УДК 254.4:338.49(73)

Теленик С. С. – кандидат юридичних наук, здобувач Національної академії внутрішніх справ, м. Київ

Досвід правового регулювання системи захисту критичної інфраструктури в США

Проаналізовано досвід правотворчості (нормативно-правові й політичні документи) та правозастосовної практики у сфері захисту критичної інфраструктури в США. Констатовано, що ці документи було розроблено відповідно до поточного стану й актуальних проблем захисту критичної інфраструктури, що дало змогу проаналізувати й оцінити ефективність різних заходів, своєчасно реагувати на актуальні запити та потреби секторів і системи загалом, визначати сферу й напрями правового регулювання. Розглянуто поняття «критична інфраструктура», систему захисту критичної інфраструктури, повноваження державних органів, засади співпраці з приватним сектором, об'єкти критичної інфраструктури. Сформульовано критичні позиції щодо нормативно-правового регулювання та діяльності державних органів. Окреслено шляхи розв'язання низки проблем, запропоновані іноземними науковцями. Обґрунтовано доцільність вивчення зарубіжного досвіду захисту критичної інфраструктури та використання кращих практик у сфері адміністративно-правового регулювання державної системи захисту критичної інфраструктури в Україні.

Ключові слова: адміністративно-правове регулювання; критична інфраструктура; захист; зарубіжний досвід; нормативні акти; директива.

Постановка проблеми. Аналіз проблематики правового регулювання захисту критичної інфраструктури (КІ) в зарубіжних країнах засвідчує, що цей напрям був визнаний актуальним і пріоритетним майже всіма провідними країнами світу, насамперед, як результат усвідомлення терористичних загроз. Згодом загальна концепція захисту КІ охопила інші види загроз і ризиків (людський чинник, техногенні аварії, природні явища, злочинність), які враховують під час визначення об'єктів КІ та механізмів їх захисту.

У правовому обігу термін «критична інфраструктура» було запроваджено як загальний, що стосується найбільш важливих об'єктів, знищення або пошкодження яких може призвести до шкідливих наслідків для економіки, охорони здоров'я, безпеки, воєнного потенціалу держави.

В Україні вже були ініціативи [1; 2] щодо напрацювання та реалізації концепції захисту КІ. Активну та системну правову роботу із залученням різних суб'єктів розпочато на виконання розпорядження Кабінету Міністрів України «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» від 6 грудня 2017 року № 1009-р [3]. Одним із завдань у цьому документі визначено розроблення Закону України «Про критичну інфраструктуру та її захист».

З огляду на те, що досвід правотворчості та практичної реалізації нормативних положень у цій галузі доступний для вивчення й аналізу, а також охоплює тривалий період, що надає можливість визначити як ефективні, так і хибні підходи до розв'язання проблем захисту КІ, убачаємо за доцільне дослідити деякі нормативні акти та правозастосовну практику зарубіжних країн. Вивчення зарубіжного досвіду також сприятиме зближенню та уніфікації законодавства, що має суттєве значення, оскільки пов'язаність об'єктів КІ та взаємозалежність у цій системі вимагають швидких й узгоджених рішень і дій різних суб'єктів, зокрема на міжнародному рівні. У цій статті розглянуто основні нормативні та політичні документи, що стосуються системи захисту КІ в США – країни, яка має найбільший досвід нормативно-правового регулювання та правозастосовної практики.

Виклад основного матеріалу. Перші політичні та законодавчі напрацювання належать США. Так, 1998 року було прийнято директиву Президента «Про захист критичної інфраструктури». Цей документ вивчали країни ЄС під час побудови власної системи захисту КІ.

Поняття КІ було визначено як фізичні та кіберсистеми, необхідні для мінімального забезпечення операцій економіки й уряду. Вони містять, однак не обмежуються такими складовими: телекомунікації, енергетика, банківська справа і фінанси, транспорт, водні системи та служби екстреної допомоги (як державні, так і приватні).

Констатовано, що завдяки досягненням у галузі інформаційних технологій і необхідності підвищення ефективності ці інфраструктури стають більш автоматизованими та взаємопов'язаними. Водночас ці успіхи спричинили нові небезпеки (вразливості) в разі збою обладнання, людської помилки, несприятливих погодних та інших природних факторів, а також фізичних і кібератак.

Систему захисту КІ визначають за рівнями відповідно до сфери діяльності (критичних функцій) для різних суб'єктів: 1) федеральний уряд здійснює основні місії національної безпеки та забезпечує загальну суспільну охорону здоров'я й безпеку; 2) державні та місцеві органи влади підтримують порядок і надають мінімальні необхідні державні послуги; 3) приватний сектор забезпечує впорядковане функціонування економіки й надання основних телекомунікаційних, енергетичних, фінансових і транспортних послуг.

Увагу акцентовано на питаннях державно-приватного партнерства, що сприймають як справжнє (реальне), взаємне і спільне. Задля досягнення такого формату констатовано

необхідність уникати дій, які посилюють державне регулювання або розширюють нефінансовані урядові мандати приватному сектору. Для кожного з основних секторів економіки, які вразливі для атаки на інфраструктуру, федеральний уряд призначає з провідної агенції старшого співробітника цієї агенції як офіційного представника зі зв'язків із сектором для роботи з приватним сектором. Ці особи, а також відділи й корпорації, представниками яких вони є, будуть сприяти розробленню Національного плану забезпечення КІ, а саме щодо: оцінювання вразливості сектору до кібератак або фізичних атак; рекомендацій для усунення значних уразливостей; пропозицій системи для виявлення та запобігання спробам істотних атак; розроблення плану попередження, стримування і відстрочення нападу, а потім, у разі необхідності, швидкого відновлення мінімальних основних можливостей після атаки.

У цьому документі сформульовано загальні принципи та проблеми, які слід ураховувати зацікавленим учасникам для усунення потенційних уразливостей, а саме:

– консультації Президента з Конгресом щодо підходів і програм, зазначених у цій директиві;

– захист КІ є спільною відповідальністю і партнерством між власниками, операторами й урядом. Федеральний уряд також заохочує міжнародне співробітництво задля подолання цієї глобальної проблеми;

– необхідно регулярно оцінювати надійність, уразливість і загрозу для КІ, оскільки технологія і характер загроз КІ швидко змінюються, тому захисні заходи й відповіді мають бути стійко адаптовані;

– державне регулювання будуть здійснювати тільки в умовах матеріальної відмови ринку для захисту здоров'я, безпеки чи благополуччя американського народу. У таких випадках установи мають виявляти й оцінювати наявні альтернативи прямому регулюванню, зокрема забезпечувати економічні стимули для заохочення бажаної поведінки, надаючи інформацію про те, який вибір може здійснити приватний сектор. Ці стимули поряд з іншими діями мають бути спрямовані на те, щоб допомогти використовувати новітні технології, напрацювати глобальні шляхи розв'язання міжнародних проблем і дозволити власникам й операторам приватного сектору досягнути та підтримувати максимально можливу безпеку;

– повноваження держави, можливості та ресурси уряду, зокрема у сферах правоохоронної діяльності, регулювання, зовнішньої розвідки й готовності до оборони, мають бути доступні в разі необхідності для забезпечення захисту КІ та його підтримання;

– необхідно забезпечувати високий рівень захисту конфіденційності. Споживачі й оператори мають бути впевнені, що інформацію буде опрацьовано точно, конфіденційно та надійно;

– федеральний уряд за допомогою своїх досліджень, розробок і закупівель заохочує впровадження оптимальних методів захисту КІ;

– федеральний уряд має бути взірцем для приватного сектору щодо того, як найкраще забезпечувати захист КІ, і поширювати результати своїх зусиль;

– слід акцентувати увагу на профілактичних заходах, а також на управлінні загрозами та кризами. Із цією метою потрібно заохочувати власників й операторів приватного сектору забезпечувати максимально можливу безпеку для контрольованих ними інфраструктур і надавати уряду необхідну інформацію для отримання допомоги щодо виконання цього завдання. Щоб цілком задіяти приватний сектор, бажано, щоб участь власників й операторів у національній системі захисту КІ була добровільною;

– тісне співробітництво й координація з державними і місцевими органами влади мають важливе значення для надійної та гнучкої програми захисту КІ. Усі плани та дії щодо захисту КІ мають врахувати потреби, види діяльності й обов'язки державних і місцевих органів влади та осіб, які відповідають за об'єкти КІ.

У цитованому документі визначено структуру й організацію захисту КІ, зокрема:

1. Провідні агентства зі зв'язків із сектором: для кожного сектору інфраструктури, який може бути об'єктом значного кіберфізичного або фізичного нападу, створюють один урядовий департамент США, який буде виконувати функції провідного агентства зі зв'язків. Секретар співпрацює з представниками приватного сектору для розв'язання проблем, пов'язаних із КІ, зокрема щодо рекомендації складових Національного плану захисту КІ. Спільно агентство та партнери з приватного сектору розробляють і впроваджують Програму щодо підвищення інформованості та просвіти щодо уразливості для свого сектору.

2. Провідні агентства для спеціальних функцій. Певні функції, пов'язані із захистом КІ, має здійснювати федеральний уряд (національна оборона, закордонні справи, розвідка, правоохоронні органи). Для реалізації кожної із цих спеціальних функцій має функціонувати провідна установа, яка буде відповідати за координацію діяльності уряду США в цій галузі. Кожна провідна установа призначить старшого офіцера,

молодшого секретаря, щоб виконувати функції координатора для федерального уряду.

3. Міжвідомча координація. Співробітники зі зв'язків із секторами та функціональні координатори провідних агентств, а також представники інших відповідних департаментів й установ, що стосується й Національної економічної ради, збираються для координації здійснення цієї директиви під егідою груп з координації КІ під головуванням національного координатора з безпеки, захисту інфраструктури та протидії тероризму. Національного координатора призначає Президент, він доповідає через помічника Президента з питань національної безпеки, який забезпечує координацію з помічником Президента з економічних питань.

4. Національна рада з гарантування інфраструктури. За рекомендацією провідних агентств, Національної економічної ради та національного координатора призначають групу основних представників інфраструктури, а також посадових осіб з державних і місцевих органів влади – Національну раду із забезпечення КІ. Президент призначає голову. Національна рада з гарантії інфраструктури проводить періодичні наради для розширення партнерства державного і приватного секторів у галузі захисту КІ, доповідає Президенту за необхідності.

Кожні відомство й агентство федерального уряду несуть відповідальність за захист своєї КІ, передусім її кіберсистем. Відповідальність за забезпечення інформації несе кожен керівник відділу інформації та управління відділом і відомством. Кожне відомство призначає головного інспектора з інфраструктури, який несе відповідальність за захист решти аспектів КІ цього департаменту. Такі посадові особи встановлюють процедури для отримання цільових і достовірних даних з метою оцінювання уразливості на урядових комп'ютерах та фізичних системах. Міністерство юстиції встановлює юридичні принципи для надання таких повноважень.

Завдання сформульовано такі:

1. Аналіз уразливостей. Для кожного сектору економіки та кожного сектору уряду, що можуть бути об'єктами атаки інфраструктури з метою завдання істотної шкоди США, слід здійснити початкове оцінювання уразливості, а потім забезпечувати періодичні оновлення.

2. Планування. На підставі оцінки уразливості розробляють рекомендований план їх усунення. У плані мають бути зазначені строки реалізації заходів, відповідальність і фінансування.

3. Попередження. Національний центр попереджає про значні атаки на інфраструктуру, розробляючи систему для

виявлення й аналізу таких атак з максимально можливою участю приватного сектору.

4. Відповідь. Необхідно розробити систему реагування на істотну атаку інфраструктури під час її здійснення з метою ізоляції та мінімізації наслідків.

5. Відновлення. Для різних рівнів атак інфраструктури створюють систему швидкого відновлення мінімально необхідних можливостей.

6. Інформованість. У межах державного та приватного секторів слід запровадити Програму підвищення інформованості і просвіти з питань уразливості, щоб привернути увагу населення до важливості безпеки, навчати їх стандартів безпеки, передусім щодо кіберсистем.

7. Дослідження і розробки. Федеральні дослідження й розробки для забезпечення захисту інфраструктури мають бути координованими, плановими, ураховувати дослідження в приватному секторі та належно фінансовані.

8. Інтелект. Передбачено розроблення та реалізацію плану щодо збирання й аналізу зовнішньої загрози для національної інфраструктури, що охоплює, однак не обмежується загрозою іноземної кіберінформаційної війни.

9. Міжнародне співробітництво. Стосується розроблення плану розширення співробітництва в галузі захисту КІ з однодумцями та дружніми країнами, міжнародними організаціями, багатонаціональними корпораціями.

10. Законодавчі та бюджетні вимоги. Охоплюють оцінювання органами законодавчої та виконавчої влади бюджетних пріоритетів щодо КІ.

У директиві визначено суб'єктів, які входять до системи захисту КІ, окреслено їхні повноваження, субординацію, співпрацю й інші аспекти діяльності.

Національний координатор з безпеки, захисту інфраструктури та протидії тероризму відповідає за координацію реалізації директиви. Цей суб'єкт не здійснює керівництво департаментами й агентствами, проте забезпечує міжвідомчу координацію для розроблення та здійснення політики і має розглядати кризові заходи щодо подій у галузі інфраструктури за участю іноземних партнерів (учасників). Національний координатор формулює рекомендації в межах річного бюджету щодо бюджетів установ для захисту КІ. Національний координатор здійснює роботу за такими напрямами:

– питання відповідальності, що постають унаслідок участі компаній приватного сектору в процесі обміну інформацією;

– наявні юридичні перепони на шляху обміну інформацією;

– класифікація документів та інформації для визначення обсягу їх поширення та використання зі збереженням конфіденційності, недопущення ризику розкриття інформації суб'єктам, які можуть нею зловживати;

– захист, що охоплює безпечні системи поширення й опрацювання інформації про таємниці промислової торгівлі, інші конфіденційні бізнес-дані, інформацію правоохоронних органів і доказовий матеріал, інформацію про національну безпеку, некласифіковані матеріали, що відображають уразливості приватних структур;

– наслідки обміну інформацією з іноземними організаціями, якщо таке спільне використання вважають необхідним для безпеки інфраструктур США;

– потенційна користь від стандартів безпеки, що передбачає субсидіювання або іншу допомогу, страхування для окремих постачальників критично важливої інфраструктури, які планують вести бізнес із США.

Національний центр захисту інфраструктури є головним органом, що здійснює оцінювання загрози, уразливості, запобігання, правоохоронну діяльність у галузі інфраструктури. Місія Національного центру полягає у своєчасному запобіганні міжнародним загрозам, усебічному аналізі, розслідуванні та реагуванні правоохоронних органів.

Усі виконавчі органи та відомства співпрацюють з Національним центром і надають допомогу, інформацію, консультації, які він запитує. До нього належать структурні елементи, що відповідають за попередження, аналіз, комп'ютерне забезпечення, координацію реагування на надзвичайні ситуації, навчання, інформаційно-пропагандистську роботу, розроблення й застосування технічних засобів. Крім того, Національний центр встановлює відносини та зв'язки з приватним сектором і з будь-якими організаціями обміну інформацією й аналізу, які може створювати приватний сектор.

Центр обміну інформацією та аналізу. Національний координатор, який співпрацює з координаторами сектору, посадовими особами зі зв'язків із сектором і Національною економічною радою, консультується з власниками й операторами критично важливих інфраструктур задля заохочення та запровадження спільної системи використання й аналізу інформації в приватному секторі. Формат роботи та функції центру, його зв'язок із Національним центром визначає приватний сектор, консультуючись із федеральним урядом і за його підтримки. Такий центр слугує механізмом для збирання, аналізу та поширення інформації. Тобто обмін інформацією про уразливості, загрози,

вторгнення та аномалії має вирішальне значення для успішного партнерства між урядом і промисловістю [4].

Отже, Директива охоплює більшість важливих питань щодо створення системи захисту КІ та заходів, що необхідні для цього.

Інші документи, що стосуються захисту КІ, розроблено на виконання проаналізованої директиви та відповідно до визначених у ній завдань: Національний план захисту інформаційних систем (National Plan for Information Systems, 2000); Указ Президента США № 13231 (Executive Order 13 23, 2001); Стратегія національної безпеки (National Strategy for Homeland Security, 2002); Національна стратегія захисту критично важливих об'єктів (The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003); Указ Президента США № 13228 (Executive Order 13 228, 2003); результатів з позицій безпеки, і перехід до системи угод про співпрацю, які надають можливість федеральному уряду та його державним і місцевим партнерам ефективно аналізувати результати.

Критика наявного підходу стосується таких його аспектів:

– складність інфраструктури. Не сформовано диференційованого підходу до визначення ступеня ризику й розподілу ресурсів. Тобто не вся інфраструктура піддається ризику тероризму і стихійних лих, тому оцінювання національного ризику не має сенсу, оскільки різні рівні ризику в сучасній інфраструктурі унеможливлюють створення стандартизованого розрахунку ризику;

– надмірна кваліфікація. Проблема визначення критичності полягає в тому, що нею часто зловживають. Політикам невигідно визнавати, що не всім нападам або нещасним випадкам можна запобігти, що визначають як критичність, тому це вимагає дедалі більше ресурсів у всій інфраструктурі, замість того, щоб спрямовувати ресурси туди, де це справді важливо;

– термін «стійкість до відмов» не має вказувати на всі витрати (охорона, зброя, будівлі), пов'язані із захистом КІ. Правильне визначення передбачає заходи для підвищення ймовірності того, що КІ може продовжувати функціонувати або швидко відновлюватися після надзвичайної події (здатність КІ швидко відновитися після терористичних атак, стихійних лих, що підвищує можливість критично важливих активів долати збої та посилює ефективність американської економіки – це головна мета захисту КІ);

– недосконалі канали обміну інформацією; проблема поширення інформації між державним і приватним секторами. Представники приватного сектору висловили занепокоєння щодо

правових і нормативних наслідків надання урядовим органам важливих даних, зокрема пропрієтарних, у галузі КІ. Крім того, менеджери компаній можуть неохоче ділитися комерційною таємницею та іншою інформацією з галузевими партнерами, які також є їх конкурентами. Для розв'язання проблеми слід уживати заходів щодо обмеження доступу до будь-яких даних, добровільно наданих компаніями, а також упроваджувати керівні принципи, що обмежують використання державними органами цієї інформації;

– визначення партнерських відносин. Такі відносини між державним і приватним секторами мають важливе значення, оскільки приватний сектор володіє та управляє близько 85 % усієї КІ США. Приватні суб'єкти мають ширші можливості для визначення та реалізації стратегій зниження ризиків і роботи з різними збоями. Державні установи можуть надавати важливі Директива Президента щодо національної безпеки № 7 (Homeland Security Presidential Directive 7, 2003, що замінює директиву 63); План захисту національної інфраструктури (National Infrastructure Protection Plan, 2006); Плани захисту національної інфраструктури (National Infrastructure Protection Plans, 2007); Національний план захисту інфраструктури (National Infrastructure Protection Plan, 2013).

Така правова політика зумовлена метою забезпечення контролю та моніторингу ситуації щодо змін і ризиків у системі КІ з відповідним коригуванням секторальних планів, програмних елементів, концепцій тощо. Тобто кожен наступний документ розробляли відповідно до поточного стану й актуальних проблем захисту КІ, що дало змогу проаналізувати й оцінити ефективність різних заходів, своєчасно реагувати на актуальні запити та потреби секторів і системи загалом, визначати сферу й напрями правового регулювання.

У США до об'єктів КІ, що підлягають захисту, належать: сільське господарство і продовольство (ферми, підприємства з виробництва продовольчих продуктів); водні ресурси (федеральні резервуари, муніципальні водостоки, дамби); суспільна охорона здоров'я (зареєстровані госпіталі); обслуговування в надзвичайних ситуаціях (населені пункти); захист індустріальної бази (фірми й підприємства); енергетика (електростанції); авіація (суспільні аеропорти); пасажирські залізниці (основні залізниці); автодороги й автомобільний транспорт (дорожні мости); нафтогазовий комплекс (нафтопроводи, місця видобутку); морський транспорт (порти на узбережжі й островах); масові перевезення громадян (транспортні компанії); банківська справа і фінанси (фінансові інститути); хімічні та інші небезпечні матеріали

(хімічні виробництва); поштова служба і мореплавство (пункти доставки); національні пам'ятки та зображення (історичні будівлі); атомні електростанції (комерційні атомні електростанції); засоби обслуговування уряду (засоби, що належать/використовуються урядом); комерційні споруди (висотні споруди) [5]. За відповідними секторами визначено галузеві (відповідальні) агентства (органи): департамент сільського господарства, продовольства і медикаментів; департамент казначейства; департамент внутрішньої безпеки; міністерство оборони; департамент енергетики; відділ внутрішніх справ; адміністрація транспортної безпеки; департамент охорони здоров'я і соціальних служб; управління безпеки на транспорті, берегова охорона; агентство з охорони навколишнього середовища.

Водночас, попри значні напрацювання щодо створення системи захисту КІ в США, постає низка проблем, на яких акцентують увагу науковці та практики. Зокрема, автори дослідження «Як виправити плани захисту критичної інфраструктури національної безпеки: настанови для Конгресу» зазначають, що проблема реалізації плану захисту КІ полягає в правильному визначенні того, які інфраструктури справді важливі, які з них важливі, однак не завжди необхідні. Діє 86 комітетів і підкомітетів, які здійснюють нагляд у сфері захисту КІ, створюючи складну й обтяжену систему, яка перешкоджає успішному здійсненню державної політики. Рекомендації для Конгресу сформовані в партнерстві з адміністрацією, приватним сектором і різними державними й місцевими суб'єктами. Вони передбачають:

– Конгрес має будувати роботу так, щоб законодавчі ініціативи ґрунтувалися на відомостях про ризики;

– фокус на стійкість до відмов з особливим визначенням захисту КІ, руйнування якого спричинить катастрофічні наслідки;

– продовження взаємодії з приватним сектором (зокрема вітчизняним та іноземним бізнесом) шляхом удосконалення каналів обміну інформацією та продовження інформаційно-пропагандистської діяльності, орієнтованої на малий і середній бізнес;

– підвищення рівня освіти, інформованості та професійної підготовки спеціалістів з питань безпеки, які задіяні в системі захисту КІ, а також ініціювання і підтримка досліджень і розробок у галузі КІ;

– перегляд наявного підходу, орієнтованого на гранти в напрямі розширення можливостей на державному й місцевому рівнях, оскільки перший часто не забезпечує необхідних ресурсів

для захисту КІ, а також наділені широкими можливостями для протидії загрозам. Наприклад, вони володіють унікальними даними щодо іноземних терористичних загроз [6].

Висновки. Отже, система захисту КІ в США формувалася шляхом поступових і послідовних політичних, правових, управлінських рішень та дій щодо визначення загального (національного) плану безпеки КІ (визначення об'єктів КІ, аналіз уразливості, програми щодо запобігання, нейтралізації, ліквідації негативних наслідків); створення засад державно-приватного партнерства та взаємодії з визначенням відповідальності; створення виконавчих органів, відповідальних за забезпечення безпеки елементів (об'єктів) КІ в різних галузях; координації діяльності різних суб'єктів (державний і приватний сектори), що стосуються захисту КІ на національному рівні; формування системи інформування та сповіщення. Важливим висновком стало надання переваги превенції над реагуванням. Утім практична реалізація зазначених та інших заходів супроводжувалася проблемами, які заздалегідь визначити було складно або неможливо. Детальне вивчення та напрацювання шляхів їх розв'язання – окремий напрям роботи щодо вдосконалення системи захисту КІ. Поширеним є тлумачення системи захисту КІ як процесу, який вимагає постійного вдосконалення та коригування відповідно до поточних даних, актуальних потреб, вимог, пріоритетів. Україні доцільно орієнтуватися на такий підхід, який надасть можливість своєчасно й ефективно виконувати завдання у сфері захисту КІ, зокрема щодо адміністративно-правового регулювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. – Київ : НІСД, 2012. – 96 с.

2. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / [упоряд.: Д. С. Бірюков, С. І. Кондратов] ; за заг. ред. О. М. Суходолі. – Київ : НІСД, 2015. – 176 с.

3. Про схвалення Концепції створення державної системи захисту критичної інфраструктури [Електронний ресурс] : розпорядження Кабінету Міністрів України від 6 груд. 2017 р. № 1009-р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80. – Назва з екрана.

4. Presedential Decision Directive PDD 63. May 22, 1998 [Electronic resource]. – Mode of access: https://fas.org/irp/offdocs/pdd/pdd-63.htm. – Title from the screen.

5. Critical Infrastructure Sectors. Homeland Security [Electronic resource]. – Mode of access: https://www.dhs.gov/critical-infrastructure-sectors. – Title from the screen.

6. Baker McNeill J. How to Fix Homeland Security Critical-Infrastructure Protection Plans: a Guide for Congress [Electronic resource] / J. Baker McNeill, R. Weitz. – Mode of access: https://www.heritage.org/homeland-security/report/how-fix-homeland-security-critical-infrastructure-protection-plans-guide– Title from the screen.

REFERENCES

1. Biriukov, D.S., & Kondratov, S.I. (2012). *Zakhyst krytychnoi infrastruktury: problemy i perspektyvy vprovadzhennia v Ukraini [Protection of critical infrastructure: problems and prospects of implementation in Ukraine].* Kyiv: NISD [in Ukrainian].

2. Biriukov, D.S., & Kondratov, S.I. (2015). Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini [Green Book on Critical Infrastructure Protection in Ukraine]. *Zb. materialiv mizhnar. ekspert narad, Sb. Materials International Expert. Meetings*. Kyiv: NISD [in Ukrainian].

3. Rozporiadzhennia Kabinetu Ministriv Ukrainy "Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury": vid 6 hrud. 2017 r. No. 1009-p [the Cabinet of Ministers of Ukraine "On Approval of the Concept for the Creation of a State System for the Protection of Critical Infrastructure" from December 6, 2017, No. 1009-p]. (n.d.). *zakon2.rada.gov.ua.* Retrieved from http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80 [in Ukrainian].

4. *Presedential Decision Directive PDD 63.* May 22, 1998. Retrieved from: https://fas.org/irp/offdocs/pdd/pdd-63.htm.

5. Critical Infrastructure Sectors. *Homeland Security.* Retrieved from: https://www.dhs.gov/critical-infrastructure-sectors.

6. Jena Baker McNeill and Richard Weitz. *How to Fix Homeland Security Critical-Infrastructure Protection Plans: a Guide for Congress.* Retrieved from: https://www.heritage.org/homeland-security/report/how-fix-homeland-security-critical-infrastructure-protection-plans-guide.

Стаття надійшла до редколегії 17.04.2018

Telenyk S. – Ph.D in Law, Researcher of the National Academy of Internal Affairs, Kyiv, Ukraine

The Experience of Legal Regulation of the Critical Infrastructure Protection System in the United States

The experience of law-making and law-enforcement practice in protecting critical infrastructure in the USA is analyzed. The concept of «critical infrastructure», the system of protection of critical infrastructure, authorities of state bodies, the principles of cooperation with the private sector, objects of critical infrastructure are considered. Critical positions regarding regulatory and legal regulation and activity of state bodies and ways to solve a number of problems offered by foreign scientists are given. The critical infrastructure protection system in the United States was formed over a period of time through gradual and consistent political, legal, managerial decisions and actions on the definition of a general (national) critical infrastructure safety plan (identification of critical infrastructure objects, vulnerability analysis, prevention, neutralization, and elimination of negative consequences); creation of the fundamentals of public-private partnership and interaction with definition of responsibility; creation of executive bodies responsible for ensuring the safety of elements (objects) of critical infrastructure in various fields; coordination of activities of various actors (public and private sector) related to the protection of the critical infrastructure at the national level; formation of a system of information and

notification. An important conclusion was to give preference to the prevention response. However, the practical implementation of these and other measures was accompanied by problems that it was difficult or impossible to determine in advance. Careful studying and working out of ways of their solution is a separate direction of work on improving the system of protection of clinical trials. The vision of the critical infrastructure protection system has now been confirmed as a process that requires continuous improvement and adjustment, taking into account current data, current needs, requirements, and priorities. It is understood that in Ukraine it is advisable to focus on such an approach, which will allow to timely and efficiently carry out tasks in the sphere of protection of the critical infrastructure, in particular in relation to administrative-legal regulation.

Keywords: administrative-legal regulation; critical infrastructure; protection; foreign experience; regulatory acts; directive.