УДК 351.863+338.246.87

ЄРМЕНЧУК Олександр Петрович

ОСОБЛИВОСТІ ВИБОРУ ОРГАНІЗАЦІЙНОЇ МОДЕЛІ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Постановка проблеми. Вибір для України тієї чи іншої організаційної моделі захисту критичної інфраструктури (ЗКІ) свідчить про доцільність ретельного вивчення наявного зарубіжного досвіду та врахування національних особливостей державотворчих процесів.

Додаткової актуальності цій науковій проблемі надає нагальна необхідність подолання загрозливих явищ у соціально-економічній та інших сферах державного управління, а також створення умов для зростання якості життя громадян, рівня їх захищеності та росту промислового виробництва і новітніх технологій, удосконалення захисту економічного потенціалу держави в умовах гібридної війни, захисту суспільства від різних загроз.

Аналіз останніх досліджень і публікацій. Аналіз європейської практики ЗКІ свідчить, що кожна держава обирає власний шлях побудови системи ЗКІ, зважаючи на загальні світові безпекові тенденції та враховуючи відповідний національний досвід. Захист критичної інфраструктури включає систему скоординованих організаційних, нормативно-правових, адміністративних, пошукових, охоронних, режимних інженерно-технічних, наукових та інших заходів, матеріальних та нематеріальних засобів, спрямованих на забезпечення стійкості та безпеки критичної інфраструктури. Він усіляко має стимулюватися та підтримуватися різними державними механізмами.

За результатами проведеного автором аналізу систем захисту КІ різних держав можна констатувати, що їх спільними притаманними рисами є такі:

1) кожна національна модель системи захисту КІ залежить від особливостей безпекової ситуації в державі, згідно з якою формується національне законодавство і політика у сфері національної безпеки;

2) важливе значення для побудови таких моделей відіграє практика застосування в національному законодавстві та сутність основоположних понять таких, як «національна інфраструктура», «критична інфраструктура», «об'єкти національної та критичної інфраструктури», «захист критичної інфраструктури», «безпека об'єкта критичної інфраструктури», «стійкість об'єкта критичної інфраструктури», «загрози», «потенціал загрози», «ризики», «уразливість об'єкта критичної інфраструктури», «важливість об'єкта» та «наслідки»;

3) система захисту КІ має багаторівневу структуру, яка базується на конституції держави і діяльності системи органів влади;

4) особливе значення для ефективності, повноти та дієвості конкретних заходів із захисту КІ відіграє стан державно-приватного партнерства;

5) важливе значення в діяльності системи захисту КІ відіграють координуючі та інформаційні центри, участь спеціальних правоохоронних органів у захисті критичної інфраструктури;

6) ефективність функціонування та якість прийняття управлінських рішень із захисту КІ залежить від інформаційно-комунікаційної складової цієї системи [1].

Мета статті. Шляхом аналізу міжнародного досвіду запропонувати до вибору в нашій державі організаційної моделі централізованого або децентралізованого захисту об'єктів критичної інфраструктури.

Виклад основного матеріалу. Першопричиною та рушійним механізмом для розбудови системи захисту є необхідність створення можливостей протидії загрозам для КІ. Їх здатність уражати важливі елементи значно впливає на стан економічної безпеки держави та на суспільно-політичні аспекти, зумовлює виникнення складних процесів організаційно-безпекового характеру та залучення до них різних партнерів. Для подальшого злагодженого функціонування в нашій державі цієї системи наразі важливо визначити основні її елементи, їх сутність та зміст і правильно здійснити її побудову [2].

Принциповим для побудови національної системи захисту КІ є обґрунтування понять «національна інфраструктура» та «критична інфраструктура». Під національною інфраструктурою вбачається взаємопов'язана система державного управління та об'єктів інфраструктури, що є основою функціонування держави, її економіки та суспільства. Критична інфраструктура – це система надзвичайно важливих матеріальних та нематеріальних об'єктів національної інфраструктури (а також їх власність та результати діяльності), що забезпечують її стале функціонування, руйнація або пошкодження яких (наявними загрозами) може призвести до людських жертв і значних матеріальних збитків із найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки. Важливо визначити поняття «об'єкт національної інфраструктури», що може об'єднувати в собі державні та приватні підприємства, організації й установи, а також їх власність і результати діяльності, що є складовими єдиного механізму функціонування держави її економіки та суспільства. Автором не випадково застосовується такі поняття, як «власність» та «результати діяльності». Вони поєднують недостатньо вживані у вітчизняному законодавстві складові інфраструктури, а саме: системи та їх частини, мережі, ресурси, вузли тощо.

Аналіз змісту категорії «загрози» для об'єкта КІ дозволяє розуміти їх як наявні або потенційно можливі явища і чинники, що можуть завдати

шкоди такому об'єкту (фізичному або у кіберпросторі), вивести його з ладу або порушити функціонування відповідно до призначення, чим створюють небезпеку життєво важливим національним інтересам України. Доцільно здійснювати їх класифікацію: від характеру походження; мети дій, що їх спричиняють; ступеня поширення; розміру людських втрат та матеріальних збитків; втрат для безпеки життєдіяльності; суспільно-політичних та культурних; втрат для забезпечення державної безпеки та громадського порядку; обсягів ресурсів, необхідних для їх локалізації. Вид загроз та їх можлива інтенсивність враховується при визначенні критичності об'єкта для формування переліку об'єктів КІ.

Узагальнення досвіду провідних країн Європи дозволяє виокремити основні три сфери, що підлягають захисту. Саме в кожній із цих ключових сфер, як правило, створюються та функціонують один чи декілька підрозділів, що здійснюють ЗКІ від загроз, зокрема:

– у сфері державної безпеки чи безпекового характеру (тероризм, диверсії, «навмисна помилка», розвіддіяльність іноземних спецслужб, економічні експансії, економічне та промислове шпигунство, конкурентна розвідка). Вони можуть включати внутрішні загрози та фізичне знищення КІ (при хуліганстві, підпалах, діяльності організованих злочинних угруповань, дії чинника «внутрішнього порушника»);

– від кіберзагроз (інформаційні атаки, кібертероризм);

– від надзвичайних ситуацій (аварії, катастрофи, стихійні лиха, пожежі, епідемії та пандемії, застосування засобів ураження або інші небезпечні події).

Разом з цим потрібно констатувати, що за останні кілька років особливо актуальними для України стають загрози у сфері державної безпеки. Серед них науковці називають: різке збільшення терористичних актів, розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих груп та осіб на економічний, науково-технічний і оборонний потенціал, диверсії та деструктивну злочинну діяльність, намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації тощо.

Попередження, своєчасне виявлення та припинення впливу цих загроз має сприяти більш плідній співпраці між операторами критичної інфраструктури, що є ціллю деструктивних устремлінь, та відповідними безпековими відомствами нашої держави. Протидія зазначеним загрозам входить до повноважень СБ України, розвідувальних та правоохоронних органів, підрозділів із надзвичайних ситуацій тощо, а тому вимагає підвищення продуктивності та удосконалення спільних дій партнерів у цьому напрямку. Саме побудова системи захисту КІ в Україні може відіграти роль рушійної сили у побудові нової системи безпеки та захисту державно-приватних інтересів, а також стати переломним етапом в ментальності пересічних громадян, у якій укоріни-

лася недовіра до спецслужб та правоохоронців, породжена за радянських часів. Причинами цих позитивних зрушень можуть стати спільні заходи з оцінювання ризиків та наслідків, забезпечення стійкості тощо.

З огляду на різні завдання, ролі та відповідальність партнерів у сфері функціонування критичної інфраструктури необхідними є гнучкі, активні та всеохоплюючі партнерські стосунки, спрямовані на підвищення надійності та стійкості критичної інфраструктури [3]. У процесі партнерства держава має бути гарантом захисту та виступати в ролі посередника в інформаційних та комунікаційних процесах, при цьому приватний сектор володіє інформацією щодо актуальних ризиків та загроз їх функціонуванню, що при налагодженому процесі обміну дозволить державі застосовувати ефективні конкретні заходи із захисту [4].

Детальні аспекти взаємодії між партнерами доцільно передбачити в рамках національної Програми захисту критичної інфраструктури, де мають бути зазначені спільні державно-приватні інтереси у забезпеченні безпеки та стійкості критичної інфраструктури. Крім того, зазначений документ стане консолідуючим фактором, оскільки полегшить та скоординує обмін інформацією, вирішення спільних проблем, забезпечить ефективність роботи органів державної влади, органів безпеки та приватного сектору пліч-о-пліч для досягнення соціально-економічного процвітання нації.

Система захисту КІ повинна мати ієрархічну структуру і включати елементи системи управління й координації на різних рівнях. Такими рівням можуть бути:

1) міжнародний рівень, на якому здійснюється співпраця та координація міжнародної політики та заходів у сфері захисту КІ через спеціально створені й уповноважені органи;

2) національний (загальнодержавний) рівень, на якому здійснюється формування, координація та реалізація державної політики у сфері захисту КІ через Верховну Раду України, Президента України, Кабінет Міністрів України, Раду національної безпеки і оборони;

3) галузевий (відомчий) рівень, на якому здійснюється координація та реалізація державної політики через центральні органи виконавчої влади та інші державні органи, які будуть визначені законом як суб'єкти у сфері захисту КІ;

4) місцевий рівень, на якому здійснюється координація спільних дій та реалізація державної політики у сфері захисту КІ через місцеві органи виконавчої влади, органи місцевого самоврядування та інші державні органи місцевого рівня;

5) об'єктовий рівень, на якому суб'єктами здійснюється реалізація державної політики у сфері захисту КІ.

Водночас модель захисту КІ може бути централізованою чи децентралізованою. Та чи інша її побудова впливає на повноваження залучених органів та потребує детального наукового і фахового аналізу, проведення конференцій та круглих столів за участю спеціалістів для подальшого обговорення та прийняття остаточного рішення.

Захист КІ може мати вигляд централізованої системи з головним державним органом, який відповідає за забезпечення безпеки КІ. Інші відомства беруть участь у визначених заходах або консультують цей орган, але не мають визначального впливу на регулювання діяльності у цій сфері. Така система запроваджена, наприклад, у Великобританії та Іспанії, де діють спеціально створені центри CPNI та CNPIC відповідно. При цьому у Великобританії з метою посилення захисту критично важливих об'єктів у Інтернет-сфері і для протидії кіберзагрозам у 2016 році створено NCSC. Водночас центр також функціонує у складі органів, що входять до Об'єднаного розвідувального комітету. У Німеччині, хоч і не створено окремий орган щодо ЗКІ, проте всі відповідні основні підрозділи є централізовані та перебувають у межах одного відомства. Також структура організації державного управління у сфері ЗКІ може бути децентралізована, коли декілька різних відомств або координують діяльність із захисту, або несуть відповідальність за безпеку КІ спільно чи окремо, залежно від наявного виду загроз. У цьому випадку захист КІ перебуває у компетенції декількох органів державного управління, які здійснюють взаємодію через міжвідомчий комітет, секретаріат тощо. Така форма організації запроваджена, наприклад, у Франції (організацію захисту КІ здійснює SGDSN, важливі функції виконують CDSN та центри у складі МВС (CIC та COGIC), міністерства здійснюють практичне впровадження рішень щодо захисту КІ у сфері свого впливу) та Данії (DEMA відповідає за збереження та продовження важливих функцій держави та суспільства у разі аварій та катастроф; питання протидії кіберзагрозам, терактам та шпигунству покладені на спецслужби в складі МО та поліції).

Основний орган щодо ЗКІ в більшості європейських країн міститься у складі відомств, підпорядкованих уряду. Існує практика створення підрозділів із захисту КІ в складі органів державної безпеки, наприклад, у Великобританії при MI5. В Іспанії контроль за захистом критичної інфраструктури здійснює Державний секретар з питань безпеки, який контролює діяльність спецслужб. При цьому у переважній більшості випадків саме спецслужби координують заходи із захисту КІ від загроз безпекового характеру та кіберзагроз, наприклад: у Німеччині – BSI, BfV; Великобританії – GCHQ та MI5; Данії – DDIS та DSIS тощо [5].

Зазвичай у країнах діють центри захисту від надзвичайних ситуацій, що протидіють загрозам від аварій, катастроф, стихійних лих. У деяких із них, наприклад, у Данії таке агентство (DEMA) є одним з основних органів у сфері захисту критичної інфраструктури, тобто при ньому знаходиться основний контактний центр щодо ЗКІ.

В Україні національна система державного управління у сфері захисту критичної інфраструктури може включати у ролі підсистем визначені законодавством – єдину державну систему цивільного захисту; єдину систему запобігання, реагування і припинення терористичних

актів та мінімізації їх наслідків; державну систему фізичного захисту, національну систему кібербезпеки та нову національну систему захисту критичної інфраструктури (має містити повноваження щодо ЗКІ у сфері державної безпеки).

Стосовно загальної координації в Україні діяльності із ЗКІ, то урахування французького досвіду дозволяє запропонувати створення моделі децентралізованої системи ЗКІ з поєднанням президентської вертикалі, РНБО та урядових структур. Робочим координуючим державним органом управління у сфері захисту КІ, наприклад, може стати Державна комісія з питань безпеки критичної інфраструктури, створена при Кабінеті Міністрів України та очолювана Прем'єр-міністром, оскільки більшість сфер, що можна віднести до критичних, регулюються саме через органи виконавчої влади. До складу комісії доцільно включити зацікавлених керівників міністерств та відомств.

Раціональне поєднання різних взаємозв'язків між елементами національної системи захисту КІ передбачає створення й різних центрів аналізу загроз і ризиків КІ, ситуаційно-аналітичних центрів КІ, координаційних рад (груп) на різних рівнях державної системи управління у сфері захисту КІ. Враховуючи положення Закону України «Про Раду національної безпеки і оборони України», за рішенням РНБО України можуть утворюватися тимчасові міжвідомчі комісії, робочі та консультативні органи для опрацювання і комплексного вирішення проблем міжгалузевого характеру, забезпечення науково-аналітичного та прогнозного супроводження діяльності РНБО України. Саме тому можна розглянути варіанти утворення при РНБО України консультативного органу – Центру з аналізу загроз та ризиків для КІ України із залученням до його діяльності (у різних формах співпраці) провідних фахівців державних органів влади, представників наукової спільноти, організацій та підприємств секторів безпеки КІ або створення відповідного структурного підрозділу у складі Апарату Ради.

Аналіз європейської практики свідчить про доцільність посилення зв'язків між спецслужбами чи створення спільних комітетів з метою попередження, виявлення та припинення загроз від розвідувально-підривної діяльності іноземних спеціальних служб, диверсій і деструктивної та терористичної злочинної діяльності щодо об'єктів КІ. Основну роль при організації протидії загрозам внутрішнього характеру в європейських країнах відіграють контррозвідувальні органи, наприклад, BfV, MI5, DSIS та інші. При них спеціально створені відповідні центри. Аналогом могло б стати створення в СБ України Центру протидії загрозам та ризикам критичній інфраструктурі у сфері державної безпеки.

Важлива роль також повинна бути відведена Національному інституту стратегічних досліджень, Статутом якого (затверджений Указом Президента України від 16 грудня 2002 року № 1158) визначено, що Інститут є базовою науково-дослідною установою аналітико-прогнозного супроводження діяльності Президента

України, яка готує та подає на розгляд Президентові України проекти програмних документів, експертиз нормативно-правових актів, аналітичних довідок та пропозицій щодо основних засад внутрішньої та зовнішньої політики, до яких повинні відноситися й засади державної політики у сфері захисту КІ.

Водночас досвід Великої Британії з побудови централізованої системи ЗКІ у сфері державної безпеки вказує на доцільність розгляду питання зі створення Національного центру захисту критичної інфраструктури. Центр міг би бути утворений як окремий орган або як структурна частина в межах діючого органу влади, який буде призначений відповідальним за координацію діяльності із захисту критичної інфраструктури. Це може бути як орган, підпорядкований Прем'єр-міністру чи РНБО, так і орган у складі СБ України (для прикладу, на базі підрозділів контррозвідувального захисту інтересів держави у сфері економічної безпеки тощо). Подібною є практика створення на базі MI5 центру CPNI, який є основним державним органом, що надає консультації з питань безпеки національної інфраструктури підприємствам, установам та організаціям. Діяльність CPNI спрямована на забезпечення збереження основних послуг економіки Великобританії, формування напрямів діяльності якого може також здійснюватися за рахунок залучення до роботи з визначення загроз та організації протидії їм представників зацікавлених міністерств та відомств.

Координацію дій учасників та нормативне впровадження рішень доцільно реалізовувати через нормативно-правові акти (рішення) РНБО, введені в дію Указом Президента, чи через акти КМ України стосовно діяльності об'єктів, які перебувають у сфері управління уряду.

Не менш важливим є питання організаційних механізмів функціонування вказаної системи.

Досить ефективним засобом організації захисту КІ є розробка та виконання відповідних програм (планів) захисту. Враховуючи зазначене, вважається за доцільне розглянути питання запровадження в Україні відповідної практики розробки Концепції захисту КІ і Концепції захисту секторів економіки України та відповідних програм на національному та регіональному рівнях. На об'єктах також мають створюватись відповідні програми захисту. СБ України доцільно розробляти Концепцію та програму контррозвідувального захисту КІ, що має містити й консолідовану позицію розвідорганів. Програми повинні бути зв'язані з механізмами державної підтримки та стимулювання розвитку економіки, а тому розроблятися у рамках відповідних державних цільових програм. Це сприятиме їх фінансовому забезпеченню.

Безпосередня діяльність учасників, що здійснюють захист об'єктів КІ, має базуватися на складній системі аналізу та визначення (оцінки) показників «загроз», «ризиків», «уразливості», «стійкості», «наслідків» тощо, які розглянуті в попередніх дослідженнях автора.

В Україні визначення ризиків настання негативних наслідків від ураження об'єктів національної інфраструктури та критичної інфраструктури загрозами доцільно здійснювати на підставі оцінювання загроз і вивчення цих об'єктів та їх характеристик.

Ризик від ураження об'єкта КІ – це ймовірність настання максимально негативного наслідку від впливу загроз на цей об'єкт. Він залежить від таких факторів, як стан захисту об'єкта від певної загрози з урахуванням її потенціалу та тривалості дії, прогнозованого терміну відновлення функціонування об'єкта КІ, а також важливості об'єкта для певного типу суб'єктів (держави, суспільства, бізнесу). Формування переліку об'єктів КІ має здійснюватися на основі оцінювання ризику.

Основною метою оцінювання негативних наслідків від ураження об'єкта КІ є визначення категорії «об'єкт КІ», що, у свою чергу, дозволяє попередити наявні чи потенційні загрози та забезпечити необхідний рівень захисту об'єкта. Їх обчислення пропонується здійснювати з урахуванням можливих масштабів втрат і таких показників, як розмір людських втрат, економічних втрат, втрат безпеки життєдіяльності, суспільно-політичних та культурних, втрат для забезпечення державної безпеки та громадського порядку.

Таким чином, негативні наслідки у контексті ЗКІ фактично є втратами.

Завдання щодо визначення ризику від ураження загрозами об'єкта, що може бути віднесений до критичної інфраструктури, та подальшої його категоризації для визначення необхідного рівня захисту також доцільно покласти на власників (розпорядників) об'єктів критичної інфраструктури на підставі письмового звернення уповноважених органів у сфері ЗКІ.

У свою чергу, на об'єктах КІ поряд з працівником, який відповідає за забезпечення безпеки, вважається раціональним вводити посаду відповідального на об'єкті КІ за визначення ризиків. Саме вони у взаємодії із зацікавленими державними та від приватного сектору уповноваженими представниками спільно визначають ризики, обґрунтовують необхідність належного захисту їх об'єкта.

Висновки. Проаналізований міжнародний досвід дозволяє запропонувати до розгляду в нашій державі моделі централізованої та децентралізованої системи захисту критичної інфраструктури.

На переконання автора, більш ефективну з цих моделей визначити важко. З метою створення дійсно дієвої системи в реаліях функціонування вітчизняного державного механізму, автор допускає можливість їх гармонійного поєднання. Досить раціональним вважається створення центрального органу у сфері захисту об'єктів критичної інфраструктури в структурі КМ України. Відповідно до визначених законом повноважень, Кабінет Міністрів України здійснює виконавчу владу безпосередньо та через міністерства, інші центральні органи виконавчої влади, місцеві державні адміністрації [6]. Таким чином, за умов загального підпорядкування системи Прем'єр-міністру всі рівні

управління системи (загальнодержавний чи національний, галузевий, регіональний, місцевий та об'єктовий) можуть охоплюватись та створювати єдиний дієвий вертикально інтегрований механізм. Досить позитивним є те, що побудова системи таким чином забезпечує найбільш пряму та коротку дію управлінських заходів та зворотного зв'язку основної частини об'єктів критичної інфраструктури з відповідним центральним органом у сфері захисту об'єктів критичної інфраструктури. Це підвищує керованість системи. Водночас така структура дозволить більш якісно застосовувати комплекс заохочень та підтримки об'єктів, які будуть внесені в перелік об'єктів критичної інфраструктури. Основою для зазначеної позиції є те, що саме серед повноважень Кабінету Міністрів України є забезпечення рівних умов для розвитку всіх форм власності, здійснення управління об'єктами державної власності, розроблення і виконання загальнодержавних програм економічного, науково-технічного, соціального, культурного розвитку, охорони довкілля, фінансова, інвестиційна, податкова, структурно-галузева політика, соцзахист, охорона здоров'я, здійснення заходів щодо забезпечення обороноздатності та національної безпеки України, громадського порядку, боротьби із злочинністю, ліквідації наслідків надзвичайних ситуацій [6].

У такому разі при СБ України має працювати окремий функціональний підрозділ, що здійснюватиме протидію загрозам та ризикам критичній інфраструктурі у сфері державної безпеки та тісно взаємодіяти із центральним органом у сфері захисту об'єктів критичної інфраструктури. Її фахівці, за прикладом діяльності спецслужб різних європейських держав, мають бути інтегровані в орган у сфері захисту об'єктів критичної інфраструктури та на об'єкти критичної інфраструктури, де виконуватимуть відповідні завдання.

Координацію та загальне управління цією системою під головуванням Прем'єр-міністра має здійснювати Голова Служби безпеки України та визначені керівники міністерств та відомств чи уповноважені ними службові особи.

Важлива роль має бути приділена РНБО для опрацювання і комплексного вирішення проблем міжгалузевого характеру та вирішення глобальних питань, що створюють загрози національній безпеці держави.

Запровадження системи захисту критичної інфраструктури передбачає цілу низку необхідних заходів, обов'язкових для кожного об'єкта КІ за таким алгоритмом:

– визначення виду притаманних загроз (стихійні явища, технічні поломки і недбалість персоналу, теракти, злочини тощо) та їх можливої інтенсивності;

– оцінка уразливих місць;

– аналіз стійкості;

– визначення ризиків;

– визначення категорії об'єкта, його рівня захисту (від наявних та потенційних загроз);

– прогнозування розвитку ситуації залежно від наслідків та загроз;

– формування мети захисту та визначення заходів, необхідних для її досягнення;

– реалізація заходів та спільних заходів держави і приватних партнерів;

– на основі аналізу та з урахуванням розвитку ситуації – постійне внесення коректив у спільні дії та регулятивні нормативно-правові акти.

Зазначені заходи мають бути чітко визначені та передбачені як обов'язковий алгоритм дій для операторів КІ та інших учасників. Доцільно розглянути можливість закріплення подібного алгоритму, наприклад, у Вимогах щодо захисту об'єктів КІ [7]. Ці Вимоги, у свою чергу, мають бути передбачені Програмою захисту та розроблятися органом у сфері захисту КІ, СБ України, зацікавленими відомствами та представниками приватного сектору.

Водночас організація захисту КІ можлива лише завдяки комплексному підходу, поєднаному зі створенням належної нормативно-правової бази. Важливим етапом у цьому процесі є передбачене керівництвом держави та закріплене в Концепції створення державної системи захисту критичної інфраструктури та відповідному розпорядженні КМ України необхідність розробки Закону України «Про критичну інфраструктуру та її захист», що на сьогодні триває, а також внесення змін до низки чинних нормативних актів.

Завдяки вжиттю зазначених заходів вітчизняна система захисту КІ охоплюватиме національний, галузевий, місцевий, об'єктовий і міжнародний рівні та закладе основи нової безпекової політики й зміцнення держави, оскільки сприятиме залученню до захисту в рамках багаторівневого єдиного механізму не лише керівництва держави та відомств, а й органів влади на місцях та безпосередньо об'єктів захисту і партнерів з приватного сектору.

Список використаних джерел

1. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія / О. П. Єрменчук. – Дніпро : ДДУВС, 2018. – 180 с.

2. Зелена книга з питань захисту критичної інфраструктури / Д. Бірюков [та ін.] ; Нац. ін-т стратегічних досліджень. – Київ, 2015. – 35 с.

3. Work programme 2011, Cooperation, Theme 10, Security (European Commission C (2010) 4900 of 19 July 2010) [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/research/participants.

4. Щодо розвитку державно-приватного партнерства як механізму активізації інвестиційної діяльності в Україні : аналітична записка [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/816.

5. BSI-Kritisverordnung (BSI-KritisV). 22.04.2016. [Електронний ресурс]. – Режим доступу : http://www.buzer.de.

6. Про Кабінет Міністрів України : Закон України від 27 лютого 2014 року № 794-VII // Відомості Верховної Ради України. – 2014. – № 13. – Ст. 222.

7. Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency. 2009.

Аннотация. Проанализирован международный опыт и выделены централизованная и децентрализованная модели защиты объектов критической инфраструктуры. В соответствии с основными принципами построения предлагается авторское виденье возможных вариантов их реализации в Украине. Считается, что защита объектов критической инфраструктуры должна базироваться на сложной системе анализа и определения (оценки) показателей «угроз», «рисков», «уязвимости», «стойкости», «последствий» и т. п.

Ключевые слова: критическая инфраструктура, защита критической инфраструктуры, государственная безопасность, международный опыт, организационная модель, централизованная и децентрализованная системы.

Abstract. The international experience is analyzed; centralized and decentralized models of critical infrastructure objects protection are distinguished. In accordance with the basic principles of construction, the author's vision of their possible implementation options in Ukraine is proposed. It is believed that protection of critical infrastructure objects should be based on a complex system of analysis and determination (assessment) of indicators of «threats», «risks», «vulnerabilities», «sustainability», «consequences», etc.

Key words: critical infrastructure, critical infrastructure protection, state security, international experience, organizational model, centralized and decentralized system.

УДК 355.404.52:[620.9:351.863

МАНЖУЛ Ірина Вікторівна

ПРОБЛЕМИ ВИКОРИСТАННЯ БІОПАЛИВА В ЕНЕРГЕТИЧНОМУ СЕКТОРІ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми. Останніми роками активно постає питання про заміну викопних джерел палива (нафти, вугілля та газу) на біологічне. Комерційне виробництво біопалива вже започаткували понад 20-ти держав. Біопаливо відіграє істотну роль в енергозабезпеченні промислово розвинених країн: у США його частка становить близько 4 %, у Данії – 6 %, у Канаді – 7 %, в Австрії – 14 %, у Швеції – 16 % загального споживання первинних енергоресурсів. Австрія, Швеція, Норвегія та Німеччина планують до кінця поточного століття забезпечити всі потреби в енергетиці за рахунок відновлювальних джерел [1, с. 126]. У США та в країнах ЄС спостерігається нарощення виробництва біодизельного палива з соєвої та ріпакової олії, а біоетанолу – головним чином з кукурудзи. З цією