УДК 339.972:351.746.1061.1ЄС

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В БЕЗПЕКОВІЙ ПОЛІТИЦІ КРАЇН ЄС

Бірюков Дмитро Сергійович,
кандидат технічних наук

Розглядаються політичні аспекти здійснення захисту критичної інфраструктури в країнах ЄС та на загальноєвропейському рівні. Досліджено становлення балансу інтересів країн ЄС щодо розвитку загальноєвропейських норм захисту критичної інфраструктури. Визначені основні пріоритети безпекової політики країн ЄС щодо захисту критичної інфраструктури, особливості її здійснення, основні внутрішні та зовнішні фактори, що впливають на її формування. Показано, що, на відміну від наднаціонального загальноєвропейського рівня, в окремих країнах ЄС захист критичної інфраструктури був впроваджений у більш повній формі, інтегрований у стратегію національної безпеки та на практиці реалізований у правовому полі та інституційно.

Ключові слова: **національна безпека, ЄС, критична інфраструктура.**

Dmytro Biriukov

CRITICAL INFRASTRUCTURE PROTECTION IN THE SECURITY POLICY OF THE EU MEMBER STATES.

This paper considers the political aspects of the implementation of critical infrastructure protection in the EU member states as well as at the European level. The formation of the balance of interests of the EU member states on the development of the European norms for critical infrastructure protection is investigated. The main priorities of the EU member states` security policy in a field of critical infrastructure protection, particularly its implementation, the major internal and external factors affecting its forming, were described. It is shown that in contrast to the supranational European level critical infrastructure protection has been implemented in a more complete manner in some EU member states, it was integrated into the national security strategy and implemented in practice within the legal framework and institutionally.

Keywords: **national security, EU, critical infrastructure.**

Шлях євроатлантичної інтеграції є незворотним для нашої держави, це цивілізаційний вибір, який зробив і обстоює ціною значних втрат український народ. За останні два роки країна зробила рішучі кроки у напрямку зближення із ЄС, водночас, із входженням до ЄС Україна не повинна «розмитися» і «втратити себе» на загальноєвропейському просторі. Отже, вкрай необхідно розуміти, яким чином національні інтереси різних країн ЄС узгоджуються в рамках функціонування даної наднаціональної структури.

Питання інтеграції України в євроатлантичні та європейські структури безпеки, окремі аспекти європейської системи безпеки та оборони досліджувалися відомими вітчизняними науковцями, теоретиками і практиками в сфері національної безпеки, серед яких О. С. Бодрук, О. С. Власюк, В. П. Горбулін, О. М. Гончаренко, В. М. Грубов, О. В. Литвиненко, К. А. Кононенко, В. В. Копійка, Б. О. Парахонський, Г. М. Перепелиця, Г. М. Яворська, І. А. Храбан та ін.

Останніми роками термін «критична інфраструктура» дедалі частіше згадується у вітчизняних експертних колах. Суттєвим поштовхом осмислення стала публікація Зеленої книги, яка з огляду на свій жанр спровокувала як наукову дискусію, так і обговорення концепції серед практиків – державних управлінців [1]. Як відзначає Ян Мецгер, захист критичної інфраструктури є міжгалузевим завданням, він може розглядатися в таких вимірах, як економічний, технологічний, правовий, безпековий (зокрема, забезпечення правопорядку, оборона

та цивільний захист) [2, 201]. Виходячи з очевидної тези про те, що критична інфраструктура, весь спектр питань, пов'язаних з її функціонуванням та захистом, більшою чи меншою мірою впливають на досягнення економічних та політичних цілей і сподівань різноманітних акторів (держави, бізнесу, суспільства), можна говорити про критичну інфраструктуру як про окремий об'єкт дослідження в теорії національної безпеки.

У захисті критичної інфраструктури бачать інструмент, за допомогою якого можна істотно впливати на стан національної безпеки, говорять про важливе прикладне значення цієї концепції, зазначають, що вона дозволяє операціоналізувати національні інтереси, тобто відстежувати вплив зміни стану такої інфраструктури на ступінь досягнення цілей, що визначаються національними інтересами [3, 19–41].

Розвиток нормативно-правових основ захисту критичної інфраструктури в ЄС, процесу імплементації загальноєвропейських вимог у законодавства окремих країн ЄС здійснив Алесандро Лазарі [4]. Детальний аналіз цього процесу поданий також в офіційних документах апарату Європейської Комісії [5], публікаціях дослідницьких центрів з питань безпеки [6].

Мета даного дослідження – визначити, яким чином захист критичної інфраструктури присутній як елемент політики в сфері безпеки в країнах-членах ЄС та на рівні ЄС.

Розглянемо спочатку питання загальноєвропейської безпекової політики щодо захисту критичної інфраструктури. Тут слід зауважити, що ЄС – наднаціональне утворення, що поступово створює власні інструменти безпекової і оборонної політики. Як відзначалось у звіті Служби досліджень Конгресу США, «розвиток Спільної зовнішньої та безпекової політики (СЗБП) Європейського Союзу протягом двох десятиліть дозволив ЄС розвинутися поза межі суто економічного актора, і його роль у міжнародних відносинах з безпекових питань додала новий важливий компонент до його ідентичності. Водночас, основним викликом для СЗБП досі залишається формування та підтримка узгодженої позиції суверенних держав» [7, 8]. Окремі країни ЄС можуть мати різні погляди, преференції та пріоритети щодо вибору «кращого» спільного курсу.

У першій редакції Європейської стратегії безпеки (2003 рік) у стислій характеристиці глобальних викликів зазначається, що із завершенням «холодної війни» змінилося безпекове середовище. Для нього характерні більш відкриті кордони, прискорений рух товарів та інвестицій, розвиток технологій та поширення демократії, а також більший вплив недержавних акторів на міждержавні стосунки, що «підвищило залежність, а отже, і вразливість, європейської взаємопов'язаної інфраструктури в галузях транспорту, енергетики, телекомунікацій та ін.» [8, 2]. Отже, слушно ставити питання про те, що захист критичної інфраструктури, а точніше, реалізація цього захисту на рівні ЄС, є свого роду «захистом формату ЄС для європейської інтеграції» [9, 12].

Можна стверджувати, що *захист загальноєвропейської критичної інфраструктури розвивається як напрям безпекової політики в рамках розбудови загальної архітектури безпеки в ЄС* на основі положень, закладених у Стокгольмській програмі [10] та Стратегії внутрішньої безпеки ЄС (щодо досягнення цілей «2. Запобігання тероризму, радикалізації і вербуванню» та «5. Підвищення стійкості Європи до кризи та стихійних лих») [11]. Це пов'язано з тим, якою має бути безпекова політика ЄС, якою мірою вона має спрямовувати політику окремих країн ЄС. Але, як відзначає Алесандро Лазарі, на порядку денному безпекової політики ЄС питання здійснення практичних кроків із захисту критичної інфраструктури опинилося, «тільки-но виник страх» того, що негативні наслідки, викликані припиненням функціонування або аварією на об'єкті критичної інфраструктури, поширяться за межі окремої країни ЄС на інші держави [4, 44]. Подією,

що прискорила таке розуміння, стали терористичні акти в березні 2004 року в Мадриді. Вони «вивели» питання захисту критичної інфраструктури на політичний рівень. Так, у червні 2004 року Європейська Рада звернулася до Європейської Комісії (ЄК) з дорученням підготувати стратегію захисту критичної інфраструктури. Перша ініціатива, підготовлена ЄК, мала назву «Захист критичної інфраструктури в боротьбі з тероризмом» [12]. У ній вказувалося, що започатковується Європейська програма захисту критичної інфраструктури (*EPCIP*) з метою визначення такої інфраструктури, проведення аналізу вразливостей та взаємозалежності її елементів, підготовки рішень щодо підвищення рівня захисту, виходячи із комплексного аналізу загроз (англ. *all hazard approach*). У документі зазначалося, що правоохоронні органи та служби цивільного захисту країн ЄС мають забезпечити включення цієї програми як складової частини процесу планування та підвищення усвідомленості щодо терористичних загроз. Питання створення EPCIP, визначення її цілей, принципів та механізмів побудови на загальноєвропейському рівні захисту критичної інфраструктури були детально висвітлені в Зеленій книзі, опублікованій ЄК в листопаді 2005 року [13].

Нині спеціальним документом ЄК, що спрямований на внормування організації захисту критичної інфраструктури на загальноєвропейському рівні, є Директива 2008/114 [14]. Вона встановлює вимоги до країн ЄС щодо визначення загальноєвропейської критичної інфраструктури та інформування з цих питань, додаткові вимоги до операторів (суб'єктів господарювання, що володіють або управляють об'єктами критичної інфраструктури) щодо наявності та ґрунтовності планів безпеки.

Хоча Директива 2008/114 і була розроблена на основі згаданої Зеленої книги, вона істотно звузила викладені в ній положення. Наприклад, країни-члени ЄС зобов'язані визначати об'єкти загальноєвропейської критичної інфраструктури на своїй території лише в двох секторах (енергетика та транспорт), тоді як у Зеленій книзі були названі 11 секторів.

У звіті Комітету з міжнародних відносин Європейського парламенту відзначається, що більшість стратегічних ресурсів, об'єктів критичної інфраструктури та потужностей перебувають під управлінням країн-членів ЄС, і, відповідно, їхнє бажання посилювати кооперацію є першорядним для забезпечення загальноєвропейської безпеки [15, 11]. Мабуть, тому в Директиві 2008/114/ЄК зазначається, що основна й остаточна відповідальність за захист загальноєвропейської критичної інфраструктури покладається на країни ЄС та власників (операторів) таких об'єктів [14]. Так само, визначення переліку об'єктів, які країни ЄС вважають за доцільне віднести до загальноєвропейської критичної інфраструктури, покладається на них, а ЄК при цьому може лише надавати консультативну допомогу в разі звернення країни-члена [4, 48].

Насправді, поступове розширення переліку секторів загальноєвропейської критичної інфраструктури можливе лише шляхом, охарактеризованим у звіті Центру європейських політичних досліджень: там ідеться про те, що Європейська Комісія має здійснити ретельно пророблений «тест субсидіарності», чітко визначити для кожного сектору економіки ті питання щодо захисту критичної інфраструктури, з яких країни мають бажання діяти узгоджено, і ті, що можуть залишатися в національній компетенції [6, 1]. Включення певних об'єктів до загальноєвропейської критичної інфраструктури тягне і зобов'язання щодо підвищених вимог до їх безпеки, тому зрозумілим є певна «інертність» країн, незначна кількість таких об'єктів [5, 4].

Напевно, захист критичної інфраструктури на рівні ЄС і надалі буде здійснюватися найбільш інтенсивно за такими напрямками, де є як загальне розуміння значущості можливих загроз для національної безпеки країн ЄС, так і розуміння пріоритетності міжна-

родних зусиль (боротьба з тероризмом та забезпечення кібербезпеки). Тут слід наголосити на тих значних організаційних і нормативно-правових зрушеннях, що відбулися за десятиліття як на рівні ЄС, так і в окремих країнах Європи в напрямку забезпечення кібербезпеки [16].

Водночас, існують й інші міркування стосовно розширення переліку загальноєвропейської критичної інфраструктури, зокрема, поширеною є думка про необхідність визначення критичних потужностей та технологій оборонно-промислового комплексу країн ЄС [15, 13].

На відміну від наднаціонального загальноєвропейського рівня, в окремих країнах ЄС захист критичної інфраструктури був впроваджений у більш повній формі [3, 41–61]. З'ясуємо політичні питання, пов'язані із забезпеченням захисту критичної інфраструктури в країнах ЄС. Першим є *соціально-економічний аспект*. Так, у країнах ЄС метою захисту критичної інфраструктури визначається *забезпечення неперервного надання життєво важливих функцій і послуг суспільству та національній економіці* [3, 46]. Ця теза відображена і в робочому документі апарату ЄК, де зазначається: «Забезпечуючи високий рівень захисту інфраструктури в ЄС та підвищуючи її стійкість (проти всіх загроз та небезпек), ми можемо мінімізувати наслідки втрат сервісів для суспільства в цілому» [5, 2].

Піонерами у розвитку та впровадженні такого підходу можна вважати країни Північної Європи. Наприклад, Норвезький інститут оборонних досліджень (*Forsvarets forskninstitutt*) спільно з Директоратом з питань цивільного захисту, починаючи з кінця 1990-х років публікують дослідження за тематикою «Захист суспільства», в яких, зокрема, визначено найважливіші системи життєзабезпечення, які необхідні сучасному суспільству для його стабільного функціонування; досліджуються взаємозв'язки між такими системами [17, 55]. Так само у Фінляндії кінцевою метою визначається забезпечення функцій, життєво важливих для суспільства, відповідно критична інфраструктура – це матеріальна основа для надання таких функцій [18], а в Німеччині ця теза включена у саме визначення терміну «критична інфраструктура», більше того, частина секторів інфраструктури віднесена до групи «соціально-економічні послуги» [19, 7].

Особливістю державної політики щодо забезпечення функціонування критичної інфраструктури є створення таких нормативних умов, за яких у надзвичайних ситуаціях, коли звичайні правила ринкової економіки не діють, буде збережений контроль над функціями інфраструктури [19, 8]. Цього можна досягти лише шляхом *створення ефективних умов державно-приватного партнерства*.

Тут слід відзначити, що в країнах ЄС значна частина об'єктів критичної інфраструктури перебуває у приватній власності, і завдання урядів полягає у створенні відповідного нормативно-правового поля, що забезпечить стійкість такої інфраструктури до загроз різного характеру [19, 8, 20, 44]. Відтак, уряд в особі призначених органів виконавчої влади відповідає за формування стратегічного підходу до забезпечення безпеки об'єктів у всіх секторах критичної інфраструктури та несе відповідальність (політичну) за наслідки реалізації такого підходу.

Також уряд визначає пріоритети та формує програми в сфері безпеки для об'єктів, функціонування яких пов'язане з найбільшим ризиком, а відповідальні органи можуть бути залучені до визначення на «тактичному рівні» достатнього переліку безпекових заходів. Натомість, ризики, пов'язані із забезпеченням безпеки об'єктів, в першу чергу, лежать на їх власниках або операторах, які несуть повну відповідальність за ефективність планів та застосування заходів, що відбивають рекомендації та вказівки органів виконавчої влади.

Проблематика протистояння країнам ЄС «прихованим» впливам на національну безпеку з боку РФ відбивається і на питаннях захисту критичної інфраструктури. Так, у Стратегії націо-

нальної безпеки Великої Британії зазначається, що іноземні спецслужби продовжують здійснювати ворожу діяльність, яка загрожує в т.ч. функціонуванню критичної інфраструктури, з метою вплинути на політику уряду, викрасти комерційні таємниці, зашкодити національній економіці [20, 18]. В умовах ліберальної ринкової економіки вплив на політику держави шляхом використання критичної інфраструктури здійснюють і недержавні актори. Такий вплив стає досить помітним у країнах ЄС, що за економічними потужностями відстають від трійки лідерів, наприклад, в Хорватії [21, 26]. Тому загрози, що їх може спричинити контроль за критичною інфраструктурою з боку іноземних компаній (в т.ч. тих, що перебувають у державній власності), усвідомлюється і відображений у стратегічних документах окремих країн ЄС.

Наприклад, у Стратегії національної безпеки Чеської Республіки зазначається, що ця держава «відслідковує іноземні інвестиції в окремі сектори критичної інфраструктури та стратегічні компанії з метою відвернути загрозу неправомірного використання таких інвестицій як каналу, через який іноземні сили зможуть досягати своїх економічних та політичних інтересів за рахунок Чеської Республіки» [22, ст. 75].

Прикладом, що наочно демонструє «провал» безпекової політики, є відставка уряду Бойка Борисова в Болгарії (лютий 2013 року), якій передували масові протести громадян через підвищення тарифів на електроенергію на фоні погіршення соціально-економічних умов життя. Тут потрібно зазначити, що тарифи підняла приватна Національна електрична компанія Болгарії, яка була змушена до того закрити чотири блоки АЕС «Козлодуй» через їх невідповідність європейським нормам безпеки та відмовитися від будівництва АЕС «Белене», а також те, що важливими постачальниками електроенергії на болгарський ринок на той момент були іноземні компанії – чеські *CEZ* та *EnergoPro* й австрійська *EVN*.

Існує певна *пов'язаність завдань державної політики щодо захисту та забезпечення стійкого розвитку критичної інфраструктури*. Наприклад, у Великій Британії уряд розробив План розвитку національної інфраструктури, в якому йдеться про необхідність забезпечення стійкості та безпеки об'єктів, а визначення переліку (ідентифікація) критичної інфраструктури розглядається як спосіб пріоритизації ресурсів [23, 127]. Тут важливим є питання балансу «посилення захисту – ціна таких заходів». Наприклад, у керівному документі, підготовленому урядом Великої Британії, вказується: «Основна відповідальність за стійкість критичної інфраструктури покладається на власників та операторів, але уряд, регулюючі органи і промислові компанії повинні працювати разом, щоб забезпечити інвестиції в інфраструктуру з урахуванням потреб у безпеці і стабільності» [24, 9].

У деяких країнах ЄС через особливості державного устрою важливим неабиякої ваги набуває питання про *делегування деяких безпекових функцій від «центру» до регіонів*. Наприклад, у Німеччині, в *Національній стратегії захисту критичної інфраструктури*, вказується, що вдосконалення захисту критичної інфраструктури є спільною відповідальністю Федерального уряду та урядів земель [19]. На регіональному рівні можуть бути прийняті та виконуватися власні стратегії та програми захисту критичної інфраструктури, прикладом цього є Шотландія [25]. У цьому аспекті цікавим є питання про розподіл повноважень із захисту критичної інфраструктури між центральними та регіональними органами влади. Наприклад, місцева поліція, як правило, не відповідає за охорону об'єктів критичної інфраструктури і лише здійснює звичайні функції із забезпечення правопорядку у випадках надзвичайних ситуацій.

Ситуацію в Україні із запровадження захисту критичної інфраструктури відображає згадувана Зелена книга [1]. Можна сказати, що схожа з українською є ситуація у країнах, які теж знаходять-

ся поза ЄС (у Македонії, Сербії, Боснії і Герцеговині), де в національних законодавствах не введено терміну «критична інфраструктура», а низку функцій з цивільного захисту, охорони важливих державних об'єктів, протидії тероризму та кібербезпеки здійснюють окремі відомства [21].

Водночас, слід зазначити, що певні зобов'язання із забезпечення стійкості загальноєвропейської критичної інфраструктури вже взяті нашою державою. Так, у Додатку XXVI Угоди про Асоціацію з Європейським Союзом ідеться про запровадження Механізму раннього попередження надзвичайних ситуацій, які спричиняють значний збій/зупинку у постачанні природного газу, нафти чи електроенергії між Україною та ЄС.

Застосувавши відомий у політології метод *SWOT*-аналізу, можна проаналізувати доцільність імплементації Директиви 2008/114/ЄК в Україні до її вступу в ЄС. Отже, «сильними сторонами» такого рішення можна вважати: запровадження загальновизнаного в країнах ЄС та НАТО підходу, ефект від демонстрації «політичної волі», залученість до процесу оцінки значущості інфраструктури на загальноєвропейському рівні. Водночас «слабкими сторонами» такого рішення є: відсутність «прямих» інструментів від ЄК для посилення безпеки і стійкості інфраструктури в Україні, необхідність підписання окремих угод щодо участі української сторони в *EPCIP*.

Імплементація Директиви 2008/114/ЄК, навіть за умов перебування України поза ЄС, надає такі можливості, як прискорення процесу створення системи захисту критичної інфраструктури Україні, привернення уваги до проблем безпеки і стійкості пріоритетних для ЄС секторів (енергетика, транспорт). Проте можна передбачити і певні загрози, пов'язані з імплементацією цього документу, насамперед, опір з боку операторів інфраструктури (викликаний необхідністю підвищувати рівень безпеки, впроваджувати додаткові з її забезпечення).

Висновки

З огляду на євроатлантичні устремління нашої держави, історичний вибір народу України, підтверджений під час Революції Гідності і протидії агресору, завдання критичного вивчення підходів до забезпечення національної і регіональної безпеки в країнах-членах Євросоюзу та на рівні ЄС є актуальним. Нині питання захисту загальноєвропейської критичної інфраструктури є частиною загальної архітектури безпеки в ЄС, а створення національних систем захисту критичної інфраструктури – невід'ємною частиною забезпечення національної безпеки. Дослідження показує, що в процесі імплементації захисту критичної інфраструктури на рівні ЄС відбувається пошук балансу національних та спільних інтересів країн-членів ЄС. Саме уряди країн ЄС несуть відповідальність за функціонування критичної інфраструктури.

Захист критичної інфраструктури як на загальноєвропейському, так і на національному рівні активізувався, передусім, через необхідність посилення дій за такими трьома напрямками: боротьба з тероризмом, протидія кібер-загрозам, забезпечення енергетичної безпеки.

На відміну від загальноєвропейського рівня, в окремих країнах ЄС захист критичної інфраструктури був упроваджений в розвиненій формі, інтегрований у стратегію національної безпеки та на практиці реалізований у правовому полі та інституційно. На деяких політичних питаннях, пов'язаних із захистом критичної інфраструктури, слід наголосити окремо. Перш за все, пріоритетом захисту декларується забезпечення неперервності соціально значущих функцій та послуг, що їх надає критична інфраструктура суспільству та національній економіці країн ЄС. Роль уряду полягає у формуванні стратегічного підходу до забезпечення безпеки об'єктів у всіх секторах критичної інфраструктури, уряд несе відповідальність (політичну) за наслідки реалізації такого підходу, тоді як остаточна відповідальність (юридична) за безпеку та стійкість інф-

раструктури лежить на власниках (операторах) інфраструктури. Отже, ключовим питанням стає створення умов для ефективного державно-приватного партнерства у сфері безпеки.

Дедалі частіше на питаннях захисту критичної інфраструктури відбивається проблематика протистояння країн Євросоюзу «прихованим» впливам на національну безпеку з боку РФ. Уряди країн ЄС стурбовані впливом зарубіжного капіталу, «темними» сторонами комерційних угод про функціонування передусім енергетичної інфраструктури.

Захист критичної інфраструктури розглядається в країнах ЄС також як необхідна передумова розвитку масштабних інфраструктурних проектів, залучення інвестицій для їх здійснення. І хоча, як правило, одні органи державної влади реалізують економічну політику, а інші – відповідають за забезпечення безпеки і стійкості інфраструктури, на рівні національних планів розвитку інфраструктури питання безпеки враховуються. Для України імплементація загальноєвропейських положень про захист критичної інфраструктури, поряд із зобов'язаннями щодо раннього попередження надзвичайних ситуацій, пов'язаних із зупинками постачання енергоносіїв, які Українська держава вже взяла на себев рамках Угоди про асоціацію, є питанням «доброї волі». Аналіз Директиви 2008/114/ЄК вказує, що поряд із перевагами та можливостями, що відкриває імплементація цього документу, можна передбачити й істотні недоліки та навіть певні загрози.

Список використаних джерел

1. *Зелена* книга з питань захисту критичної інфраструктури в Україні [Електронний ресурс] – НІСД, 2015. – Режим доступу: http://www.niss.gov.ua/
2. *Business* and Security: Public–Private Sector Relationships in a New Security Environment / Edt. A. Bailes, I. Frommelt. – Oxford University Press, 2004. – 328 p.
3. *Концепція* захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні : зб. матеріалів міжнар. наук.-практ. конф. (7-8 листопада 2013 р., Київ – Вишгород). – К. : НІСД, 2014. – 147 с.
4. *Lazari* A. European Critical Infrastructure Protection. – Springer, 2014. – 154 p.
5. *SWD(2013)* 318 final: On a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure [Електронний ресурс]. – EC staff working document. – Режим доступу. – http://ec.europa.eu/
6. *Protecting* critical infrastructure in the EU. – Centre for European Policy Studies, 2010 – 100 p.
7. *The* European Union: Foreign and Security Policy [Електронний ресурс]. Congressional Research Service, 2013. – Режим доступу: https://www.fas.org/sgp/crs/row/R41959.pdf
8. *European* Security Strategy: A Secure Europe in a Better World [Електронний ресурс]. – European Commision, 2003. – Режим доступу: https://www.consilium.europa.eu/
9. *The* Making of Europe's Critical Infrastructure: Common Connections and Shared Vulnerabilities / Edt. P. Högselius, at al. – Palgrave Macmillan, 2013. – 313 p.
10. *The* Stockholm Programme: An Open and Secure Europe Serving and Protecting the Citizens

References

1. *Zelena* knyga z pitan zahystu krytychnoi infrastruktury v Ukraïni (2015) [Green Paper on Critical Infrastructure Protection in Ukraine]. Kyiv, NISS. – Retrieved from http://www.niss.gov.ua/ [inUkrainian].
2. *Bailes, A.,* Frommelt I. (Ed.) Business and Security: Public–Private Sector Relationships in a New Security Environment (2009) . Oxford University Press. – 328 p.
3. *Koncepcija* zahystu krytychnoi infrastruktury: stan, problemy ta perspektyvy yi vprovadzhennja v Ukrayni (2014): Proceedings of the International Scientific Practical Coference (7-8 November 2013, Kyiv – Vyshgorod). – NISS. – 147 p.
4. *Lazari, A.* European Critical Infrastructure Protection (2014). Springer..
5. *SWD(2013)* 318 final: On a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure. – EC staff working document. – Retrieved from http://ec.europa.eu/
6. *Protecting* critical infrastructure in the EU (2010). Brussels, Centre for European Policy Studies.
7. *The* European Union: Foreign and Security Policy. Congressional Research Service, (2013). – Retrieved from https://www.fas.org/sgp/crs/row/R41959.pdf
8. *European* Security Strategy: A Secure Europe in a Better World. – European Commission, (2003). – Retrieved from https://www.consilium.europa.eu/
9. *Högselius, P.* (Ed.)The Making of Europe's Critical Infrastructure: Common Connections and Shared Vulnerabilities (2013). London, Palgrave Macmillan.
10. *The* Stockholm Programme: An Open and Secure Europe Serving and Protecting

(Council Document 17024/09) [Електронний ресурс]. – Режим доступу. – http://eur-lex.europa.eu/

11. *COM(2010)* 673 final: The EU Internal Security Strategy in Action: Five steps toward a more secure Europe [Електронний ресурс]. – Communication from the Commission to the European Parliament and the Council. – Режим доступу. – http://eur-lex.europa.eu/

12. *COM(2004)* 702 final: Critical Infrastructure Protection in the fight against terrorism [Електронний ресурс]. – http://eur-lex.europa.eu/

13. *COM(2005)* 576 final: Green paper on a European programme for critical infrastructure protection [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

14. *Directive* 2008/114/EC: On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

15. *INI* 2014/2220: Report on the implementation of the Common Security and Defence Policy (based on the Annual Report from the Council to the European Parliament on the Common Foreign and Security Policy) [Електронний ресурс]. – Committee on Foreign Affairs. – Режим доступу: http://www.europarl.europa.eu/

16. *CIIP* Governance in the European Union Member States [Електронний ресурс]. – ENISA, 2016. – Режим доступу: https://www.enisa.europa.eu/

17. *Beskyttelse* av samfunnet: Sluttrapport [Електронний ресурс]. – Норвежський інститут оборонних досліджень: Заключний звіт «Захист суспільства» – Режим доступу: http://rapporter.ffi.no/rapporter/97/01459.pdf

18. *Government* Resolution 23.11.2006: The strategy for securing the functions vital to society [Електронний ресурс]. – Government of Finland, 2006. – Режим доступу: http://www.webcitation.org/6Q3hh1csj

19. *Nationale* Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) [Електронний ресурс]. – BMI, 2009. – Режим доступу: http://www.kritis.bund.de

20. *National* Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. – Williams Lea Group, 2015. – 94 p.

21. *Proceedings* of the Int. Scientific Conf. «National Critical Infrastructure Protection Regional Perspective» / Edt. I. Dimitrijević, University of Belgrade, Faculty of Security Studies. – Belgrade, 2013. – 57 p.

22. *Security* Strategy of the Czech Republic 2015 [Електронний ресурс]. – Ministry of Foreign Affairs of the Czech Republic. – Режим доступу: http://www.mzv.cz/

23. *National* Infrastructure Plan 2014 [Електронний ресурс]. – HM Treasury, 2014 – Режим доступу: www.gov.uk/

24. *Keeping* the Country Running: Natural Hazards and Infrastructure. – Civil Contingencies Secretariat, Cabinet Office. – https://www.gov.uk/

25. *Secure* and resilient: a strategic framework for critical national infrastructure in Scotland. – Edinburgh: The Scottish Government, 2011. – Режим доступу: http://www.gov.scot/

the Citizens (Council Document 17024/09) Retrieved from http://eur-lex.europa.eu/

11. *COM(2010)* 673 final: The EU Internal Security Strategy in Action: Five steps toward a more secure Europe. – Communication from the Commission to the European Parliament and the Council. – Retrieved from http://eur-lex.europa.eu/

12. *COM(2004)* 702 final: Critical Infrastructure Protection in the fight against terrorism Retrieved from http://eur-lex.europa.eu/

13. *COM(2005)* 576 final: Green paper on a European programme for critical infrastructure protection Retrieved from http://eur-lex.europa.eu/

14. *Directive* 2008/114/EC: On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection Retrieved from http://eur-lex.europa.eu/

15. *INI* 2014/2220: Report on the implementation of the Common Security and Defence Policy (based on the Annual Report from the Council to the European Parliament on the Common Foreign and Security Policy). – Committee on Foreign Affairs. – Retrieved from http://www.europarl.europa.eu/

16. *CIIP* Governance in the European Union Member States. , (2016). Brussels, ENISA – Retrieved from https://www.enisa.europa.eu/

17. *Beskyttelse* av samfunnet: Sluttrapport [Protection of Society: Final Report]. Norwegian Defence Studies Establishment. – Retrieved from http://rapporter.ffi.no/rapporter/97/01459.pdf

18. *Government* Resolution 23.11.2006: The strategy for securing the functions vital to society. – Government of Finland, 2006. – Retrieved from http://www.webcitation.org/6Q3hh1csj

19. *Nationale* Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) [National Strategy on Critical Infrastructure Protection] (2009). Berlin, BMI. – Retrieved from http://www.kritis.bund.de

20. *National* Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom (2015). London, Williams Lea Group.

21. *Dimitrijević, I.* (Ed.) Proceedings of the Int. Scientific Conf. «National Critical Infrastructure Protection Regional Perspective» (2013). Belgrade, University of Belgrade .

22. *Security* Strategy of the Czech Republic 2015 . – Ministry of Foreign Affairs of the Czech Republic. – Retrieved from http://www.mzv.cz/

23. *National* Infrastructure Plan 2014. London, HM Treasury. – Retrieved from www.gov.uk/

24. *Keeping* the Country Running: Natural Hazards and Infrastructure (2011). London, Civil Contingencies Secretariat, Cabinet Office. – Retrieved from https://www.gov.uk/

25. *Secure* and resilient: a strategic framework for critical national infrastructure in Scotland (2011). Edinburgh, The Scottish Government. – Retrieved from http://www.gov.scot/