4. Кучеров И.И. Налоговое право зарубежных стран : курс лекций. Москва : АО «Центр ЮрИнфоР», 2013. С. 314.

5. Попович В.П. Окремі проблеми встановлення кримінальної відповідальності за декларування недостовірної інформації. URL: http://scholar.googleusercontent.com/scholar.

6. Про запобігання корупції : Закон України від 14 жовтня 2014 р. № 1700-VII. URL: http:// rada.gov.ua/pls/zweb2/web.

7. Сисоєв Д.О. Криміналізація зловживання повноваженнями службовою особою юридичної особи приватного права незалежно від організаційно-правової форми в контексті державної антикорупційної політики. *Наше право*. 2014. № 7. С. 118–126.

8. Тацій В.Я., Тютюгін, В.М., Киричко В.І. Проблеми кваліфікації корупційних і пов'язаних з корупцією злочинів : навчально-методичний посібник. Харків : Нац. юрид. ун-т ім. Ярослава Мудрого, 2017. 114 с.

КОНДРАТЮК М. В.,
аспірант кафедри кібербезпеки
та інформаційного забезпечення
(Одеський державний університет внутрішніх справ)

УДК 342.9
DOI https://doi.org/10.32842/2078-3736-2019-6-2-7

КІБЕРБЕЗПЕКА УКРАЇНИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У статті розкриті актуальні питання функціонування системи кібербезпеки в системі національної безпеки України. Розкрито основні дефініції – кіберпростір, національна безпека та кібербезпека, показано їх взаємозв'язок і взаємовплив. Визначено, що, незважаючи на широкі можливості застосування поняття кіберпростору на практиці, є чимало часто діаметрально протилежні думки щодо його практичного використання, а в багатьох системах національних законодавств провідних країн світу не виділяються окремі законодавчі акти для його захисту та регулювання. Вказано, що кіберпростір як базова основа кібербезпеки визначається як унікальна форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на породження, сприйняття, запам'ятовування, переробку та обмін інформацією.

Подано авторські дефініції національної безпеки та кібербезпеки України відомих вітчизняних вчених, проаналізовано основні авторські підходи до їх врегулювання. Досліджено, що Україні питання кібербезпеки регулюється багатьма законодавчими актами, серед яких найбільшу вагу має Закон України № 2163-VIII від 05 жовтня 2017 р. «Про основні засади забезпечення кібербезпеки України». Він визначив як загальні засади організації та регулювання безпеки кіберпростору, так і конкретні заходи, норми регулювання, об'єкти та суб'єкти кібербезпеки України. Прослідковано також механізм та хід формування нормативно-правової бази забезпечення кібербезпеки України, зокрема згадано про рішення РНБО «Про стратегію кібербезпеки України», та подано основні зауваження відомих юристів щодо протидії вітчизняних без пекових систем сучасним зовнішнім та внутрішнім кіберзагрозам.

Виокремлено основні проблемні моменти забезпечення кібербезпеки в системі національної безпеки України, проаналізовані думки вчених із цього приводу. Зрештою, виділено ключові шляхи оптимізації боротьби із кіберзагрозами на сучасному етапі розвитку вітчизняної системи національної безпеки.

Ключові слова: *кіберпростір, кібербезпека, національна безпека, загрози, інформація, система.*

The article deals with topical issues of functioning of the cybersecurity system in the national security system of Ukraine. Basic definitions are disclosed – cyberspace, national security and cybersecurity, and their interconnections and interactions are shown. It is determined that, despite the wide possibilities of application of the concept of cyberspace in practice, there are often diametrical opinions in scientific opinion on its practical use, and in many systems of national laws of the leading countries of the world there are no separate legislative acts for its protection and regulation. It is stated that cyberspace as the basic basis of cybersecurity is defined as a unique form of coexistence of a set of tangible and in tangible objects and processes aimed at the generation, perception, memorization, processing and exchange of information.

The author's definitions of national security and cybersecurity of famous Ukrainian scientists are presented, the main author's approaches to their settlement are analyzed. It has been researched that the issue of cybersecurity is regulated by many legislative acts, among which Law of Ukraine № 2163-VIII of 05.10.2017 "On the basic principles of ensuring cybersecurity of Ukraine" is of the greatest importance. He defined the general principles of the organization and regulation of cyberspace security, as well as specific measures, norms, objects and subjects of cybersecurity of Ukraine. The mechanism and course of formation of the regulatory framework for ensuring cybersecurity of Ukraine were also investigated, in particular, the NSDC decision "On the cybersecurity strategy of Ukraine" was mentioned, and basic remarks of well-known lawyers on counteracting domestic without internal systems with cyber threats were presented.

The main issues of cybersecurity in the national security system of Ukraine are identified, the opinions of scientists on the subject are analyzed. Finally, the key ways to optimize the fight against cyber threats at the current stage of development of the national security system are highlighted.

Key words: *cyberspace, cybersecurity, national security, threats, information, system.*

Вступ. Сьогодні питання забезпечення національної безпеки держави стало надзвичайно актуальним через активізацію зовнішній безпекових загроз, до яких слід віднести посилення військової присутності країни-агресора в регіоні, енергетична залежність України від зовнішніх джерел, посилення тиску в сфері економіки, інформаційної політики, технологій тощо. Поєднуючись із внутрішніми проблемами в державі (розбалансованістю реформаційних процесів, загальним зниженням обороноздатності країни, дефіцитом державного бюджету та ін.), така ситуація вимагає системних комплексних дій по нейтралізації вказаних загроз, в першу чергу в інформаційному середовищі. Саме інформаційний простір та ресурси, інформаційні технології та інфраструктура найбільше впливають на вирішення зазначених проблем. Тому кібербезпека сьогодні є однією із найважливіших складових елементів у системі національної безпеки України.

Проте сьогодні слід вказати, що реальна ситуація справ у сфері кібербезпеки не в повному обсязі забезпечує можливість держави протистояти зовнішнім і внутрішнім загрозам. Тому постає нагальна потреба в докорінній трансформації системи інформаційної безпеки для забезпечення життєздатності її основних системоутворюючих елементів. Це твердження і визначає актуальність і значимість даного дослідження.

Питання забезпечення кібербезпеки України в системі її національної безпеки розглядалося К.Л. Бугайчуком, І.В. Діордіцою, В.А. Ліпканом, Є.Д. Скулишем, В.І. Ткаченком, В.М. Фурашевим, В.П. Шеломенцевим та ін. У своїх дослідженнях вони розглядали тлумачення проблеми кіберпростору та кібербезпеки, роль кібербезпеки у формуванні системи національної безпеки України, окреслювали коло проблем, пов'язаних із формуванням механізму кіберзахисту в державі тощо. Проте ще залишаються малодослідженим питання пошуку ефективних шляхів і механізмів оптимізації кібербезпеки в Україні, чому і присвячена ця стаття.

Постановка завдання. Метою статті є висвітлення системи кібербезпеки України та її місця і ролі у єдиному комплексі національної безпеки держави, для чого було поставлено завдання проаналізувати зміст поняття та дефініцію кібербезпеки, визначити її актуальні проблемні питання та окреслити ймовірні шляхи їх вирішення.

Результати дослідження. На початку XXI ст. у світі формується принципово нове, унікальне середовище, що тісно пов'язане з проникненням новітніх технологій та глобальної мережі Інтернет у наше життя – кіберпростір. Кіберпростір виник на основі комп'ютерних, мережевих, телекомунікаційних та інформаційних систем і являє собою віртуальний простір, який надає змогу здійснювати ефективну комунікацію в сфері суспільних відносин через існування сумісних між собою комунікаційних систем з допомогою електронних ресурсів та мережі Інтернет, а також інших ймовірних мереж передачі інформації. Саме таке визначення поняття кіберпростору міститься в Законі України № 2163-VIII від 05 жовтня 2017 р. «Про основні засади забезпечення кібербезпеки України» [1].

Незважаючи на законодавче закріплення даного поняття у вітчизняному законодавстві, в науковому середовищі існують чимало часто діаметральних думок щодо його практичного використання. Так, Є.В. Скулиш вказує, що саме через сумніви щодо можливості застосування поняття кіберпростору на практиці у багатьох системах національних законодавств провідних країн світу не виділяються окремі законодавчі акти для його захисту та регулювання, а натомість використовуються традиційні законодавчі акти [8, с. 175].

В.М. Фурашев, доповнюючи думки Є.В. Скулиша, зазначає, що під кіберпростір – це «форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на породження, сприйняття, запам'ятовування, переробку та обмін інформацією». Тим самим вчений ототожнює кіберпростір та віртуальний світ, який, ґрунтуючись на реальній, матеріальній основі, має складні та неоднозначні наслідки свого функціонування та розвитку [10, с. 162].

У цих твердженнях, на нашу думку, є значний сенс, оскільки, незважаючи на те, що кіберпростір неможливо відчути, побачити чи осягнути іншими органами чуттів, він одночасно включає в себе і матеріальну складову (засоби комп'ютерної та мережевої техніки, засобі телекомунікацій, зв'язку та ін..). Кіберпростір став на сьогоднішній день однією із найважливіших складових частин інформаційного простору та ареною ведення справжніх війн у віртуальному середовищі. Тому кібербезпека є основним елементом регулювання кіберопростору і водночас системи національної безпеки країни.

Система забезпечення національної безпеки – це комплекс різноманітних заходів (управлінських, нормативних, методологічних, інформаційних, аналітичних, розвідувальних і контр розвідувальних, пошукових, наукових, технічних кадрових та ін.), які направлені на оптимізацію процесу управління зовнішніми та внутрішніми загрозами національній безпеці держави. Саме таке визначення поняття національної безпеки знаходимо у дослідженнях В.А. Ліпкана, який, на нашу думку, найбільш точно та широко охарактеризував дане поняття. Вчений вказує, що саме національна безпека України гарантує розвиток української нації, її державних інституцій, духовно-культурного життя та внутрішнього добробуту громадян [6, с. 57].

В.П. Гетьманчук, В.К. Грищук, Я.Б. Турчин та інші відомі політологи визначають поняття системи національної безпеки як систему суб'єктів (органів влади, посадових осіб, громадських організацій, громадян тощо), яких об'єднує спрямованість захисту національних інтересів України в процесі здійснення ними визначеної законодавством діяльності [7, с. 332].

Питання національної безпеки держави постійно було в центрі уваги всіх державницьких структур та органів від самого початку існування незалежної України. Так, ще в Декларації про державний суверенітет України (прийнята 16 липня 1990 р.) поняття національної безпеки було винесено при розгляді міжнародних відносин, внутрішньої та зовнішньої політики, екології тощо. Безпекові питання постійно обговорюються як надзвичайно важливі та актуальні в роботі Президента, Верховної Ради, Кабінету Міністрів, інших відомств та організацій і пов'язуються передусім з правом України на власну армію та оборону.

Система національної безпеки, як зазначив В.І. Ткаченко, ґрунтується на відповідній нормативній базі, яка формує офіційну державну позицію на цінності нації, її інтереси, прагнення та цілі розвитку, а також способи та методи протидії внутрішнім та зовнішнім загрозам. Однією з таких загроз і є небезпека, пов'язана з кіберпростором [9, с. 4].

Сьогодні в умовах розвитку інформаційного суспільства кібернетична безпека, або кібербезпека, є необхідною і важливою умовою функціонування та розвитку інформаційного суспільства. З огляду на постійні інтеграційно-глобалізаційні процеси в світі провідні світові держави вже приділяють посилену вагу до питання пошуку систем захисту та протидії кіберзагрозам як внутрішнього, так і зовнішнього характеру. Для цього формуються національні системи кібербезпеки, які здатні об'єднувати зусилля багатьох систем, органів та приватного сектору для боротьби із такими загрозами.

Отже, система кібербезпеки держави – це комплекс спеціальних врегульованих нормативно суб'єктів забезпечення кібербезпеки, а також відповідних методів, засобів, прийомів та заходів, які використовуються та здійснюються з даною метою у кіберпросторі.

В Україні своя власна система кібернетичної безпеки знаходиться в стадії формування. Так, ще в 2005 р. Україна ратифікувала норми Конвенції Ради Європи про кіберзлочинність (Закон України № 2824-IV від 07 вересня 2005 р.). крім того, в свій час у цій сфері була прийнята ще ціла низка нормативно-правових актів, серед яких слід назвати Закони України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про інформацію», «Про державну таємницю», «Про основи національної безпеки України», а також окремі положення Кримінального кодексу, постанови уряду та рішення РНБО [11, с. 301].

Важливим етапом у створенні системи кібербезпеки держави став Указ Президента України № 1119/2010 від 10 грудня 2010 р. «Про виклики та загрози національній безпеці України у 2011 р.». Цей закон схвалив ідею створення Єдиної загальнонаціональної системи протидії кіберзлочинності. Згодом в 2012 р. було створено спеціальний департамент контр розвідувального захисту інтересів держави у сфері інформаційної безпеки відповідно до Указу Президента України «Про внесення змін до деяких законів України про структуру та порядок обліку кадрів Служби Безпеки України» № 34 від 25 січня 2012 р. Крім того, ще в липні 2010 р. для боротьби із кіберзлочинами та пов'язаної з ними торгівлі людьми при МВС України був створений новий підрозділ – Департамент боротьби із кіберзлочинністю та торгівлею людьми.

Згодом питання кібербезпеки, особливо із розв'язанням Росією неоголошеної «гібридної» війни на сході України, вийшло на новий щабель свого обговорення та розв'язання. Так, в травні 2015 р. РНБО прийняла рішення «Про стратегію національної безпеки України», затверджене згодом Указом Президента України № 287/2015 в травні 2015 р. Згодом у січні 2016 р. Рада національної безпеки та оборони ухвалила своїм рішенням новий програмний документ «Про стратегію кібербезпеки України». Дане рішення було введене в дію 16 березня 2016 р. Указом Президента України № 96/2016. Прийнята Стратегія, ґрунтуючись на основних положеннях Конвенції Ради Європи про кіберзлочинність, вітчизняного законодавства в даній сфері, основ зовнішньої та внутрішньої політики. Ця стратегія розрахована до 2020 р. і передбачала розробку, впровадження та реалізацію системи відповідних заходів, напрямів і прийомів забезпечення кібербезпеки держави:

− створення й адаптація державної політики України, спрямованої на подальший розвиток кіберпростору з одночасним досягненням у майбутньому повної сумісності з відповідними без пековими стандартами ЄС і НАТО;

– формування відповідного безпекового середовища у царині електронних комунікаційних мережевих структур, а також надання різноманітних послуг кіберзахисту та захисту інформації;

– залучення висококваліфікованих експертів та експертних груп вітчизняних наукових установ, окремих приватних професійних та громадських об'єднань до обговорення та вирішення питань підготовки проектів концептуальних актів у сфері кібербезпеки;

– подальше підвищення електронної грамотності населення та відповідної культури безпечного поводження в мережі Інтернет;

– подальший розвиток міжнародного кібербезпекового співробітництва [2].

Надалі у грудні 2016 р. РНБО прийняла рішення ««Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», яке було введено в дію відповідним Указом Президента України № 32/2017 від 13 лютого 2017 р. [3]. Нарешті 05 жовтня 2017 р. був прийнятий Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Цей закон визначив:

1) основний термінологічний ряд дефініцій, які використовуються в понятті «кібербезпека»; так зокрема, кібербезпека трактується як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі…»; також були визначені дефініції індикаторів кіберзагроз, кібератаки, кіберзагрози, кіберзахист, кіберзлочин (або комп'ютерний злочин), кіберзлочинність та ін.;

2) принципи та межі застосування норм кібербезпеки;

3) нормативно-правові засади забезпечення кібербезпеки України, яку становлять:

– Конституція України;

– Закони України, які торкаються засад національної безпеки, захисту інформації, мережевих ресурсів;

– Конвенція Ради Європи про кіберзлочинність та інші ратифіковані Верховною Радою України міжнародні правові акти в даній сфері;

– Укази Президента України в сфері кібербезпеки;

– акти уряду, РНБО та інших структур;

4) об'єкти та суб'єкти кібербезпеки і кіберзахисту в Україні;

5) об'єкти інфраструктури, які визначені як критичні в сфері кібербезпеки;

6) основні засади створення та функціонування Національної системи кібербезпеки України та органи, які забезпечують її діяльність;

7) принципи та норми реагування на комп'ютерні НС в Україні згідно команди CERT-UA;

8) основні засади державно-приватної взаємодії у царині кібербезпеки;

9) принципи та форми контролю за дотриманням норм і проведенням відповідних заходів із забезпечення кібербезпеки України [1].

До речі, хочеться окремо наголосити саме на команді CERT-UA. ComputerEmergency ResponseTeamofUkraine, або CERT-UA – спеціалізована команда реагування на надзвичайні комп'ютерні ситуації введена в дію ще в 2007 р. як окремий структурний підрозділ при державному центрі захисту ІТ- систем Державної служби спеціального зв'язку та захисту інформації. Основна мета діяльності CERT-UA – забезпечувати захист державних ресурсів інформації від злочинного незаконного доступу та неправомірного їх застосування, системних порушень цілісності інформаційних систем, їх конфіденційності та доступності.

Відзначимо, що сьогодні кібербезпекові загрози характеризуються значною асиметрією, глобальністю та динаміко, що значно ускладнює можливість їх виявлення та практичній реалізації відповідних заходів реагування з боку держави. Ще більше підвищують ризики кіберпростору, за словами І.В. Діордіци, його глобальність і всеосяжність. Вчений разом із В.А. Ліпканом виводить основні кіберзагрози національній безпеці України, серед яких:

– загрози гібридної війни з боку Російської Федерації;
– недостатній рівень кіберграмотності та медіа-культури населення;
– недостатній рівень про робленості на державному рівні комплексного цілісного підходу до комунікативної політики;
– вразливість до сучасних кіберзагроз ключових вітчизняних об'єктів інфраструктури й офіційних електронних ресурсів, особливо від кібератак хакерів;
– моральна застарілість і фізична зношеність матеріальної бази кіберпростору;
– застарілість і недосконалість сучасних форм і методів боротьби з кіберзлочинністю;
– слабкість системи охорони державної таємниці в Україні тощо [5; 6, с. 60].

Саме для подолання цих кіберзагроз і необхідно створення єдиної національної системи кібербезпеки, яке передбачене вище згадуваною нами Стратегією кібербезпеки України для створення безпечних умов використання кіберпростору в інтересах держави і всього суспільства.

Як справедливо зазначають К.Л. Бугайчук і Г.М. Шорохова, для подальшої розбудови ефективної та дієвої системи кібернетичної безпеки в Україні необхідно:

1) Чітко визначити спрямованість, зміст, форми та методи державної політики в сфері кібербезпеки.

2) Створити та впорядкувати відповідні організаційні структури, які будуть займатися дотриманням безпеки у кіберпросторі.

3) Налагодити ефективний процес управління безпекою у кіберпросторі та створити належні умови для реалізації запланованих заходів по кібербезпеці.

4) Налагодити чітку взаємодію між відповідними компетентними державними органами у сфері кібербезпеки та відповідну ефективну координацію їх діяльності.

5) Створити новітні механізми державного управління кібербезпекою через відкриття спеціалізованих наукових установ, центрів підготовки та експериментальних майданчиків.

6) Проводити активні дослідження у сфері інформаційних операцій, заохочувати дослідно-конструкторську та науково-технічну роботу в даній сфері [4, с. 135].

Саме тому питання кібекрбезпеки держави і далі повинно стояти на порядку денному всіх державних інституцій та систем влади.

Висновки. Кібербезпека є вкрай важливим елементом у системі національної безпеки держави, головна мета якої полягає у забезпеченні безпеки кіберпростору. Саме відповідний рівень захищеності кіберпростору і систем інформації є необхідною умовою функціонування та розвитку сучасного інформаційного суспільства. Нині, незважаючи на велику увагу до даної проблеми, сучасна система кібербезпеки в України тільки формується. Ще й досі проблемним питанням залишається ефективність і злагодженість взаємодії компетентних органів та інституцій з громадськістю у цьому питанні. У майбутньому має бути вибудувана чітка єдина Національна система кібербезпеки, яка має ґрунтуватися на вдосконаленій нормативно-правовій базі, скоординованій взаємодії СБУ, МВС, РНБО, інших зацікавлених органів та структур та, зрештою, всього суспільства.

Список використаних джерел:

1. «Про основні засади забезпечення кібербезпеки України» : Закон України № 2163-VIII від 05 жовтня 2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005#n107 (дата звернення: 11.11.2019).

2. Про рішення Ради Національної безпеки та оборони від 27 січня 2016 р. «Про стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 р. № 96/2016. URL: https://zakon5.rada.gov.ua/ laws/show/96/2016 (дата звернення: 11.11.2019).

3. Про рішення Ради національної безпеки і оборони України від 10 липня 2017 р. «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» : указ Президента України № 32/2017 від 13 лютого 2017 р. URL: http://zakon3.rada.gov.ua/laws/show/254/2017 (дата звернення: 11.11.2019).

4. Бугайчук К.Л., Шорохова Г.М. Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно-правові аспекти. *Протидія терористичній діяльності* : міжнародний досвід і його актуальність для України : матеріали ІІ Міжнародної науково-практичної конференції (15 грудня 2017 р.). Київ : Національна академія прокуратури України, 2018. С. 135–138.

5. Діордіца І.В. Поняття та зміст національної системи кібербезпеки. URL: http://goal-int.org/ponyattyata-zmist-nacionalnoi-sistemi-kiberbezpeki/ (дата звернення: 11.11.2019).

6. Ліпкан В.А. Поняття системи забезпечення національної безпеки України. *Право і Безпека*. 2003. Т. 2. № 4. С. 57–60.

7. Політологія : навчальний посібник / М.П. Гетьманчук, В.К. Грищук, Я.Б. Турчин та ін. ; за заг. ред. М.П. Гетьманчука. Київ : Знання, 2010. 415 с.

8. Скулиш Є.Д. Інформаційна безпека: нові виклики українському суспільству. *Інформація і право*. № 2 (5). 2012. С. 175–183.

9. Ткаченко В.І., Смірнов Є.Б., Астахов О.О. Шляхи формування системи забезпечення національної безпеки. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2015. № 2. С. 3–8.

10. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* № 2 (5). 2012. С. 162–175.

11. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* Київ : Міжвідом. наук.-дослід. Центр з проблеми боротьби з організ. злочинністю. 2012. № 2 (28). С. 299–309.

КРАВЧУК М. Ю.,
кандидат юридичних наук,
доцент кафедри кримінального права та процесу
(Тернопільський національний економічний університет)

УДК 343.985:343.326
DOI https://doi.org/10.32842/2078-3736-2019-6-2-8

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО УКРАЇНИ У СФЕРІ ПРОТИДІЇ ЗАГРОЗАМ БІОЛОГІЧНОГО ТЕРОРИЗМУ

У статті проаналізовано факт існування загроз біологічного тероризму як глобальну проблему світової спільноти та охарактеризовано тенденції міжнародної правової протидії цьому негативному явищу. Доведено, що протидія біотероризму вимагає консолідації зусиль усіх держав, а участь України у цьому процесі здійснюється відповідно до міжнародних договорів.

Здійснено аналіз норм окремих міжнародних нормативно-правових актів, що регулюють питання протидії тероризму. Визначено їх основні нормативно-правові приписи, необхідні для виконання Україною, які полягають у тому, що для ефективної боротьби зі збільшенням кількості і посиленням наслідків актів тероризму, а також у зв'язку із міжнародним характером терористичної діяльності, наша держава повинна посилювати співробітництво в цій сфері шляхом: