з лютого 2022 року спостерігалося зростання всіх типів кібератак, включаючи саботаж, кібершпигунство, фінансове шахрайство та політично-мотивовані атаки. З точки зору національної безпеки Балтійських країн, найбільш серйозні загрози включали різні спроби вторгнення, фішингові кампанії, розподілені атаки на відмову в обслуговуванні, а також атаки на ланцюги поставок і операційні технології, та саме через це країни Балтії з перших днів війни активно засуджують російську агресію проти України, надаючи їй стабільну політичну, військову, гуманітарну та фінансову допомогу.

З початку російської агресії Естонія надала Україні військово-технічної допомоги на суму понад 400 мільйонів євро, що перевищує 1% ВВП країни. За обсягом військової допомоги у перерахунку на душу населення Естонія є одним з лідерів.

Естонські державні установи та постачальники критичних послуг також є одними з головних об’єктів російського кібершпигунства після початку повномасштабного вторгнення. У листопаді 2022 року зафіксовано кібератаки, об'єктами яких стали організації у п'яти східноєвропейських державах (Естонії, Польщі, Румунії, Болгарії та Молдови), зокрема зовнішньополітичні дослідницькі установи та розвідувальні відомства. Через декілька днів, 19 листопада кібератаки призвели до збоїв у роботі п'яти естонських компаній, серед яких була енергорозподільча група «Eesti». Естонським управлінням інформаційних систем що хоча остаточно встановити винних неможливо, наявні дані вказують на прокремлівських кіберзлочинців[28].

Саме 2024 рік став вирішальним, оскільки Естонія публічно приписала кібератаку Головному розвідувальному управлінню Генерального Штабу Росії (далі – ГРУ), яка ще у 2020 році отримала доступ до десятків тисяч загальнодоступних документів із позначкою «лише для службового користування» та залишалася активною. Попри те, що ці документи не містили державної таємниці, аналітики ГРУ зібрали інформацію з фрагментів документів «лише для службового користування» щоб отримати висновок про інформацію, яка в Естонії є державною таємницею. У зв’язку з цим, естонський Департамент поліції безпеки (Kaitsepolitseiamet) (далі – КаПо[29]) видав звіт, в якому 14% обсягу припадало на аналіз загроз конституційному ладу, включаючи російські спроби підривної діяльності в інформаційному просторі та спотворення історичної пам'яті.

---

[28]CERT-EU. “DDoS-атаки на зовнішньополітичні аналітичні центри та розвідувальні служби”. 2022. URL: https://www.cert.europa.eu/publications/threat-intelligence/cb22-12/?utm_source=chatgpt.com (date of access: 21.04.2025).

[29]Riigi Portaal.Riigi sisejulgeoleku tagamine. 2024 URL: https://www.eesti.ee/eraisik/ru/artikkel/bezopasnost-i-oborona/bezopasnost/obespecenie-bezopasnosti-vnutri-gosudarstva (date of access: 21.04.2025).

Протягом квітня 2025 року прокремлівські дезінформатори активніше поширювали неправдиву інформацію, спрямовану на дискредитацію демократичних інститутів, конституційного порядку та політики національної безпеки Естонії. Основні теми розповідей стосувалися ймовірної державної підтримки дискримінації, цензури, мілітаризації та неефективного економічного управління. Прокремлівські джерела представляли військову ініціативу як провокацію НАТО, що несе загрозу миру в регіоні. Вони підкреслювали невдоволення місцевого населення відсутністю прозорості та соціальними витратами мілітаризації, зображуючи Естонію як «маріонетку» Заходу в його політиці залякування Росії [30].

Через ці загрози та дезінформацію, до Закону Естонської Республіки про інформаційну безпеку та кібербезпеку було внесено зміни у зв'язку із зростаючою інформаційною вразливістю, що почалася у лютому 2022 року.

У 2024 році Естонія та партнери офіційно започаткували Таллінський механізм з метою спільної координації та посилення підтримки цивільної кібербезпеки в Україні. До цього механізму входять Канада, Данія, Естонія, Франція, Італія, Німеччина, Нідерланди, Польща, Швеція, Україна, Велика Британія та Сполучені Штати Америки. Європейський Союз та НАТО підтримували цю ініціативу та брали участь у ній як спостерігачі з моменту її створення. Талліннський механізм слугував платформою для координації допомоги Україні, спрямованої на підтримку та зміцнення її національної кібербезпеки та кіберстійкості, захист критичної інфраструктури та запобігання російським кібероперація̈м.

[30] Lithuania Monthly: Real Estate Tax Protest Becomes a Tool for Kremlin's Disinformation. *Civic Resilience Initiative – Baltic Disinformation.* 2025. URL: https://balticdisinfo.eu/ (date of access: 21.04.2025).

Національним органом з сертифікації в галузі інформаційної безпеки у значенні статті 58 Регламенту Європейського парламенту та Ради про ENISA (Агентство Європейського союзу з кібербезпеки) та про сертифікацію в галузі кібербезпеки інформаційних та комунікаційних технологій та безпеки)[31] є Орган із захисту прав споживачів та технічного нагляду. Якщо інформація, розповсюджена серед громадськості за допомогою послуги інформаційного суспільства, розпалює ненависть, насильство або дискримінацію за ознакою національності, етнічного походження, мови, релігії або інших обставин, зазначених у статті 12 Конституції Естонської Республіки, підбурює до війни або необхідне для запобігання загрозі, Департамент захисту прав споживачів та технічного нагляду має право винести розпорядження постачальнику послуги інформаційного суспільства та вимагати видалення інформації, наданої за допомогою послуги інформаційного суспільства, або обмеження доступу до інформації з урахуванням особливостей.

Естонська держава у 2024 році також представила на громадське обговорення проєкт, розроблений відповідно до плану ЄС щодо гармонізації стандартів інформаційної безпеки. У проєкті визначено кіберзагрози, пов'язані зі зростанням цифровізації, та запропоновано заходи для їх запобігання. The security of Network and Information Systems (далі – NIS), яка набула чинності у 2016 році, першочергово стосувалася компаній, що забезпечують функціонування критичної інфраструктури, а також постачальників цифрових послуг, включаючи онлайн-ринки, пошукові системи та хмарні сервіси, такі організації, як постачальники послуг у транспортній галузі (залізничний, авіаційний та морський транспорт), компанії зв'язку, медичні установи, банки

[31] Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки. С. 15–69.

та державні органи (Міністерства та місцеві адміністрації з їхніми дочірніми підприємствами). Директива NIS започаткувала перше загальноєвропейське законодавство з інформаційної безпеки, яке держави-члени ЄС мали впровадити в національне право до 9 травня 2018 року. 16 січня 2023 року набула чинності NIS2, яка остаточно замінила попередню Директиву про безпеку мереж та інформаційних систем (NIS) 17 жовтня 2024 року.

Директива NIS2 мала на подальшій меті посилити кібербезпеку в ЄС через налагодження дієвої системи управління кіберкризами, уніфікацію вимог до безпеки та звітності, а також запровадження базового рівня заходів з управління кіберризиками та відповідних обов'язків для всіх охоплених секторів. Директива NIS2 регулює обмін інформацією щодо кібербезпеки та використання ресурсів у надзвичайних ситуаціях як на національному, так і на європейському рівні.

З набранням чинності NIS2 збільшилася кількість організацій, зобов'язаних дотримуватися вимог інформаційної безпеки, передбачених відповідним законом, що спричинить додаткові витрати часу та ресурсів. Закон про внесення змін до Закону про кібербезпеку та інші закони[32] застосовується до установ, що надають критично важливі послуги на території Європейського Союзу, а для того, щоб допомогти компаніям визначити, чи підпадають вони під дію Закону про кібербезпеку, держава планує розробити відповідний інструмент на момент набрання чинності законом. Після цього у нових компаній три роки на виконання вимог кібербезпеки. На додаток, держава

[32] Закон про внесення змін до Закону про кібербезпеку та інші закони (транспонування 2-ї Директиви про кібербезпеку). *Eelnõude infosüsteem*. 2024. URL: https://eelnoud.valitsus.ee/main/mount/docList/c774c2e2-0c3e-4137-b24b-b49d1249f326#iTp8S0dP (дата звернення: 01.04.2025).

надає гранти, методичні матеріали та інструменти для полегшення впровадження вимог кібербезпеки, передбачених Директивою NIS2.

Також було внесено зміни до Закону про публічну інформацію[33], завданням якого є забезпечення загального доступу громадян та кожної людини до публічної інформації, відповідно до принципів демократичної, соціальної та правової держави, а також відкритого суспільства. Водночас, Закон має на меті створити можливості для громадського нагляду за виконанням державних обов'язків. На додаток, до Закону про кібербезпеку у липні 2022 році було прийнято законодавство про внесення змін. Пункт 2 статті 1 отримав формулювання, що з 2022 року Закон не регулює обробку державних секретів та секретної інформації іноземних держав, а також функціонування систем, що використовуються для їх обробки; функціонування систем, необхідних для міжнародного військового співробітництва та забезпечення військової готовності держави у сфері компетенції Міністерства оборони. Для виконання визначених обов'язків та гарантування кібербезпеки систем, Уряд Республіки або уповноважений міністр своєю постановою затвердив: вимоги до управління інформаційною безпекою, відомі як E-ITS; загальні вимоги до заходів безпеки; а також спеціальні вимоги до заходів безпеки для різних систем та сфер їх застосування.

У грудні 2024 року було внесено зміни до Закону Естонії «Про Уряд Республіки»[34], де Міністерство юстиції та цифрових технологій відповідає за забезпечення якості законотворчого процесу та його координацію, розробку та впровадження правової політики, зменшення бюрократичних перешкод,

[33] Riigi Teataja. Avaliku teabe seadus. *Riigikogu.* 2025. PP. 13-25.
[34] Закон про внесення змін до Закону про Уряд Республіки та пов'язаних з цим поправок до інших законів: Закон від 01.01.2025 № 499. URL: https://www.riigiteataja.ee/akt/130122024001 (date of access: 17.04.2025).

систематизацію законодавства та видання Державного вісника, а також питання захисту даних, планування та координацію впровадження політики цифрового суспільства, узгодження розвитку державних електронних сервісів та створення їхньої уніфікованої платформи, сприяння розвитку цифрових навичок, проєктування та координацію державних інформаційних систем, включно з політикою у сфері даних та координацію розвитку центральної мережі та інформаційних систем.

Розглядаючи наступну Балтійську країну – Латвію, то вона сама пройшла через роки радянської окупації та боротьбу за незалежність, з особливою гостротою сприйняла агресію проти суверенної європейської держави. Її реакція була миттєвою та багатогранною. На політичному рівні Латвія одразу ж зайняла чітку та безкомпромісну позицію, рішуче засудивши дії Росії як грубе порушення міжнародного права та акт неспровокованої агресії. Голос Латвії лунав потужно на міжнародних майданчиках, закликаючи до консолідованої відповіді світової спільноти, посилення санкцій проти агресора та надання всебічної підтримки Україні.

9 квітня 2024 року Кабінет міністрів Латвії [35] ухвалив рішення підтримати підписання Угоди між Латвійською Республікою та Україною про довгострокові зобов'язання щодо підтримки та безпеки. Угода підтвердила рішучу та непохитну підтримку Латвією безпеки України. Вона передбачала надання всебічної військової та невійськової допомоги Україні в її боротьбі з агресором, а також підтримку Латвією прагнення України до членства в Європейському Союзі та НАТО.

---

[35] Офіційне інтернет-представництво Президента України. Угода між Латвією та Україною про довгострокову підтримку та зобов'язання з безпеки. 2024. URL: https://www.president.gov.ua/news/ugoda-mizh-ukrayinoyu-ta-latvijskoyu-respublikoyu-pro-dovgos-90189 (дата звернення: 30.04.2025).

Угода закріплювала зобов'язання Латвії надавати Україні військову підтримку в обсязі 0,25% від ВВП до 2026 року, продовжуючи таким чином цілеспрямовану військову допомогу, яку Латвійська держава надає з першого дня війни у 2022 році. Угода визначає конкретні напрями військової підтримки, включаючи участь у очолюваній Латвією Коаліції безпілотників, постачання військової техніки та озброєння, а також навчання військовослужбовців.

Внаслідок цього Росія почала активніше розносити дезінформацію у Латвійській Республіці. Наприклад, в країні спостерігалося широке поширення невоєнних змов та сфабрикованих історій. У Латвії та Литві поширювалися фейкові заяви про те, що землетруси в Сирії та Туреччині були навмисно спричинені США «кліматичною зброєю» з метою дискредитації низки організацій та осіб. Рішення про створення в Селії нового військового полігону, що мало збільшити військову присутність НАТО в Латвії, стало об'єктом поширення інформації з боку проросійських латвійських політиків на дезінформаційній арені. Інтернет-тролі та окремі місцеві політики вбачали в цьому доказ залежності Латвії від США у прийнятті рішень, а також підтвердження її намірів щодо військового конфлікту з Росією.

У 2023 та 2024 роках Росія також продовжувала становити головну інформаційну загрозу латвійським установам і суспільству. Підтримка України Латвією є вагомим додатковим мотивом для ворожих кібератак. Діяльність ворогуючих держав та інших кіберакторів здійснювалася хвилеподібно, що призвело до обмеженого збитку. Атаки не спричинили значних і тривалих наслідків, підтверджуючи, що латвійський кіберпростір добре захищений.

Спостерігаючи за цим, Латвія також вирішила посилити свою безпеку в інформаційному просторі, тому вже 28 вересня у 2023 році на засіданні Сейму схвалила Концепцію національної безпеки. Концепція мала на меті

нейтралізацію загроз, які прямо або опосередковано впливають на національну безпеку Латвії. Ці загрози включають розвиток ситуації у сфері міжнародної безпеки, війну Росії в Україні, гібридні загрози, зловмисну кібердіяльність та тенденції міжнародного тероризму. З 2023 року Концепція визначає загальні пріоритетні напрямки запобігання цим загрозам у кожній відповідній сфері. Розробка політики органами державної влади, планування та здійснення заходів, а також взаємодія у сфері забезпечення національної безпеки мають базуватися на пріоритетах, визначених у Концепції.

Незважаючи на прийняття рішень для посилення інформаційної безпеки, Росія продовжувала намагатися послабити авторитет латвійського населення.

Було кілька публічних заходів, під час яких слід було очікувати кібератаки та інформаційні розбіжності з боку РФ. Перед виборами до Європейського парламенту 8 червня 2024 року проросійські акаунти Telegram закликали людей зірвати виборчий процес у Латвії та інших країнах Європи, але жодних інцидентів, безпосередньо пов’язаних із виборчими системами чи безпекою виборів, не спостерігалося. Так само не було зафіксовано значних проблем під час третього парламентського саміту Міжнародної Кримської платформи 24 жовтня 2024 року.

Політично вмотивовані розподілені атаки на відмову в обслуговуванні російськими хакерськими групами стали невід’ємною частиною латвійського інформаційного простору. Ці атаки покликані помститися за політичні рішення Латвії та підтримку України, порушити роботу державних і приватних установ, спричинити плутанину та незручності у повсякденному житті жителів. У 2024 році Латвія пережила кілька хвиль таких атак після візиту президента України Володимира Зеленського до столиці Латвійської Республіки – Риги, чи заяв латвійського уряду щодо додаткової підтримки, зокрема військової, Україні. Атаки здебільшого були спрямовані на державні

установи та конкретні компанії (постачальники послуг електронного зв'язку, транспортні компанії, енергетичний сектор).

Разом з тим, рішення Національної ради з електронних ЗМІ було змінено в 2025 році щодо обмеження доступу до російських сайтів: sfr.gov.ru; 74.ру; mgimo.ru; www.dp.ru; don24.ru; krd.ru; artek.org. Національна рада з електронних засобів масової інформації (далі – Рада), під головуванням Іварса Аболіньша, за участі заступниці голови Єви Калдераускі та членів Ілви Мілзари й Андіса Плаканса, провела розгляд звіту про перевірку російських каналів та сайтів, а також інформації, отриманої від компетентного державного адміністративного органу. Під час перевірки вказаних веб-сайтів (результати якої відображено у звіті про перевірку Департаменту моніторингу Ради України від 12 грудня 2024 року та в листі уповноваженого органу від 9 лютого 2025 року), було встановлено, що ці веб-сайти поширюють викривлену та неправдиву інформацію про події у світі, зокрема про війну в Україні, виправдовують російське вторгнення та анексію українських територій. Зазначено, що поширення подібної інформації в латвійському інформаційному просторі може призвести до спотворення сприйняття світових подій, негативно позначитися на злагоді між різними групами суспільства та становити загрозу національній безпеці Латвії. У рішенні також деталізується характер інформації, яка розміщується на зазначених веб-сайтах [36].

Під час засідання Ради 22 січня 2025 року було проведено аналіз контенту, що поширюється на згаданих веб-сайтах. Частина перша статті 112 Закону про

[36] Про обмеження доступу до сайтів *sfr.gov.ru; 74.ру; mgimo.ru; www.dp.ru; don24.ru; krd.ru; artek.org*: Рішення від 23.01.2025 № № 111/2019. URL: https://likumi.lv/ta/id/358232-par-piekluves-ierobezosanu-timekla-vietnem-sfrgovru-74ru-mgimoru-wwwdpru-don24ru-krdru-artekorg (дата звернення: 02.05.2025).

електронні комунікації[37] визначає, що «Національна рада з електронних ЗМІ, оцінивши інформацію, надану державними установами, має право ухвалити рішення про обмеження доступу до веб-сайтів, доступних на території Латвії, які поширюють контент, що загрожує або може загрожувати національній безпеці або громадському порядку та безпеці, шляхом заборони доступу до доменного імені або адреси інтернет-протоколу (IP) цих». Згідно з вищезазначеною нормою закону, Рада має право, на основі оцінки інформації, отриманої від інших державних адміністративних органів, ухвалювати рішення про обмеження доступу до веб-сайтів, якщо розміщений на них контент становить загрозу або може становити загрозу національній безпеці чи громадському порядку та безпеці.

Литва також відіграла важливу роль у підтримці України під час російської військової агресії, блокування Чорного та Азовського морів і мілітаризацію Чорноморського регіону загалом. Рішуча та ефективна підтримка України з боку Литви особливо яскраво проявилася з початком повномасштабного вторгнення РФ 24 лютого 2022 року. З перших днів повномасштабної війни Литва активно надає Україні значну політичну підтримку, практичну допомогу, включаючи військово-технічну, інформаційну та макрофінансову.

За ініціативою, зокрема, Литви, у квітні 2022 року було сформовано Спільну слідчу групу для розслідування воєнних злочинів та злочинів проти людяності, скоєних на території України, в діяльності якої активно залучені представники Литви.

Проте російська пропаганда проти Литви з моменту повномасштабного вторгнення зосереджена на звинуваченнях в історичному ревізіонізмі,

---

[37] Закон про електронні комунікації. Стаття 112. *Права Національної ради з електронних ЗМІ.* 2022. URL: https://likumi.lv/ta/id/334345-elektronisko-sakaru-likums#p112 (дата звернення: 02.05.2025).

підтримці нацистської ідеології та розпалюванні русофобії. Оцінюється, що Кремль прагне заплямувати імідж Литви на міжнародній арені, виправдати геополітичні інтереси Росії в регіоні та дискредитувати антирадянський опір Литви.

Велика та скоординована мережа російських інструментів пропаганди, що складається з контрольованих державою ЗМІ, соціальних мереж і проросійських веб-сайтів, забезпечує поширення наративів, які дискредитують Литву. Оцінюється, що Росія найактивніше використовує додаток Telegram для проведення своїх пропагандистських і дезінформаційних кампаній. Для підтримки поширення пропаганди російські інформаційні політики використовують ботів (автоматизовані профілі) і мережі тролів, а також таргетовану рекламу. Кампанії з дезінформації зазвичай проводяться за перевіреною моделлю: початкова провокаційна інформація розміщується на незрозумілому веб-сайті або в обліковому записі в соціальних мережах, а потім поширюється через відомі канали Telegram із великою кількістю підписників, таким чином посилюючи його охоплення. Для охоплення ширшої аудиторії інформація може бути перекладена кількома мовами.

Розглядаючи інциденти, 9 травня 2024 року в Литві затримали двох осіб, відомих своєю антинатовською позицією. Пізніше ця інформація була на російських новинних веб-сайтах і проросійських литовських веб-сайтах. Ключовим елементом інформаційної політики Росії проти Литви є представлення її як однієї з найбільш ворожчих до Росії країн Європи. Цей наратив в основному базується на твердженні про те, що Литва дискримінує російськомовних людей і прагне маргіналізувати прихильників Росії, незалежно від їхньої національності. Росія проводить паралелі між налаштуванням литовців проти Росії та геноцидом, що свідчить про те, що

росіяни в Литві та інших країнах Балтії наразі переживають те ж саме, що робили євреї під час Другої світової війни.

У зв’язку з тим, що у 2022 році Російська Федерація вкотре грубо порушила міжнародне право та міжнародні договори, включаючи Мінські угоди, а також фальсифікує інформацію, Сейм Литовської Республіки «Про агресію Росії та Білорусі проти України»[38] в кінці лютого 2022 року вніс зміни у законодавство, та закликав держави-члени ЄС та Раду ЄС взяти на себе міжнародне лідерство у справі об'єднання всіх держав демократичного світу для підтримки України та прагнути до того, щоб якнайбільше держав світу приєдналися до санкцій проти російського та білоруського режимів. Було закликано до зміцнення стійкості суспільств ЄС та НАТО до гібридних загроз, що походять від ворожих країн та їх спецслужб. Парламент Литовської Республіки звернувся до парламентів своїх союзників – держав-членів Європейського Союзу та НАТО – із закликом зберегти та розширити заборону на передачу будь-яких стратегічно важливих даних та інформацію до Росії та Білорусі.

За оцінкою загроз національній безпеці у литовському звіті за 2021-2025 роки «Gresmiu Nacionaliniam Saugumui Vertinimas»[39], Литва стикається зі спробами кібервпливу на свої важливі рішення. Серед найактивніших ворожих сил у кіберпросторі виділяються хакерські групи, що мають зв'язки з Росією та Китаєм, які першочергово націлені на тривалий і безперервний збір даних про зовнішню та внутрішню політику держави. Зловмисники в кіберпросторі прагнуть проникнути в ІТ-інфраструктуру державних органів, організацій і

[38]Про агресію Росії та Білорусі проти України: Проєкт резолюції від 02.02.2022 № XIVP–1350.URL:https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/cf09e8b0957811ec9e62f960e3ee1cb6 (дата звернення: 03.05.2025).

[39] Lietuvos Respublikos Valstybes Saugumo Departamentas. *Grėsmių Nacionaliniam Saugumui Vertinimas.* Vilnius, 2025. P. 40–47.

підприємств, щоб викрасти важливу інформацію та отримати технічні відомості про їхній стан, структуру та слабкі місця. Крім того, спостерігаються зусилля зі створення інструментів для довготривалого несанкціонованого доступу. За останні роки в литовському кіберпросторі було виявлено нові групи, що координуються спецслужбами недружніх країн, які характеризуються агресивними діями, зокрема руйнівними атаками.

Литва здійснює комплекс заходів, спрямованих на підготовку до мобілізації необхідних державних ресурсів, одночасно зміцнюючи кібернетичну безпеку, охорону критичної інфраструктури та боротьбу з дезінформацією та пропагандою. З огляду на інтенсивність інформаційних атак, які Литва зазнає з боку Російської Федерації та Білорусі, це питання є вкрай актуальним. Протягом 2023 року литовськими оборонними відомствами було виявлено понад 3,5 тисячі ворожих інформаційних впливів. Поширені пропагандистські тези включають звинувачення Литви та НАТО у провокаціях щодо Росії та Білорусі, а також твердження про начебто існуючі плани держав-союзників щодо військового нападу на Російську Федерацію. Пропагандистські зусилля також мали на меті знецінити військовий потенціал Альянсу та Литви, а також дискредитувати економічну й військову підтримку, яку західні держави надають Україні.

Таким чином, проведений огляд змін у законодавстві країн Балтії після початку повномасштабного вторгнення Росії в Україну демонструє рішучу та згуртовану реакцію цих держав на агресію. Спільними рисами законодавчих змін є посилення національної безпеки та оборони, запровадження санкцій проти Росії та Білорусі, підтримка України та українських біженців, а також протидія російській пропаганді та дезінформації.

3.2. Реакція країн Балтії на нові виклики та загрози в умовах російсько-української війни

Представники країн Балтії зазначають, що спостерігаючи за стражданнями українського народу, вони з болем усвідомлюють, наскільки подібними є методи російської агресії до тих, які застосовувалися під час радянської окупації їхніх країн. Балтійські дипломати зазначили, що страждання українців, спричинені депортаціями, тортурами та викраденнями дітей, викликали в їхніх країнах глибокий резонанс та «культурне стирання», оскільки вони нагадують про «власні найтемніші спогади та страхи» в історії.

Російський режим, очолюваний Путіним, продовжує вважати країни Балтії своєю винятковою сферою геополітичного впливу, прагнучи повернути їх під свій контроль. У новітній геополітичній ситуації Естонія, Латвія і Литва зіткнулися із серйозними викликами безпеці, зокрема через присутність на їх територіях значних російських етнічних і російськомовних громад. Основними інструментами російської політики в регіоні є дестабілізаційні дії, такі як проєкти, спрямовані на розвиток культурного та освітнього співробітництва з Росією, фінансуються, зокрема дестабілізаційні заходи, які вживає Росія, включають підтримку лояльних до неї організацій та кібернетичні атаки на урядові сайти та об'єкти критичної інфраструктури, дискредитація балтійських країн на міжнародній арені та підтримка проросійських політичних сил є частиною російської стратегії впливу в регіоні [40].

Представники країн Балтії наголосили на необхідності бути готовими до того, що «екзистенціальна загроза» їхній незалежності може бути замаскована

[40]Martyniuk O. V. Foreign experience in the formation and implementation of state policy in the field of state border security. *Public management and administration in Ukraine*. 2024. No. 44. P. 163–166. URL: https://doi.org/10.32782/pma2663-5240-2024.44.27 (date of access: 15.05.2025).

під «гібридні атаки», зокрема, масштабні кібератаки та дезінформаційні кампанії. В умовах, що склалися, нерішучість рівнозначна поразці. Тому країни Балтії та їхні союзники повинні бути готові до швидкої, переконливої та ефективної відповіді на будь-які види загроз.

Державні та приватні органи країн Балтії активно працюють з 2022 року над підвищенням обізнаності населення у сфері інформаційної безпеки, проводячи різноманітні інформаційні кампанії та навчальні заходи. У контексті реакції країн Балтії на нові політичні проблеми, покладаючись на рішення Національної ради з електронних ЗМІ щодо обмеження доступу до російських сайтів, у квітні 2023 року Естонський регулятор TTJA (Consumer Protection and Technical Regulatory Authority of Estonia) заблокував доступ до 53 онлайн-платформ, через які транслювалися російські телеканали, що потрапили під санкції ЄС. Для захисту свого інформаційного поля та дотримання санкцій Європейського Союзу Естонія заблокувала трансляцію 51 російського телеканалу та доступ до 195 веб-сайтів, які їх ретранслювали. Крісті Тальвінг – генеральний директор TTJA повідомила, що опитування на замовлення Державної канцелярії показало значне зниження за рік як згадування російських телеканалів серед важливих джерел інформації (з 33% до 11%), так і довіри до них (з 40% до 18%), що свідчить про ефективність заходів із захисту інформаційного простору Естонії.

Уповноважені органи Естонії також заявили про продовження контролю за телевізійними каналами та інтернет-платформами, що можуть транслювати російські телеканали, які знаходяться під санкціями. TTJA зобов'язав операторів телебачення припинити трансляцію низки російських та білоруських телеканалів ще 25 лютого 2022 року, пояснивши це рішення тим, що канали поширювали заборонену інформацію. Оператори телевізійних послуг отримали наказ негайно припинити трансляцію каналів «РТР

Планета», «НТВ Мир», «НТВ Мир Балтик», «Білорусь 24», «Росія 24» (ВДТРК) та «ТВ Центр International» (TVCI). Департамент ліцензував діяльність телеканалів «Канал 7», «Канал 7+», «Кіно 7», «Орсент ТВ», OTV, «Сімейка», Super Baltic, Super Plus та «3+ Естонія». Крім того, Естонське національне телерадіомовлення має свій російськомовний канал ETV+[41].

Як зазначалося раніше, 20 грудня 2023 року з ініціативи Естонії, 11 країн, включаючи США та більшість країн ЄС, запустили новий механізм співпраці – Талліннський, спрямований на посилення кібербезпеки. Запуск Талліннського механізму є результатом спільних зусиль кількох держав, спрямованих на зміцнення кібербезпеки України в умовах російської агресії, через те, що є розуміння, що боротьба України – це не лише виживання України, а й безпека всього Балтійського регіону та Європи. Основна мета – об'єднати зусилля міжнародних партнерів для посилення кібербезпеки України, захисту критичної інфраструктури та протидії російським кібероперація̈м. Новий механізм не лише доповнить існуючі зусилля з кібербезпеки, а й розширить коло учасників, залучаючи неурядові організації та приватний бізнес для спільного захисту критичної інфраструктури України.

Щодо появи нових платформ в країнах Балтії у зв'язку з російсько-українською війною, то безпосередньо нових великих платформ, створених саме через війну не з'явилося, а існуючі цифрові інфраструктури, стратегії та платформи (Латвійське агентство інвестицій та розвитку (LIAA), Національна стратегія розвитку інформаційного суспільства (Стратегія HICO), Балтійський центр боротьби з інформаційними порушеннями (BECID)), в країнах Балтії й наразі використовуються для боротьби з дезінформацією, для

[41]Republic of Estonia. Consumer Protection and Technical Regulatory Authority. 2022. URL: https://ttja.ee/ru/novosti/ttja-prinyal-reshenie-o-zaprete-translyacii-pyati-telekanalov-na-territorii-estonskoy (date of access: 07.04.2025).

підтримки України та посилення національної безпеки в умовах війни, європейські спецслужби практично одностайно констатують зростання активності російської агентури. При цьому спостерігається чітка закономірність: реакція на безпекову та інформаційну загрозу тим спокійніша, чим далі географічно розташована країна від Росії, втім, це правило має винятки. Деякі країни стикаються з такими специфічними ризиками, які в Україні можуть здатися навіть анекдотичними.

3.3. Напрями та перспективи розвитку сфери інформаційної безпеки країн Балтії

Росія стала ще активніше використовувати інформаційні кампанії та дезінформацію для маніпуляції громадською думкою в країнах Балтії після початку повномасштабного вторгнення в Україну та намагається підривати політичну стабільність в регіоні. Відповідно, стратегії країн Балтії у боротьбі з дезінформацією були значно посилені.

Опитування, проведене на замовлення Європейського парламенту з 19 квітня по 16 травня 2022 року, охопило 26 578 респондентів у 27 країнах-членах ЄС, яке проводилося особисто, з можливістю онлайн-інтерв'ю за потреби, та результати були зважені з урахуванням чисельності населення кожної країни ЄС показало, що у зв'язку з війною Росії проти України європейці стали сильніше підтримувати Європейський Союз. Особливо помітне зростання підтримки ЄС у Литві, яке почалося в 2022 році. Результати опитування свідчать, що 65% європейців позитивно оцінюють членство своєї країни в ЄС, що є найвищим показником з 2007 року. При цьому у більшості країн-членів, за винятком Греції та Словаччини, абсолютна більшість громадян підтримує членство в ЄС.

У Литві відзначено найбільший приріст підтримки ЄС порівняно з результатами осені 2021 року (на 20 процентних пунктів), досягнувши 82%. Литовці демонструють високий рівень схвалення членства своєї країни у Європейському Союзі та відрізняються відсутністю негативного ставлення до ЄС, хоча 17% населення зберігають нейтралітет щодо членства країни в Європейському Союзі. У середньому Європою 52% громадян позитивно ставляться до ЄС, а 12% – негативно.

Останні події суттєво вплинули на сприйняття європейцями великих зарубіжних країн: позитивне ставлення до Росії висловили лише 10% громадян ЄС, що на 30 відсотків менше, ніж у 2018 році. До Китаю позитивно належать 22% резидентів ЄС. У той же час, прихильність до Сполученого Королівства та Сполучених Штатів серед європейців значно зросла, досягнувши 65% та 58% відповідно. У Литві позитивне ставлення до Росії висловили лише 5% опитаних, а до Китаю – 25%. Найбільш високу оцінку литовці дали Великобританії (86%) та Сполученим Штатам Америки (81%).

На додаток, опитування показало, що литовці довіряють своїй армії та військовій професії, готові захищати свою країну, розраховують на підтримку союзників і позитивно ставляться до їхньої присутності у Литві. 90% опитаних схвалюють членство Литви в НАТО, більше половини (52%) готові брати участь у збройному опорі у разі агресії, а 61% готові до участі у мирному опорі. Такі погляди населення було зафіксовано під час опитування громадської думки, яке було замовлено Міністерством національної оборони та проведено у грудні вже 2024 року.

У Литві громадяни також демонструють обізнаність та адекватне сприйняття гібридних, кібер- та інформаційних загроз. Згідно з результатами опитування громадян Литви віком 18-75 років було проведено компанією Spinter Research на замовлення Міністерства національної оборони у грудні

2024 року, 76% респондентів вважають, що Росія є гібридною загрозою для Литви, а 78% переконані, що Росія цілеспрямовано впливає на інформаційний простір Литви з метою маніпуляції громадською думкою.

Незважаючи на це, 71% опитаних стверджують, що здатні розпізнавати інформаційні атаки та дезінформацію, 51% знають, що робити у разі інциденту кібербезпеки, а 56% перевіряють безпеку веб-сайтів перед тим, як надавати особисті дані.

На замовлення Урядової канцелярії, компанія “Turu-uuringute AS” у грудні 2023 року провела опитування, метою якого було вивчення ставлення громадян Естонії до ключових суспільних тем, включаючи економічний добробут, безпеку, підтримку України, а також довіру до державних інститутів та медіа. Опитування охопило 1252 респонденти з Естонії, віком від 15 років і старше, та було виявлено, що 60% жителів Естонії, які належать до інших національностей, переважно російськомовних, засуджують військову агресію Росії в Україні, 11% підтримують, а 29% не змогли або не захотіли висловити свою думку. При цьому 96% естонців висловили несхвалення військової агресії Росії. Якщо аналізувати відповіді всіх учасників опитування, то 84% естонців засуджують військові дії Росії, а 4% висловлюються на їхню підтримку. Ці показники зберегли свою стабільність упродовж останнього року.

За даними опитування, 63% учасників підтримали прийом українських військових біженців, 30% висловили незгоду, а 7% не змогли дати відповіді. Результати опитування свідчать про зниження підтримки прийому військових біженців порівняно з роком початку повномасштабної агресії. У грудні 2022 року 74% жителів Естонії підтримали прийом біженців, а 21% виступили проти.

Представники емігрантського населення Естонії, говорячи про війну в Україні, віддають перевагу естонським ЗМІ, хоча їхня довіра до них помітно нижча, ніж у естонців. У той же час довіра до російських ЗМІ серед цієї групи населення знизилася з 39% на початку лютого до 27% у середині березня 2023 року. Відповідно до репрезентативного дослідження, замовленого Державною канцелярією та проведеного Turu-uuringute AS, естонці як основні джерела інформації виділяють естономовні телеканали (74%), портали новин (61%) і радіо (36%).

Проте, на відміну від естонців, люди інших національностей, які проживають в Естонії, найчастіше використовують портали новин (43%), соціальні мережі (35%) та російські телеканали (32%) для отримання інформації.

Порівнюючи з даними, отриманими минулих років, можна відзначити, що від лютого 2022 року портали новин і російські телеканали стали менш затребуваними джерелами інформації серед представників інших національностей, які проживають в Естонії. При цьому результати щодо російських телеканалів показують значні розбіжності у різних дослідженнях. Естонці віддають перевагу естонським телеканалам, таким як «ERR» (ETV і ETV2), естонським радіостанціям та естонським порталам новин, розглядаючи їх як найбільш достовірні інформаційні джерела новин і знань.

Російським ЗМІ (новинним порталам чи телеканалам) довіряють 33% жителів Естонії, які не належать до естонської національності. Цей показник знизився з 40%, порівняно з даними, отриманими наприкінці лютого 2022.

Щодо інформації про російсько-український конфлікт, естонці продовжують довіряти переважно естонським каналам (89%), а довіра до західних, українських та російських каналів становить 67%, 52% та 2% відповідно.

Відносно опитувань Латвії, проведене на замовлення Державної канцелярії у 2024 році, показало, що 37,9% жителів цієї країни найбільш активно стежать за новинами про війну Росії в Україні, які транслюються у ЗМІ. Другим за популярністю питанням серед мешканців Латвії є охорона здоров'я, інтерес до якої висловили 37,6% опитаних.

Інтерес до війни Росії в Україні серед опитаних жителів Латвії збільшився на 5,4 процентних пункти порівняно з 2023 роком, досягнувши 67,9% минулого року з 62,5%. Результати опитування демонструють, що війна Росії в Україні продовжує займати центральне місце у латвійських ЗМІ. 40% респондентів вважають, що латвійські ЗМІ приділяють цій темі надмірну увагу. Проте, спостерігається тенденція до зниження кількості респондентів, які вважають, що латвійські ЗМІ часто висвітлюють війну в Україні: з 87,1% у 2022 році до 79,9% у 2024 році. Паралельно з цим, довіра до комерційного телебачення та комерційних інтернет-порталів новин також зменшилася. Якщо у 2022 році до комерційного телебачення довіряли 48,2% респондентів, то у 2023 – 45%. Довіра до комерційних новинних інтернет-порталів знизилася з 43,8% у 2023 році до 39,9% у 2024 році.

Згідно із дослідженням онлайн-опитування, проведене компанією Berg Research на замовлення Державної канцелярії в період з 15 жовтня по 24 листопада 2024 року, охопило 1009 жителів Латвії віком від 18 до 74 років.

Результати показали, що 59,1% опитаних мешканців Латвії довіряють інформації про війну в Україні, яку надають латвійські державні установи, а 58,7% довіряють інформації від латвійських ЗМІ.

Підводячи підсумки результатів опитувань у країнах Балтії, можна відзначити загальне зростання підтримки Європейського Союзу серед населення. У Литві більшість вважає Росію гібридною загрозою через її вплив на інформаційний простір, при цьому громадяни виявляють високу здатність

розпізнавати дезінформацію. В Естонії більшість естонців засуджують військову агресію Росії і довіряють національним ЗМІ, проте серед російськомовних громадян спостерігається зниження довіри до російських медіа. У Латвії також переважає довіра до інформації від державних установ і ЗМІ, і хоча довіра до медіа зменшилась, інтерес до війни в Україні залишається високим серед громадян. Усі ці результати свідчать про зростаючу обізнаність населення країн Балтії щодо загроз та посилену підтримку європейських цінностей і безпеки.

У зв'язку з воєнно-політичними викликами Балтійські держави розробляють нові стратегії та плани для забезпечення інформаційної безпеки, адже в умовах сучасної глобалізації інформаційні загрози можуть мати не лише локальний, а й глобальний характер.

У Стратегії захисту інформації Естонії на 2024–2030 роки під назвою «Найдружніша до ІТ Естонія» було зазначено, незважаючи на невеликі розміри Естонії за кількістю населення та територією, вона має можливість впливати на розвиток свого інформаційного середовища не тільки на національному рівні, але й на міжнародній арені, діючи продумано та стратегічно. Естонія планує брати участь в законодавчих процесах Європейського Союзу та формуванні політичних і стратегічних напрямків, аби активно сприяти цим тенденціям у глобальному масштабі через механізми ООН та співпрацю в галузі розвитку[42].

Враховуючи виклики цифровізації та автоматизації, які стоять перед естонськими компаніями, планується включення питання кібербезпеки в усі національні ініціативи щодо покращення можливостей у цих сферах. В Естонії

[42]Ministry of Economic Affairs and Communications of Estonia. Majandus Ja Kommunikatsiooniministeerium. Cybersecurity Strategy 2024-2030 "*A more it-sensitive Estonia*". 31 p.

є підприємці, які сприймають кібербезпеку як технічну задачу для ІТ-фахівців і не завжди розуміють її значення для їхнього бізнесу. Державні органи та організації, що займаються кібербезпекою, планують продовжувати працювати над підвищенням обізнаності про реальні кіберзагрози та роз'яснювати механізми контролю та захисту від них.

У 2024 році у документі "Вимоги Естонського стандарту інформаційної безпеки (E-ITS)" було зазначено, що Естонія знаходиться на початкових стадіях впровадження електронної інформаційно-технічної системи (E-ITS) [43].

Система планується бути в подальшому основним інструментом для вирішення питань інформаційної безпеки в Естонії, відповідаючи вимогам національного законодавства. Цей стандарт був розроблений для забезпечення захисту бізнес-процесів та інформаційних систем, що використовуються для виконання державних функцій. Проте це вимагає поступового розвитку та додаткових зусиль для практичної реалізації, хоча політики та посібники вже створені. Стратегія на подальші роки підкреслює важливість постійної уваги та співпраці з постачальниками послуг, які надають інформацію щодо документів, що містять інформацію про всі організації, які не працюють. Успішне впровадження E-ITS залежить від якісної взаємодії з надійними постачальниками, які здатні забезпечити належну реалізацію технічних вимог.

Подальші наміри Литовської Республіки задумуються у наступні роки у впровадженні рекомендацій, що призведуть до управління ризиками безпеки інформаційних технологій на національному рівні, створенню умов для цифрового проведення оцінки та моніторингу відповідності вимогам кібербезпеки та ІТ-безпеки.

[43] Kadri Koit. Estonian Information Security Standard (E-ITS) Requirements Description in Public Procurement. *Department of Computer Science.* 2024. 102 p.

В стратегії майбутнього Литовської Республики «Литва 2050» зазначається, що рушійною силою майбутнього Литви є зацікавлені громадяни, а також відкриті до змін політики, які підтримують довірливий діалог між суспільством та державними установами. Литва планує:

– розвиток фізичної комунікаційної інфраструктури, яка зв'язує Литву з її ключовими партнерами, що має сприяти зростанню впливу Литви на прийняття значущих рішень;

– активно брати участь у міжнародній оборонній промисловості (ЄС та НАТО);

– впровадження розширеної національної системи кібербезпеки та захисту, що призведе до досягнення та підтримання литовською державою високого рівня кібернетичної безпеки.

Національний план прогресу, розрахований на десять років і чітко визначаючи стратегічні цілі, завдання та фінансування, є інструментом реалізації бачення майбутньої Литви «Литва 2050», де ключовими елементами є діалог між суспільством та державою, зосередженість на пріоритетах і активне залучення громадськості

Рада прогресу держави здійснює контроль за втіленням бачення "Литва 2050", організовуючи громадські дискусії, оцінюючи прогрес, систематично інформуючи Сейм та Уряд про результати аналізу, свої пропозиції та рекомендації, а також забезпечуючи прозору комунікацію з суспільством.

Упродовж наступного десятиліття основні зусилля будуть спрямовані на:

– реформу державного управління;

– створення та зміцнення системи всеосяжної оборони;

– забезпечення економічної, енергетичної та кібернетичної безпеки й стійкості держави.

Роблячи огляд на подальші плани та стратегії Латвійської Республіки, то «Концептуальний звіт про національну стратегічну комунікаційну та інформаційно-просторову безпеку» на 2023–2027 роки (далі – Концепція), визначає національне бачення та цілі безпеки інформаційного простору зміцнення, включаючи розвиток можливостей стратегічних комунікацій, на 2023–2027 роки, а також пріоритетні напрямки дій та завдання. У реалізації усіх завдань, планується залучити всі державні та місцеві органи влади, а також організоване громадянське суспільство, академічний та приватний сектори скоординовано, відповідно до їхніх можливостей та компетенцій.

Концепція має на меті всебічне зміцнення безпеки інформаційних просторів у трьох взаємопов'язаних ключових напрямках до 2027 року.

1. До 2027 року передбачається розбудова потужних централізованих структур стратегічної комунікації, що ефективно взаємодіють зі стратегічно орієнтованою та професійною державною адміністрацією й місцевим самоврядуванням, а також налагодження комунікації між установами через цифрові канали.
2. Концепція передбачає комплексне посилення таких аспектів ЗМІ, як незалежність, якість, безпека та інклюзивність, а також розвиток їхньої здатності пристосовуватися до викликів, що зумовлюють війні у світі, до 2027 року.
3. До 2027 року передбачається досягти стійкості латвійського суспільства до маніпуляцій в інформаційному просторі, зокрема шляхом підвищення медіа- та інформаційної грамотності, а також залучення неурядового, приватного та академічного секторів до скоординованого та ефективного зміцнення безпеки інформаційного простору.

Стратегії визначають шляхи досягнення країн Балтії технологічної незалежності шляхом ефективного використання та розвитку наявних інструментів і ресурсів, а також окреслюють посилення співпраці з міжнародними партнерами, які поділяють цінності демократії, верховенства права та прав людини.

Вони зосереджується на подальшій безпеці критично важливих сервісів (лікарні, енергетика, залізниця) та зростаючої кількості підключених пристроїв, передбачаючи спільні механізми реагування на масштабні кібератаки, співпрацю з міжнародними партнерами для глобальної кібербезпеки та координовану відповідь на загрози через Спільний підрозділ з кібербезпеки, що об'єднує ресурси та досвід Балтійських країн як членів ЄС.

Порівнюючи подальші кроки країн Балтії покращення ситуації з Україною, то Україна також робить значні кроки та планує заходи протидії у напрямку безпеки інформаційного простору, та є стратегічним союзником для подальшої розробки та імплементації комплексної стратегії захисту інформаційного простору Балтійських країн. Зокрема, оновлений склад Кабінету Міністрів (Шмигаль Д. А. – Прем'єр-міністр України, Свириденко Ю. А. – Перший віце-прем'єр-міністр, віце-прем'єр-міністри) у вересні 2023 року схвалив концепцію усунення загроз інформаційному простору Латвії з боку Російської Федерації, та передав її на розгляд до Канцелярії Президента та Сейму. Рішення щодо цього документа було ухвалено у жовтні 2023, тому він набув статусу обов'язкового для виконання.

Національний і глобальний індекси країни не тільки відображають внутрішні досягнення країни, але й визначають її роль і статус у міжнародному контексті. Вони є показниками розвитку, економічної стабільності, рівня життя, а також політичної та соціальної стабільності. Тенденцію зростання індексів можна побачити, аналізуючи по роках. З кожним

роком усі три країни піднімаються за рейтингом з інформаційної безпеки та цифрової конкурентоспроможності.

За даними Національного індексу кібербезпеки (далі – NCSI), що оновлюється в реальному часі, вимірює готовність країн до протидії інформаційним загрозам та управління кіберінцидентами, та одночасно виступає як база даних з публічними доказами та засіб для зміцнення національної кібербезпеки, можна зазначити, що Естонія вирізняється серед країн Балтії найрозвинутішою системою інформаційного захисту та найвищим рівнем безпеки в інформаційному просторі. Згідно з останніми даними Естонія займає шосте місце серед всіх країн. Показник Глобального індексу Естонії – 45-та позиція.

Станом на 2024–2025 роки показники індексу Естонської Республіки в сфері кіберзахисту не відчутно відрізняються, але спостерігаючи статистику, можна зазначити, що з кожним роком покращуються. Згідно з останніми даними NCSI, Естонія стабільно займає високі позиції у світовому рейтингу. Станом на грудень 2024 року Естонія посідала 6-те місце з індексом 88.33. Це свідчить про значну увагу, яку країна приділяє розвитку кібербезпеки. Графік за 2025 рік відображає поточний стан готовності Естонії у інформаційних сферах, показуючи її сильні сторони та області, які потребують подальшого розвитку.

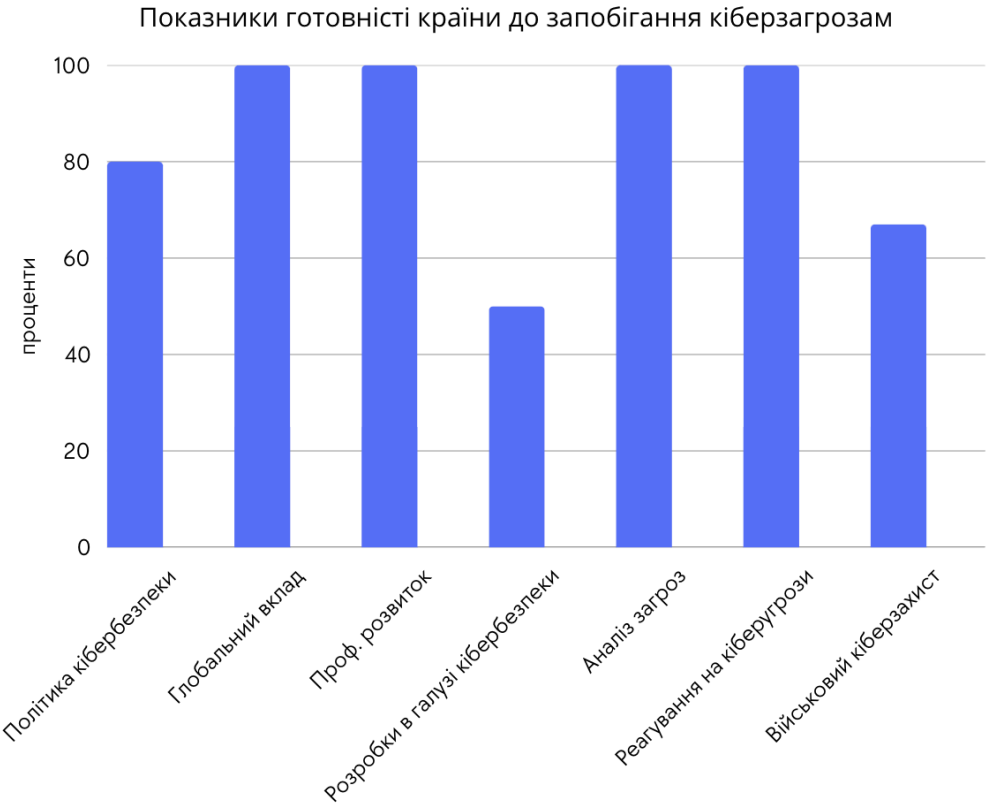

Рис. 3.1. Національний індекс кібербезпеки в Естонії за 2025 рік [44]

У Глобальному індексі кібербезпеки, який складає Міжнародний союз електрозв'язку, Литва займає 55-ту позицію станом на 2025 рік. Восьме місце серед усіх країн Литва займає з Національного індексу кібербезпеки.

[44]NCSI. Estonia. 2024-2025. URL: https://ncsi.ega.ee/country/ee/ (date of access: 02.05.2025).

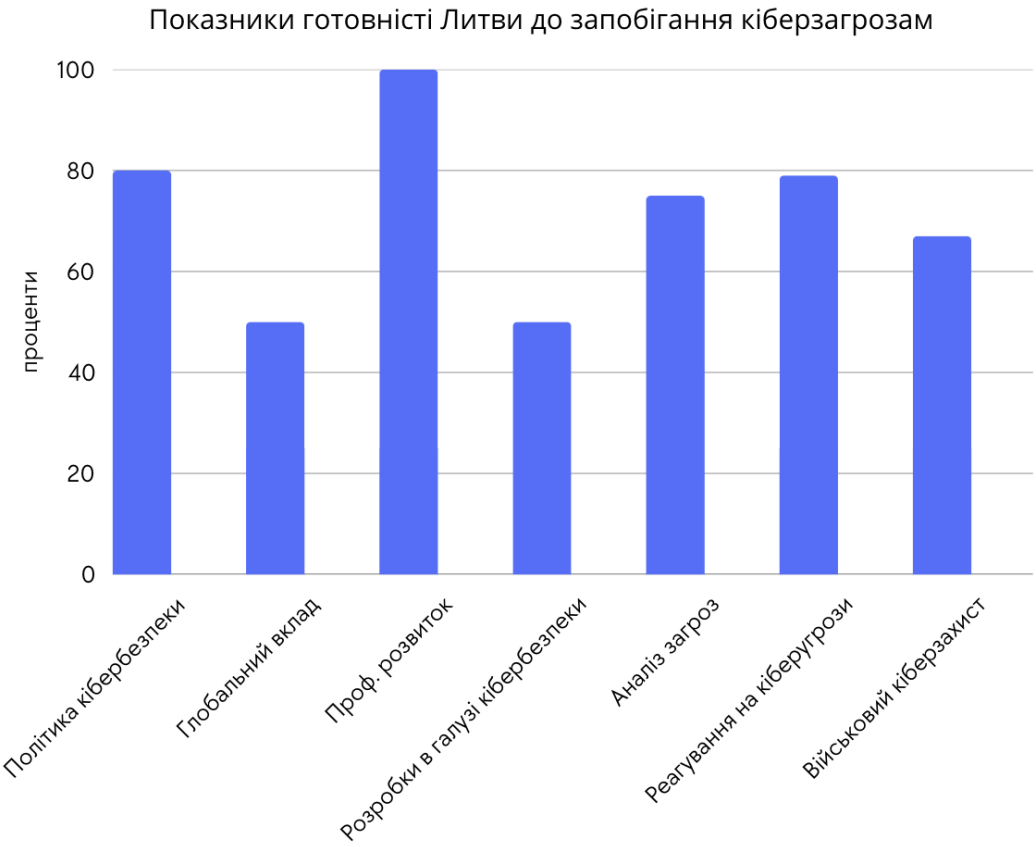

Рис. 3.2. Національний індекс кібербезпеки в Литві за 2025 рік[45]

З огляду на Латвійську державу, її Національний індекс кібербезпеки становить 19-те місце, а Глобальний індекс кібербезпеки – 79 станом на 2024-2025 роки, що свідчить про високий рівень готовності країни у сфері кібербезпеки. Графік за 2025 рік детально показує прогрес Литви за кожним із зазначених аспектів. Він відображає сильні сторони країни та сфери, де є потенціал для подальшого розвитку.

[45] NCSI. Lithuania. 2024-2025. URL: https://ncsi.ega.ee/country/lt/ (date of access: 02.05.2025).

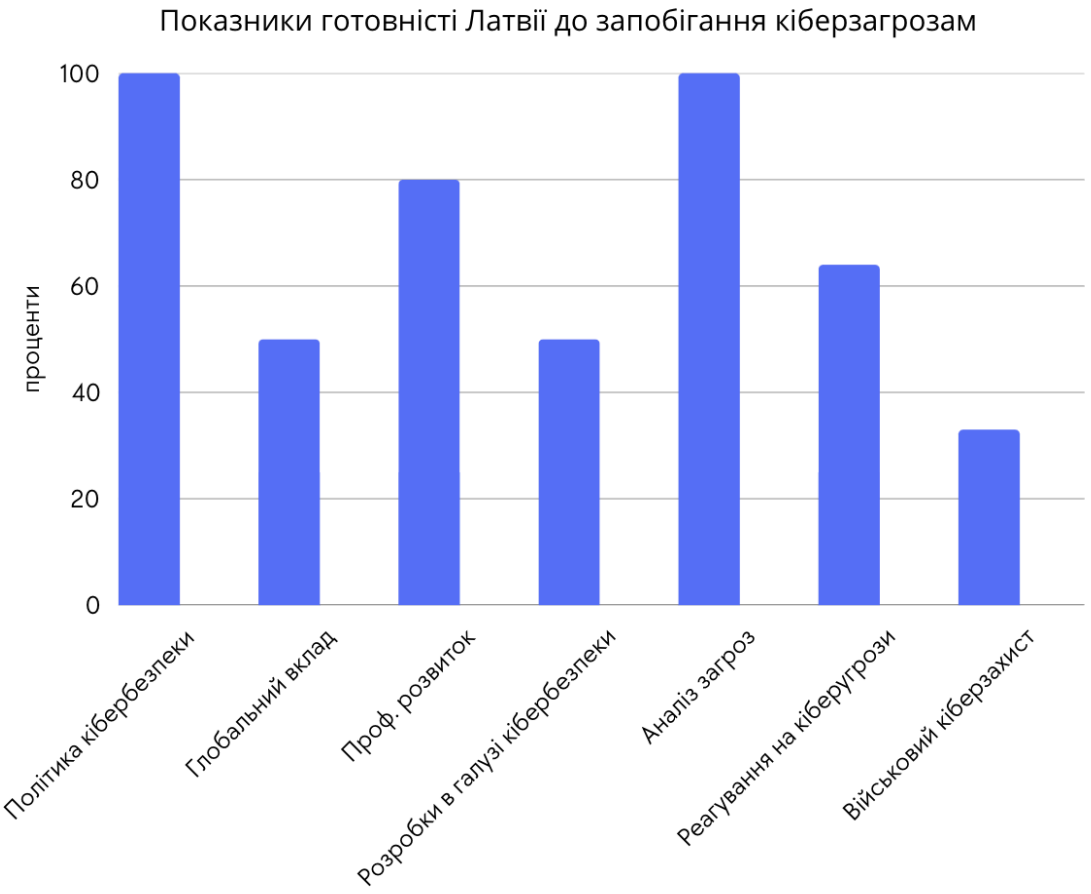

Рис. 3.3. Національний індекс кібербезпеки в Латвії за 2025 рік[46]

Таким чином, країни Балтії демонструють стабільний прогрес у сфері кіберзахисту. Естонія лідирує серед балтійських країн завдяки високим результатам на міжнародному рівні, в той час як Литва і Латвія покращують свої позиції в національному контексті. Всі три країни продовжують інвестувати в розвиток кіберзахисту, зокрема в модернізацію інфраструктури, підвищення кваліфікації кадрів та впровадження новітніх технологій для забезпечення кібербезпеки. Однак для подальшого покращення є можливості,

[46] NCSI. Latvia. 2024-2025.URL: https://ncsi.ega.ee/country/lv/ (date of access: 02.05.2025).

зокрема у сфері міжнародної співпраці та обміну інформацією щодо кіберзагроз.

ВИСНОВКИ

У процесі дослідження було виявлено сучасний стан наукової розробки проблеми інформаційної безпеки країн Балтії в умовах російсько-української війни, що відображає зростаюче розуміння її критичної важливості для національної безпеки та стабільності. Науковці всебічно вивчають різні аспекти цього складного питання, включаючи кібернетичні загрози, політичні обмеження та технологічні рішення, що поглиблює розуміння викликів і перспектив, які постають перед балтійськими країнами. Внаслідок розширення дослідницької бази, Україні варто брати приклад з досвіду Балтійських країн, де успішно реалізуються стратегії та політики, спрямовані на підвищення стійкості інформаційної безпеки. Для цього необхідна подальша міждисциплінарна взаємодія та емпіричні дослідження, які допоможуть розробити ефективні підходи до забезпечення інформаційної безпеки в умовах сучасних викликів.

Визначено основні поняття та категорії, які використовуються при аналізі інформаційної безпеки, що забезпечує надійне підґрунтя для розуміння складної взаємодії факторів, що її визначають. У плані методології застосовано детальні, прогностичні та розвідувальні дослідження, що дає змогу всебічно розглянути питання інформаційної безпеки з різних точок зору, поглиблюючи та розширюючи наукове дослідження в цій значущій галузі.

Встановлено, що історичний контекст розвитку країн Балтії визначає сучасну систему забезпечення їхньої інформаційної безпеки, а також сприяє швидкому прогресу та впровадженню передових інформаційних, телекомунікаційних і кібернетичних технологій. Безпекова ситуація в Балтійському регіоні тісно пов'язана з міжнародними подіями, причому основні загрози безпеці носять транснаціональний характер, що зумовлює

необхідність забезпечення стабільності безпеки як на регіональному, так і на світовому рівнях.

Доведено, що регулювання інформаційної безпеки балтійських країн здійснюється через комплекс національних законодавчих актів, а також у рамках загальноєвропейських ініціатив. Кожна з трьох країн — Естонія, Латвія та Литва — має власні органи та нормативно-правові документи, що відповідають за захист інформаційних систем та інфраструктури, забезпечення кібербезпеки та захист персональних даних. Усі ці країни активно взаємодіють на міжнародному рівні через механізми ЄС, ООН та інші міжнародні платформи, що забезпечують додаткові норми та регулювання для підвищення рівня кібербезпеки в глобальному контексті.

Проведено дослідження загроз та викликів інформаційній безпеці Естонії, Латвії та Литви до початку повномасштабної війни, яке показало вразливість балтійських країн до різноманітних інформаційних небезпек. Кіберзагрози постійно створювали значні ризики для національної безпеки та стабільності цих держав. Крім того, поширення дезінформаційних кампаній, спрямованих на підрив довіри суспільства та розпалювання ворожнечі, ще більше ускладнювало забезпечення інформаційної безпеки в Естонії, Латвії та Литві. Для протидії цим численним загрозам, посилення кібербезпеки, міжнародна співпраця та підвищення стійкості стали ключовими заходами для зменшення ризиків та захисту від майбутніх інцидентів.

Ідентифіковано нові, посилені виклики та загрози інформаційній безпеці після початку повномасштабного вторгнення, які становлять значний ризик для цифрової інфраструктури та національної безпеки країн Балтії. В умовах ескалації гібридної війни та зростання міждержавної недовіри, спричиненого агресором, балтійські країни зіткнулися зі збільшенням кількості кібератак – від деструктивних операцій до прихованого збору розвідданих. Крім того,

дезінформаційні кампанії, спрямовані на формування вигідних наративів та підрив довіри суспільства, стали інтенсивнішими, поглиблюючи соціальні розбіжності та ускладнюючи боротьбу з неправдивою інформацією. Подолання цих проблем потребує комплексного підходу, що включає зміцнення кіберзахисту, поглиблення міжнародної співпраці та підвищення рівня медіаграмотності для протидії поширенню дезінформації, що є необхідним для захисту інформаційного простору країн Балтії в умовах триваючого конфлікту та геополітичної нестабільності.

Підкреслено, що російсько-українська війна не лише поглибила геополітичні зміни, але й спричинила значні трансформації у суспільній думці балтійських країн, посиливши їхню євроатлантичну орієнтацію, відчуття власної вразливості, але й консолідації та солідарності з Україною. Це також створило нові виклики для інтеграції певних груп населення та формування майбутньої національної політики. Було з’ясовано, що передові технології кардинально змінюють підходи до інформаційної безпеки, пропонуючи новаторські інструменти для протидії постійно зростаючим інформаційним загрозам. Такі технологічні рішення, як CERT-центри (CERT-EE, CERT-LT, CERT.LV), Загальний регламент щодо захисту даних (GDPR), ENISA та Директива NIS, забезпечують розширені можливості для виявлення загроз, реагування на інциденти та захисту даних. Крім цього, впровадження та оновлення законодавства сприяє запобіганню витокам інформації, несанкціонованому доступу та маніпуляціям, що має вирішальне значення для національної безпеки.

Доведено, що Стратегічне планування протидії інформаційним загрозам на майбутнє та спільні міжнародні проєкти в межах спільноти інформаційної безпеки сприяють обміну досвідом, професійному розвитку та розробці заходів для поліпшення ситуації, що формують глибше розуміння глобального

середовища загроз та пришвидшує виявлення інцидентів і реагування на них. Міжнародна співпраця у сфері інформаційної безпеки є ключовим фактором у протидії глобальним кіберзагрозам та створенні безпечного інформаційного середовища. Через спільні ініціативи, як-от платформи обміну інформацією, спільні навчання та кібербезпекові альянси, держави мають змогу обмінюватися розвідданими про загрози, ділитися найкращими практиками та координувати дії у відповідь на інциденти. Завдяки зміцненню довіри та співпраці між країнами, міжнародні зусилля сприяють підвищенню загальної стійкості світової спільноти кібербезпеки, а також надають зацікавленим сторонам інструменти для ефективнішої боротьби з кіберзагрозами. Вкладаючи зусилля в удосконалення кадрового потенціалу, балтійські держави отримують можливість посилити власну інформаційну безпеку, збільшити стійкість до загроз та ефективніше адаптуватися до нових викликів у сучасному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Акімова Л. М. Аналіз гібридних загроз економічній безпеці України: міжнародний досвід та українські реалії. *Інвестиції: практика та досвід*. 2018. № 22. С. 110–115. URL: https://doi.org/10.32702/2306-6814.2018.22.110 (date of access: 20.05.2025).

2. Білоножко С. Західний вектор зовнішньої політики країн Балтії: шлях від незалежності до євроінтеграції. Наукові праці історичного факультету Запорізького національного університету. 2015. № 44 (2). С. 130–135.

3. Бодрук О. Цілеспрямованість, рішучість і послідовність - характерні ознаки політики країн Балтії. Стратегічна панорама. Київ, 1999. № 3. С. 26.

4. Бородакий Ю. В., Добродєєв А. Ю., Бутусов І. В. Кібербезпека як основний фактор національної та міжнародної безпеки XXI століття (ч. 1). Питання безпеки.

5. Бутрімас Вітаутас. Балтійське співробітництво у сфері кібербезпеки. Per Concordiam. 2016. № 2. Том 7. С. 19–23.

6. Гладиш М., Краєвська О. Балтійський вимір Європейської політики безпеки та оборони. Грані. 2015. № 4 (120). С. 80–85.

7. Давимука О.О., Кравченко В. В. Особливості безпекової співпраці України та Литви в умовах протидії російській загрозі. Стратегічні пріоритети. № 3 – 4 (51). 2019. С. 70–75.

8. Дозвіл про Резолюцію уряду Литовської Республіки від 12 березня 2014р. 244 «Про затвердження програми розвитку інформаційного суспільства на 2014–2020 Литовської Республіки»: від 20.12.2017.

9. Європейське агентство з мережевої та інформаційної безпеки (ENISA).

URL:https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management (дата звернення: 01.05.2025).

10. Завацький В.М. Європейська інтеграція країн Балтії (1991–2004 рр.): дис.канд. іст. наук. Донецьк, 2008. С. 225.

11. Закон про кібербезпеки № 2024-13535 поправка XII-1428: Закон про кібербезпеки від 18.10.2024. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/1a8657f2427a11efb121d2fe3a0eff27?jfwid=-w4asrfskx (дата звернення: 02.05.2025).

12. Закон про національну кібербезпеку: від 01.09.2024. URL: https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums?&search=on (дата звернення: 30.04.2025).

13. Замікула М.О. Країни Балтії на початку 1990-х років: передумови євроатлантичної інтеграції. *Наукові праці Чорноморського державного університету імені Петра Могили. Серія «Історія».* 2010. Т. 129. Вип. 116. С. 91–94.

14. Звоздецька О. Кібербезпека країн Балтії: сучасні виклики та загрози. Медіафорум : аналітика, прогнози, інформаційний менеджмент: збірка наукових праць. Чернівці: Чернівецький національний університет, 2017. Том 5. С. 20-34.

15. Зінич Л. В. Інформаційна безпека Естонії: досвід для України. *Актуальні проблеми вдосконалення чинного законодавства України.* 2019. № 50. С. 26–38. URL: https://doi.org/10.15330/apiclu.50.26-38 (дата доступу: 20.05.2025).

16. Івасечко О. Я., О. В. Коваль. Загрози та виклики для країн Балтії на сучасному етапі євроінтеграції. *Вісник Маріупольського державного університету.* Серія: Історія. Політологія. 2016. Вип. 16. С. 248-255. URL: http://nbuv.gov.ua/UJRN/Vmdu_ip_2016_16_33 (дата звернення: 30.04.2025).

17. Кавин С. Нормативно-правові механізми забезпечення кібербезеки в країнах Балтії. 2020. URL: http://pgp-journal.kiev.ua/archive/2020/12/56.pdf (дата звернення: 01.05.2025).

18. Карауц О. Результати Вільнюського саміту НАТО 11-12 липня 2023 року. 2023. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/rezultaty-vilnyuskoho-samitu-nato-11-12-lypnya-2023-roku (дата звернення: 01.05.2025).

19. Ковальов А.А., Балашов А.И. Міжнародно-правові аспекти політики кібербезпеки деяких європейських країн колишнього радянського блоку. *Вісник Поволзького інституту управління.* 2018. № 5 (18). С. 105–114

20. Литва готує стратегію громадянського опору: 50 % населення протидіятимуть окупанту. *Українська правда*. 2023. 23 серп. URL: https://www.eurointegration.com.ua/news/2023/08/23/7168087/

21. Лінкявічюс Л. «Литва готова і надалі активно підтримувати Україну та практично допомагати в усіх сферах у відповідності зі статусом стратегічного партнерства». Міністерство закордонних справ України. 2019. URL: https://mfa.gov.ua/news/72168-linas-linkyavichyus-litva-gotova-i-nadali-aktivno-pidtrimuvati-ukrajinu-ta-praktichno-dopomagati-v-usih-sferah-u-vidpovidnosti-zi-statusom-strategichnogo-partnerstva (дата звернення: 01.05.2025).

22. Нападиста В. Україна в контексті викликів та загроз: погляд з країн Балтії. *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України.* 2018. Вип. 1. С. 243-268.

23. Палій Г. НІСД. Зміцнення безпеки країн Балтії в контексті зміни стратегічної концепції оборони НАТО. *Значення для України.* 2024. URL: https://niss.gov.ua/news/komentari-ekspertiv/zmitsnennya-bezpeky-krayin-baltiyi-v-konteksti-zminy-stratehichnoyi (дата звернення: 14.01.2025).

24. Палій О.А. Специфіка та наслідки інтеграції країн Балтії до євроатлантичних структур безпеки. *Наукові записки НаУКМА. Політичні науки.* 2002. Том 20. С. 55–60

25. Поправка до Закону №818 «Про затвердження Національної стратегії кібербезпеки»: від 12.05.2018: станом на 1 січ. 2019 р. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce (дата звернення: 13.03.2025).

26. Посольство України в Литовській Республіці. Підтримка і солідарність Литви і литовського народу. URL: https://lithuania.mfa.gov.ua/spivrobitnictvo/3791-turizm (дата звернення: 25.01.2025).

27. Про затвердження Програми розвитку електронної інформаційної безпеки (Кібербезпека) на 2011-2019 роки: від 16.07.2019 № 1111100NUTA00000796. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.403385 (дата звернення: 26.04.2025).

28. Резолюція 130 «Посилення ролі МСЕ у зміцненні довіри та безпеки під час використання інформаційно-комунікаційних технологій». Повноважна конференція Міжнародної спілки електрозв'язку. *Заключні акти Повноважної конференції Міжнародної спілки електрозв'язку*. Пусан, 2014 р. ITU, 2015. С. 241–299.

29. Ромашкіна Н. Озброєння без контролю: сучасні загрози міжнародній інформаційній безпеці. Шляхи миру та безпеки. 2018. № 2(55). С. 64–83. URL: https://doi.org/10.20542/2307-1494-2018-2-64-83 (дата звернення: 21.03.2025).

30. Русначенко А. Між двома імперіями: країни Балтії та Україна у 1918 році. *Дриновський збірник.* 2019. Том XII. URL: https://doi.org/10.7546/ds.2019.12.23 (дата доступу: 20.05.2025).

31. Політика безпеки та оборони. *Сайт Міністерства закордонних справ Латвії.* URL: https://www.mfa.gov.lv/en/security-and-defence-policy (дата звернення: 20.02.2025).

32. Президент Латвії: країни-члени НАТО повинні продовжувати зміцнювати свою стійкість до гібридних та інформаційних загроз. 2018. URL: https://www.president.lv/lv/jaunums/valsts-prezidents-jaturpina-stiprinat-nato-dalib valstu-noturibu-pret-hibrido-un-informacijas-telpas-apdraudejumu (дата звернення: 13.02.2025).

33. Сергунін О. Соцієтальна безпека у регіоні балтійського моря: російська перспектива. *Балтійський регіон*. 2020. С. 4–20.

34. Сидорук М. Особливості інтеграції держав Балтії до ЄС. *Наукові записки Національного університету «Острозька академія»*. Серія «Міжнародні відносини». 2010. Вип. 2. С. 97–104

35. Скриль С. А. Трансформація політичних систем Латвії, Литви та Естонії в умовах інтеграції в європейське співтовариство. Актуальні проблеми політики. 2015. Вип. 54. С. 146–152.

36. Стельмах В. О. Балтійська регіональна співпраця на шляху до західних інтеграційних структур. Цивілізаційні засади трансформаційних процесів на пострадянському просторі за заг. ред. канд. іст. наук, доцента А. Г. Бульвінського державного університету «Інститут всесвітньої історії НАН України». К., 2018. С. 192–205.

37. Сухобокова О. О. Політична та військова допомога країн Балтії у перші місяці повномасштабної російсько-української війни. The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects: Scientific monograph. Riga, Latvia: Baltija Publishing, 2022, Pp. 661–670.

38. Туряниця І. Пріоритети оборонної політики та національної безпеки Литовської Республіки на сучасному етапі. Наукові зошити історичного факультету Львівського університету. 2017. № 18. С. 323–333.

39. Федоров А. «Війни пам'яті» – елемент інформаційної війни проти Росії. 2020. С.88–97.

40. Чакарс Я., Екманіс І. Інформаційні війни в країнах Балтії: довга тінь Росії, пер. з англ. Ємельянової І. – Бостон: Academic Studies Press, 2025.

41. Чугаєв О.А. Наслідки вступу до ЄС для країн Балтії. Актуальні проблеми міжнародних відносин: збірник наукових праць. Київ : Київський національний університет імені Тараса Шевченка, Інститут міжнародних відносин, 2006. Вип. 59. Ч. І. С. 129–135.

42. Щедрова Г.П. Адаптація України до вимог ЄС: досвід країн Балтії. Politicus. 2017. Вип. 1. С. 156–161.

43. About CERT Estonia. *Republic of Estonia. Information System Authority*. URL: https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee (date of access: 12.03.2025)

44. About the NATO Summit Wales 2014. 2014. URL: https://www.gov.uk/government/topical-events/nato-summit-wales-cymru-2014/about (date of access: 29.03.2025).

45. CERT.LV. Kiberincidentu noversanas institucija. URL: https://www.cert.lv/lv/par-mums (date of access: 12.03.2025).

46. Denisenko V. How the Kremlin uses the “ European field ” to win the propaganda game. *Myth detector. Information Wars in the Baltic States*. 2018. C. 93–120

47. Dougherty, J., Kaljurand, R. (2015). Estonia’s “virtual Russian world”: The influence of Russian media on Estonia’s Russian speakers. International Centre for Defence and Security. Vihalemm T., Juzefovics J., Leppik M. (2019). Identity

and media-use strategies of the Estonian and Latvian Russian-speaking populations amid political crisis. Europe-Asia Studies, 71(1), 48–70.

48. Estonia's aid to Ukraine. Republic of Estonia. Ministry of Foreign Affairs. URL: https://vm.ee/en/estonias-aid-ukraine (date of access: 02.05.2025).

49. Galbreath D. Continuity and change in the Baltic Sea region: Comparing foreign policies / D. J. Galbreath, A. Lašas, J. W. Lamoreaux. Amsterdam-New York: Rodopi, 2008. 183 p.

50. Grėsmių Nacionaliniam Saugumui Vertinimas. Vilnius. 2025. P. 40–47

51. Huhtinen, A. (2017). The Baltic Sea region: From a hinge between Russia and the west to rhizomatic information channel. In A. Makarychev, A. Vatsyk (Eds.), Borders in the Baltic Sea region: Suturing the ruptures. Pp. 53–80.

52. Jakniunaite, D. 2016. Changes in Security Policy and Perceptions of the Baltic States 2014–2016. Journal on Baltic Security. Vol. 2. No. 2. Pp. 6–35.

53. Kachuyevski, A. (2017). The "Russian world" and the securitization of identity boundaries in Latvia. In A. Makarychev, A. Yatsyk (Eds.), Borders in the Baltic Sea region: Suturing the ruptures (pp. 227–247). Palgrave Macmillan, 239.

54. Krumins G. (2018). *Soviet economic gaslighting of Latvia and the Baltic States*. Defence Strategic Communications, 4(1), 49–78.

55. Lietuvos Respublikos Vyriausybė. Nutarimas. Del elektronines informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 METais programos patvirtinimo. Nr 796. Vilnius. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.403385 (date of access: 09.04.2025).

56. Lithuania's vision for the future. "Lithuania 2050". 2023. 33 p.

57. Marnot D. Baltikumi Julgeolekupolitika dokumentide Vordlus. 2020. P. 165–171.

58. National Cyber Security Index (NCSI). 2024. URL: https://ncsi.ega.ee/ncsi-index/ (date of access: 01.05.2025).

59. National Security Strategy of the Republic of Lithuania. Ministry of National Defence of the Republic of Lithuania, Totorių str. 25, LT-01121. Vilnius. 2017. P. 5

60. Personal Data Protection Act. § 56. Competence of Estonian Data Protection Inspectorate upon exercise of state and administrative supervision: of 15.01.2019. URL: https://www.riigiteataja.ee/en/eli/523012019001/consolide (date of access: 18.04.2025).

61. Piret Pernik with Emmet Tuohy. Cyber Space in Estonia: Greater Security, Greater Challenges. August 2013. P.1.

62. Realizing the Vision: The Baltic 2030 Action Plan. Strategic documents. 2020. P. 7–11

63. Riigikogu. National security concept of Estonia. 2010. P. 7–8.

64. Simons G. Perception of Russia's soft power and influence in the Baltic States. *Public Relations Review*. 2015. Vol. 41, no. 1. P. 1–13. URL: https://doi.org/10.1016/j.pubrev.2014.10.019 (date of access: 20.05.2025).

65. Small States in Turbulent Environment: The Baltic Perspective. Edited by Atis Lejins, Zaneta Ozolina. Riga : Latvian Institute of International Affairs, 1997. P. 253

66. The Constitution of the Republic of Estonia. Passed 28.06.1992. R349Entry into force 03.07.1992. URL: https://www.riigiteataja.ee/en/eli/521052015001/consolide (date of access: 11.05.2025).

67. The Reeigikogu discussed the updated national security concept. Parliament of Estonia. 06.02.2023. Plenary session. URL: https://www.riigikogu.ee/en/istungi-ulevaated/the-riigikogu-discussed-the-updated-national-security-concept/ (date of access: 11.05.2025).

68. The European Union and the Baltic States: Visions, Interests and Strategies for the Baltic Sea Region / Ed. by Jopp M. and Arnswald S. Helsinki : The Finnish Institute of International Affairs, 1998. P. 269.

69. Udo Helmbrecht, 2018. Adequate and effective cybersecurity: state of play. Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht – Cybersecurity Conference organised by the Austrian Presidency of the Council of the European Union. *European Union Agency For Network and Information Security Vienna, Austria 3rd December 2018*, pp. 1-6.

70. Vitkus, G. Lithuania's Security and Defence in 2017–2018: the International Context and New Research. Preface. 2018. *Lithuanian Annual Strategic Review 2017–2018.* Vol. 16. Pp. 5–11.

71. Voltri J. Vene teabe Mõjutustegevusele vastamine balti riikides: Eesti, Läti ja Leedu lähenemiste vordlus. P. 34. URL: https://www.kvak.ee/files/2023/01/Johannes-Voltri_VENE-TEABEMOJUTUSTEGEVUSELE-VASTAMINE-BALTI-RIIKIDES-EESTI-LATI-JA-LEEDU-LAHENEMISTE-VORDLUS.pdf (date of access: 10.05.2025).

72. Stoicescu, K. 2019. Russia's non-conventional hybrid warfare against Estonia. CEPA. URL: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-estonia/ (date of access: 04.05.2025).