УДК 342.9
DOI https://doi.org/10.32840/pdu.2-1.38

Г. Ю. Зубко
кандидат юридичних наук

ДЕРЖАВНА ІНФРАСТРУКТУРНА ПОЛІТИКА: ДОСВІД БАЛТІЙСЬКИХ КРАЇН

У статті обґрунтовано особливості здійснення державної інфраструктурної політики у сфері безпеки стратегічної інфраструктури. Наведено схожі та відмінні риси проведення даної політики в Балтійських країнах.

У статті розглянуто, що в Естонії за здійснення державної інфраструктурної політики відповідає Державне агентство з питань системної інформації. Цікавим є те, що Естонія не використовує термін «критична інфраструктура», натомість застосовує таку формулу: захист інфраструктури критичної важливої інформації (ІКВІ) – гарантування, того, що важливі з погляду держави мережеві та інформаційні системи працюють без перебоїв.

З'ясовано, що питаннями критичної інфраструктури в Латвії опікується Міжвідомча комісія з національної безпеки. Комісія є колегіальним консультативним органом, який оцінює та формує перелік об'єктів критичної інфраструктури, включаючи європейську критичну інфраструктуру, та заходи безпеки.

У ще одній Балтійській державі – Литві – також левова частка уваги в рамках реалізації державної інфраструктурної політики належить питанням забезпечення безпеки в Литовській Республіці об'єктів критичної інфраструктури у сфері кібернетичної безпеки, що покладено на Міністерство оборони Литовської Республіки.

Проаналізовано стан нормативно-правового забезпечення здійснення такої діяльності і встановлено, що для ефективного здійснення партнерської взаємодії у сфері захисту критичної інфраструктури має бути ухвалено базовий Закон України «Про безпеку стратегічної інфраструктури». Визначено, що найбільш розповсюдженою моделлю державної інфраструктурної політики виступає об'єктова. Окрім виявлено особливі додаткові правові механізми забезпечення безпеки інфраструктури.

Ключові слова: *державна інфраструктурна політика, стратегічна інфраструктура, критична інфраструктура Литви, захист критичної інфраструктури Естонії, взаємодія державного і приватного партнерів в Латвії, міжнародне співробітництво.*

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями.

Формування оновленої безпекової політики має багато векторів. Одним із них виступає необхідність удосконалення державної інфраструктурної політики. На часі ухвалення відповідного проекту закону, одним із завдань якого, з-поміж багатьох організаційних та функціональних, виступатиме формування системи нормативно-правового регулювання інфраструктурних відносин. Одним із важливих завдань на цьому шляху є вивчення передового зарубіжного досвіду.

Одразу ж зауважу що даний аналіз зроблено на підставі синтезу вивчення: довідок, що їх готували різні посольства, а також відповідних документів Кабінету Міністрів, вітчизняних наукових [1-3] та іноземних джерел; даних і Інтернет. Через це, відповідно до теми мого дослідження посилання я буду робити на правові акти, згідно з якими здійснюється та реалізується державна інфраструктурна політика. Також відмічу, шо здійснення порівняльно-правового дослідження передбачає виявлення не лише тих особливостей, що різнять підходи, а й тих, що демонструють їх схожість. Вивчення міжнародного досвіду також дозволяє лише зрозуміти структуру моделі державної інфраструктурної політики залежно від форми державного устрою и взагалі правової системи.

Проведення компаративного дослідження також дозволить сформулювати основні моделі ДІФСП, адже кожна країна

має власні як правові, так і безпекові традиції, різний рівень імплементації окремих положень міжнародних договорів, зумовлений характером обов'язковості та адміністративно-правовим статусом суб'єктів надання згоди на обов'язковість їх виконання. Окрім цього, можна підійти до розуміння категорії публічного інтереси, змісту поняття суб'єкти владних повноважень у сфері ДІФСП, а також відмітити існуючи адміністративні процедури забезпечення даної політики.

У даному аспекті можна підтримати думку фахівців НІСД, що більшість держав активно модернізує власні сектори безпеки відповідно до викликів сучасності, і особливо – зважаючи на потенціал використання мережі *Інтернет*. Цей процес відбувається із: активним реформуванням систем управління відповідним сектором безпеки; впорядкуванням нормативного поля, що має забезпечити цілісність державної політики в даній сфері; активною роз'яснювальною роботою серед населення щодо небезпек кіберзагроз; збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту; розробкою кіберозброєнь та проведення пробних військово-розвідувальних акцій у кіберпросторі; посилення контролю за національним інформаційним простором [4]. Отже можна дійти висновку про те, що найбільш пріоритетним з огляду на вказані тенденції набуває захист саме інформаційної та кібернетичної інфраструктури, а також відповідних системи, що забезпечують ефективне функціонування інших видів інфраструктури, зокрема й енергетичної, фінансово-економічної, транспортної тощо.

Відтак, окремої уваги набувають питання вивчення зарубіжного досвіду для удосконалення форм та методів міжнародного співробітництва у сфері безпеки стратегічної інфраструктури.

Ступінь наукової розробленості теми. Останнім часом науковий інтерес до проблематики захисту критичної інфраструктури проявляли такі дослідники, як: В. В. Бєгун, Д. С. Бірюков, Д. Г. Бобро, В. Ф. Гречанінов, О. В. Євдін, В. А. Заславський, С. І. Кондратов, А. О. Корченко, А. О. Мороз, Є. Степанова, О. М. Суходоля, С. С. Теленик.

Суттєву роль у науковій дискусії на цю тему відіграють дослідження Національного інституту стратегічних досліджень, які можуть слугувати вагомою джерельною базою для вирішення визначених мною вище наукових завдань у правовій царині.

Водночас цілком очевидно, що аналіз комплексу проблем у сфері інфраструктури здійснюється не на достатньому рівні. Поза науковим обігом лишаються важливі теоретико-правові напрацювання, зокрема в векторі розвитку кібербезпеки щодо об'єктів стратегічної інфраструктури.

Метою статті є наукове обґрунтування правових засад здійснення державної інфраструктурної політики в країнах Балтії.

Завдання дослідження:

- вивчити досвід Естонії;
- проаналізувати досвід Латвійської Республіки;
- вивчити особливості досвід Литовської Республіки.
- запропонувати шляхи удосконалення державної інфраструктурної політики в Україні.

Виклад основного матеріалу

1. Державна інфраструктурна політика Естонії

В Естонії за здійснення державної інфраструктурної політики відповідає Державне агентство з питань системної інформації [5].

До об'єктів *стратегічної інфраструктури* в Естонії належать:

Категорія А – найважливіші з точки зору функціонування держави відомства, в яких ухвалюються *стратегічно* важливі рішення (Офіс Президента, Будинок Уряду, Рійгікогу (парламент), міністерства);

Категорія Б – державні відомства, які забезпечують життєво важливі послуги та інші об'єкти, нанесення ударів по яких може призвести до катастрофічних наслідків або суттєво порушити надання ними послуг (Центр тривоги, електростанції та об'єкти газопостачання);

Категорія В – об'єкти, атаки на які або їхнє знищення можуть піддати ризику життя та здоров'я великого числа людей або призвести до знищення національної культурної спадщини (національний

мистецький музеї KUMU та ERM), а також найбільш важливі мости та тунелі;

Категорія Г – об'єкти, які пов'язані з державною обороною (військові частини та склади);

Категорія Д – об'єкти, що знаходяться у розпорядженні органів безпеки.

Цікавим є те, що Естонія не використовує термін „критична інфраструктура", натомість застосовує таку формулу: *захист інфраструктури критичної важливої інформації (ІКВІ)* – гарантування, того, що важливі з погляду держави мережеві та інформаційні системи працюють без перебоїв.

Мета і дії:

- збір інформації щодо ІКВІ та управління нею;
- складання огляду ризиків ІКВІ за галузями;
- секторальне залучення постачальників послуг щодо обміну інформацією;
- розроблення заходів безпеки;
- складання інструкцій і демонстраційних матеріалів;
- консультація постачальників послуг щодо сутності і надання рекомендацій зі складання аналізу ризиків і більш ефективному застосуванню заходів безпеки;
- підвищення усвідомленості кібербезпеки.

Адміністративно-правове регулювання державної інфраструктурної політики Естонії в інформаційній та кібернетичній сферах здійснюється такими актами [6]:

1) *Закон Естонії „Про кібербезпеку"* [7] – передбачає обов'язки постачальників істотно важливих послуг при забезпечення безпеки мережевих та інформаційних систем, а також основи інформування про суттєві кіберінциденти, в т.ч. уточнює критерії кіберінцидента із істотним впливом. Також закон визначає завдання Департаменту державної інфосистеми щодо координації забезпечення кібербезпеки і в організації транскордонного співробітництва;

2) *Стратегія з кібербезпеки на 2014-2017 роки* [8] – зосереджена на таких трьох ключових сферах: 1) забезпечення життєво важливих послуг; 2) підвищення ефективності боротьби з кіберзлочинністю; 3) розроблення можливостей та спроможностей державної оборони. Одним із головних завдань Стратегії виступає опис системи заходів із безперебійної роботи та стійкості життєво важливих послуг і щодо захисту інфраструктури критичної важливої інформації від кіберзагроз. Увагу в документі також зосереджено на інфотехнологічні перехресні залежності життєво важливих послуг, забезпечення яких не залежить від наявних у Естонії можливостей;

3) *Постанова міністра підприємництва та інфотехнологій „Вимоги до аналізу ризиків мережевих та інформаційних систем та опис заходів безпеки"* [9] – встановлює вимоги до складання аналізу ризиків мережевих та інформаційних систем, що використовується для надання послуг, перерахованих в Законі про кібербезпеку, описують організаційні, інфотехнологічні і фізичні заходи безпеки.

Також суспільні відносини у сфері ДІФСП регулюють такі Закони Естонії:

1. Закон «Про захист персональних даних»
2. Закон «Про електронні платіжні системи»
3. Закон «Про електронні повідомлення»
4. Закон «Про послуги інформаційного суспільства»

Естонія також здійснює активне міжнародне співробітництво у цій галузі. Важливим виступає співробітництво із стратегічним партнером Естонії – США. Ініціатива зі співробітництва була ініційована на зустрічі глав держав Естонії, Литви та Латвії та Президента США Барака Обами у серпні 2013 року. Метою зустрічі став обмін досвідом в контексті активізації безпекового діалогу між країнами Балтійського регіону та США

Також Естонія бере активну участь у Об'єднаному центрі передових технологій з кібероборони НАТО.

Окремо слід сказати і про участь у в Організації Стратком, яка забезпечує реалізацію концепції стратегічних комунікацій у найбільш важливих сферах життєдіяльності, в тому числі і стратегічної інфраструктури [10].

Окремо слід згадати і про співробітництво з TERENA25 , TF-CSIRT

2. Державна інфраструктурна політика Латвійської республіки

Питаннями критичної інфраструктури в ***Латвії*** опікується Міжвідомча комісія з національної безпеки [11].

Комісія є колегіальним консультативним органом, який оцінює та формує перелік об'єктів критичної інфраструктури, включаючи європейську критичну інфраструктуру, та заходи безпеки. До складу комісії входять уповноважені особи з таких державних установ: Міністерство оборони, Міністерство закордонних справ, Міністерство економіки, Міністерства фінансів, Міністерство внутрішніх справ, Міністерство транспорту, Міністерство юстиції, Міністерство охорони здоров'я, Міністерство охорони навколишнього природного середовища та регіонального розвитку, Служба державної безпеки, Служба військової розвідки і безпеки, Національні Збройні Сили, Бюро захисту Конституції, Державна пожежно-рятувальна служба, Державна поліція, Інститут з питань захисту інформаційних технологій ЛР та Банк Латвії.

Цікавим фактом є те, що перелік об'єктів критичної інфраструктури в Латвії становить державну таємницю. Таким чином можемо констатувати, що Латвія теж використовує об'єктну модель ДІФСП, більше того із застосуванням особливих адміністративно-правових засобів.

У Латвійській Республіці нормативне регулювання функціонування системи захисту критичної інфраструктури здійснюється з врахуванням відповідних нормативних документів ЄС (Директива Ради Європи 2008/114/ЄС від 08.12.2008 р. «Щодо визначення та призначення європейських критичних інфраструктур й оцінки необхідності поліпшення їх захисту») та НАТО.

На національному рівні нормативно-правову базу в цій сфері складають:

– *Концепція національної безпеки Латвійської республіки від 26.11.2015 р. (Розділи 4.2, 4.7 та 4.8)*. Документ, серед іншого, визначає перелік основних поточних загроз національній безпеці Латвії в різних сферах (вплив третіх країн, терористична загроза, у тому числі в інформаційному та кібернетичному просторах), а також заходів на державному рівні, спрямованих на нейтралізацію вказаних загроз.

– *Закон Латвійської Республіки «Про національні інформаційні системи" від 02.05.2002 р.* Даний нормативно-правовий акт спрямований на регулювання суспільних відносин із забезпечення належного рівня доступу та якості інформації, що надається державними та місцевими органами влади в державних інформаційних системах. Документ визначає порядок створення, реєстрації, функціонування, реорганізацію і ліквідацію державних інформаційних систем; права і обов'язків її та користувачів; забезпечення безпеки користування та обігу інформації в системах.

– *Постанова Кабінету Міністрів Латвійської Республіки від 28.07.2015 р. № 442 «Про порядок забезпечення систем інформаційно-комунікаційних технологій мінімальним вимогам безпеки».* У даному нормативно-правовому акті регулюються суспільні відносини у сфері формування вимог та встановлення порядку забезпечення безпеки для систем поширення інформації та комунікації, а також порядок забезпечення дотримання відповідності систем органів державної та місцевої влади цим вимогам. Однак цікавим є те, що цей порядок не поширюється на системи інформаційно-комунікаційних технологій для обробки або збереження інформації з обмеженим доступом НАТО, ЄС та іноземних інституцій.

– *Постанова Кабінету Міністрів Латвійської республіки від 01.02.2011 р. № 100 «Про порядок планування і реалізації заходів безпеки для об'єктів критичної інфраструктури»*. Ця Постанова спрямована на забезпечення реалізації положень Закону «Про захист інформаційних технологій» й визначає порядок розроблення та реалізації заходів безпеки для об'єктів критичної інфраструктури в сфері інформаційних технологій.

– *Постанова Кабінету Міністрів Латвійської Республіки від 01.06.2010 р. № 496 «Про заходи планування та впровадження критичної інфраструктури, включаючи європейську критичну інфраструктуру".* Нормативний акт регламентує склад, завдання та повноваження

Міжвідомчої комісії з національної безпеки Латвійської республіки, а також інших органів державної влади в сфері забезпечення безпеки критичної інфраструктури.

Для перевірки систем безпеки критичної інфраструктури та кібербезпеки Інститутом з питань захисту інформаційних технологій Латвійської Республіки у співпраці з Центром підвищення кваліфікації кіберзахисту НАТО в рамках загальної міжнародної програми кіберзахисту «Locked Shields» щорічно в країнах Балтії проводяться тематичні навчання «Crossed Swords». У 2018 р. навчання проходили в Латвії, у 2019 р. – в Естонії. В ході цьогорічних навчань відпрацьовувались сценарії відбиття кібернетичних нападів на об'єкти критичної інфраструктури за участі близько 100 експертів з 21 країни.

3. Державна інфраструктурна політика Литовської республіки

У ще одній Балтійській державі – Литві – також левова частка уваги в рамках реалізації державної інфраструктурної політики належить питанням забезпечення безпеки в Литовській Республіці об'єктів критичної інфраструктури у сфері кібернетичної безпеки, що покладено на Міністерство оборони Литовської Республіки.

З метою ефективної реалізації визначених завдань кібербезпеки, з початку січня 2018 року в МО Литовської Республіки були створені Департамент кібернетичної безпеки та інформаційних технологій, Служба інформаційних технологій та реформований Національний центр кібернетичної безпеки (НЦКБ).

Для забезпечення безпеки інформаційних мереж державних об'єктів критичної інфраструктури, МО Литовської республіки на теперішній час реалізує проект створення захищеної державної мережі обміну даними (Safe State Data Network), управління якою буде здійснювати Міністерство оборони Литовської Республіки та Державний центр телекомунікацій, підпорядкований МО (колишня державна компанія "Infostruktūra").

22.05.2019 Уряд Литовської Республіки затвердив перелік установ, які визначені користувачами захищеної державної мережі обміну даними (Safe State Data Network). За наявною інформацією з відкритих джерел, до зазначеного переліку включено 451 установу, на які покладені функції кризового реагування під час надзвичайних ситуацій, стихійних лих, природних та техногенних катастроф, мобілізації, війни та інших критичних інцидентів:

– органи державної влади та їх окремі структурні підрозділи;
– органи управління силових структур;
– органи муніципальної влади;
– об'єкти енергетичної інфраструктури;
– медичні заклади;
– об'єкти транспортної інфраструктури;
– інші установи.

Відповідно до Закону Литовської республіки „Про управління державними інформаційними ресурсами" передбачається, що зазначені установи будуть використовувати виключно послуги комунікації, які надаються захищеною державною мережею обміну даними. Підключення до інших загальнодоступних систем комунікацій планується здійснювати також через захищену мережу.

Висновки та пропозиції

В *Естонії* хоча дотично і згадується про Директиву Європейського Союзу 2008/114/ЄС») [12], в цілому уникають застосування терміну „критична інфраструктура", надаючи перевагу терміну „інфраструктура критичної важливої інформації", тобто прикметник „критичний" щодо інфраструктури не застосовується. Також примітним є використання таких термінів, як „істотно важливі послуги", „життєво важливі послуги".

Характерним є те, що Естонія робить на голос на забезпеченні безпеки інфраструктури [13], причому щодо інфраструктури наголос робиться саме на інформаційній. Це є важливим і таким, що відповідає тенденціям розвитку інформаційного суспільства, а також рівню кіберглобалізації. Для України є важливим вивчення досвіду міжнародної співпраці у даному напрямі.

Естонія використовую *об'єктну* модель ДІФСП.

В Латвійській республіці, так само як і в Естонії левова частка увагу при формуванні державної інфраструктурної політики приділена забезпеченню безпеки об'єктів критичної інфраструктури в інформаційній та кібернетичній сфері.

У даній державі перелік об'єктів критичної інфраструктури є таємним і на наш погляд це є вірним, адже застосування додаткових режимів захисту даної категорії об'єктів свідчить про налагоджені інституційні спроможності держави в реалізації визначеної політики.

Важливим є те, що в Латвії майже не використовують термін „захист критичної інфрастурктури", натомість всюди застосовується термін безпека інфраструктури в інформаційній та інших сферах. Також можемо підкреслити, що використання терміну „критична інфраструктура" також відбувається лише в аспекті формування безпекових механізмів разом із НАТО та ЄС. Тобто відбувається калькування поняття.

Так само як і в Естонії, в Латвії використовується *об'єктна модель ДІФСП*.

На поточному етапі Латвія вбачає першочергову загрозу для об'єктів критичної інфраструктури з боку безпілотних літальних апаратів (насамперед, несанкціонована фото– та відеозйомка) й працює над удосконаленням чинної нормативно-правової бази, що регулює сферу використання БПЛА.

У цьому аспекті значна увага приділена міжнародному співробітництву.

Як і в інших двох Балтійських країнах питання забезпечення саме кібернетичної безпеки державних об'єктів критичної інфраструктури на теперішній час є одним із пріоритетів діяльності керівництва Литовської Республіки у сфері національної безпеки. Враховуючи чутливість цього питання, значна частина інформації, що його стосується, має гриф обмеженого доступу, так само і як і а Латвійській Республіці.

Також характерним є використання інструментарію безпекової політики при реалізації ДІФСП, а також об'єктної моделі.

Так само, як і інші Балтійські країни, важливим напрямом ДІФСП виступає *міжнародне співробітництво*. Так, зокрема, ЄС ініціював старт 17 проектів у сфері оборони та безпеки. Йдеться про проекти в рамках ініціативи PESCO (Permanent Structured Cooperation) – ініціативи постійного структурного співробітництва, механізм якого було запущено 6 березня 2017 року. Цікавим є те, що дана ініціатива складається із двох органічних частин: зобов'язань і проектів. Участь є добровільною, до нього приєдналися 25 країн (окрім Великої Британії, Данії та Мальти). Причому кожна держава взяла на себе 20 зобов'язань. Кожен із проектів проводить одна країна, решта ж 24 можуть добровільно до нього приєднуватися.

Зокрема в рамках одного з них Литва та шість інших держав працюють спільно над створенням груп швидкого реагування з кібербезпеки. Вони мають допомагати долати наслідки кібератак на комп'ютерні мережі як воєнного призначення, так і інших державних органів, а також цивільну інфраструктуру. Литва постійно стає об'єктом кібератак. Прикладом стало розповсюдження феків про міністра оборони Литовської Республіки Раймундаса Каробліса про те, начебто він гомосексуал. Серед отримувачів цих листів-фейків був також і Президент Литви, але окрім самої фейкової новини. Ці повідомлення містили вірус, за допомогою якого хакери прагнули отримати доступ до даних політиків. Сліди хакерів на думку міністра, ведуть в Росію [14].

Україна також має розглянути механізми своєї участі в різних формах у даних проектах, що наблизить її до європейських стандартів забезпечення безпеки стратегічної інфраструктури.

Є спільний досвід у програмах із захисту критичної інфрастурктури у Литви з Україною. Зокрема у 2017 році розглядалося питання вдосконалення методів захисту стратегічних об'єктів в умовах ведення «гібридної війни» РФ.

Представники Служби безпеки України та Департаменту державної безпеки Литви провели зустріч щодо захисту критичної інфраструктури. «Делегація Служби безпеки України для перейманння досвіду спецслужб Євросоюзу у сфері захисту критичної інфраструктури взяла участь у робочій зустрічі з представниками Департаменту державної безпеки Литовської Республіки. Сторони розглянули питання вдосконалення методів захисту стратегічних об'єктів в умовах ведення Росією «гібридної війни» проти нашої країни» [15].

Як зазначається, представники спецслужб України та Литви виробили нові механізми з блокування і припинення посягань на інфраструктурні об'єкти. Крім того, плануються подальші міжвідомчі заходи з локалізації загроз і викликів національній безпеці обох держав.

У рамках зустрічі, зокрема, обговорювалися напрямки практичної реалізації литовського закону «Про підприємства та об'єкти, які є стратегічно важливими для національної безпеки, та інші підприємства, які є важливими для національної безпеки». Відповідно до закону, головними пріоритетами національної безпеки Литви є, зокрема, захист незалежності та суверенітету держави, європейська та трансатлантична інтеграція, зменшення загроз і ризиків в енергетичному й інших секторах, які мають вирішальне значення для державної безпеки.

«На переконання представників литовської спецслужби, реалізація таких ініціатив дозволить наблизити СБУ в контексті її реформування до стандартів ЄС та НАТО, підвищить рівень сумісності із закордонними партнерами і забезпечить виконання спільних завдань із захисту критичної інфраструктури» [15].

Список використаної літератури:

1. Гібридні загрози Україні і суспільна безпека. досвід ЄС і східного партнерства Аналітичний документ / За загальною редакцією В. Мартинюка (керівника проекту). Київ, 2018. 106 с.
2. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду / В.О. Євсєєв // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2016. – № 4(49). – С. 168-172.
3. 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.
4. Кібербезпека: світові тенденції та виклики для України – http://www.niss.gov.ua/articles/510/.
5. https://www.ria.ee/en.html.
6. https://www.ria.ee/ru/kiberbezopasnost/zashchita-infrastruktury-kriticheski-vazhnoy-informacii.html.
7. Küberturvalisuse seadus (lühend – KüTS) // Режим доступу: https://www.riigiteataja.ee/akt/122052018001.
8. Küberjulgeoleku strateegia 2014-2017 // Режим доступу : https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf
9. Võrgu– ja infosüsteemide riskianalüüsi nõuded ning turvameetmete kirjeldus Vastu võetud 05.07.2018 nr 40 // Режим доступу : https://www.riigiteataja.ee/akt/110072018006/
10. https://www.stratcomcoe.org/
11. Cyber Security Strategy of Latvia 2014-2018. URL: www.enisa.europa.eu/topics/national-cybersecurity-strategies/ncss-map/lv-ncss.; NATO Strategic Communications Centre of Excellence Riga, Latvia. URL: http://www. stratcomcoe.org/.; CERT-LT URL: https://www.cert.lt/en/.
12. NÕUKOGU DIREKTIIV 2008/114/EÜ, 8. detsember 2008, Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta // Режим доступу : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ET:PDF.
13. The Estonian Informatics Centre became the Estonian Information System's Authority. 16.06.2011. URL: https://www.ria.ee/en/theestonian-informatics-centre-became-theestonianinformation-systems-authority.htm.
14. Как Литва будет помогать Евросоюзу защищаться от кибератак // Режим доступу : https://www.dw.com/ru/%D0%BA%D0%B0%D0%BA-%D0%BB%D0%B8%D1%82%D0%B2%D0%B0-%/.
15. Спецслужби України та Литви провели зустріч щодо захисту критичної інфраструктури // Режим доступу : https://www.rbc.ua/ukr/news/spetssluzhby-ukrainy-litvy-proveli-vstrechu-1496057641.html/.

Zubko H. State infrastructure policy: an experience of the Baltic countries

The article substantiates the features of implementing the state infrastructure policy in the area of strategic infrastructure security. The author provides similarities and differences in introducing this policy in the Baltic countries.

The research states that in Estonia, the System Information Authority is responsible for carrying out the state infrastructure policy. Interestingly, Estonia doesn't use the term "critical infrastructure"; it applies the following formula instead – critical information protection (CIP), a guarantee that state-important network and information systems keep the operations up and running.

The author has found that in Latvia, the Interdepartmental Commission on the National Security deals with the issues of critical infrastructure. The Commission is a collegiate advisory body, which assesses and forms a list of critical infrastructure entities, including the European critical infrastructure, and security measures.

Another Baltic country – Lithuania – in the context of implementing the state infrastructure policy, the lion's share of attention belongs to the safety and security of critical infrastructure entities in the Republic of Lithuania that is entrusted to the Ministry of Defense of the Republic of Lithuania.

The article has analyzed the state of statutory support of the realization of such activity and established that a framework Law of Ukraine "On Strategic Infrastructure Security" should be approved for effective partnership cooperation in the area of critical infrastructure protection. It has established that an entity-based policy is the most widespread model of the state infrastructure policy. Moreover, special additional legal mechanisms of the enforcement of infrastructure security have been identified.

Key words: *state infrastructure policy, strategic infrastructure, critical infrastructure of Lithuania, protection of critical infrastructure of Estonia, international cooperation.*