РОЗДІЛ 11
МІЖНАРОДНЕ ПРАВО

УДК 341: 343.34: 316.774

ПОНЯТТЯ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АСПЕКТ

THE DEFINITION OF INTERNATIONAL CYBER SECURITY: COMPARATIVE LEGAL ISSUE

Грицун О.О.,
здобувач кафедри міжнародного права
Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

Стаття присвячена аналізу концепцій розвитку поняття міжнародної інформаційної безпеки як з позицій міжнародного права, так і з точки зору окремих національних доктрин. Значну увагу автором приділено принципам, елементам та науковим підходам до розуміння принципових питань міжнародної інформаційної безпеки. Аналіз міжнародних договорів та норм національного законодавства окремих держав дає змогу краще зрозуміти доктринальні підходи до поняття міжнародної інформаційної безпеки, визначити їх спільні та відмінні риси.

Ключові слова: міжнародна інформаційна безпека, інформаційний простір, міжнародне право, міжнародні організації, національна доктрина.

Статья посвящена анализу концепций развития понятия международной информационной безопасности как с точки зрения международного права, так и с точки зрения отдельных национальных доктрин. Значительное внимание автором уделено принципам, элементам и научным подходам к пониманию принципиальных вопросов международной информационной безопасности. Анализ международных договоров и норм национального законодательства отдельных государства позволяет глубже понять доктринальные подходы к определению международной информационной безопасности, определить их общие и отличительные черты.

Ключевые слова: международная информационная безопасность, информационное пространство, международное право, международные организации, национальная доктрина.

This article is devoted to the analysis of the development frameworks of the concept of international cyber security, both from the point of view of international law, and from the point of view of certain national doctrines. Author pays significant attention to the principles, elements and scientific approaches to understanding the fundamental issues of international cyber security. The analysis of international treaties and provisions of national legislation gives us a key to understand the doctrinal approaches to the international cybersecurity concepts and to determine theirs' common and distinctive features.

Key words: international cyber security, cyber space, international law, international organization, national doctrine.

Постановка проблеми. Питання посилення міжнародної інформаційної безпеки стоїть на порядку денному переважної більшості міжнародних організацій та всіх без виключення держав. Доказом цього може служити той факт, що в рамках Організації Об'єднаних Націй питання міжнародної інформаційної безпеки визнані одними з найбільш пріоритетних та щорічно піднімаються під час засідань Генеральної Асамблеї ООН у відповідних резолюціях з метою визначення єдиного підходу до розуміння цього поняття, класифікації загроз та опрацювання напрямів співробітництва. Актуальність теми дослідження викликана відсутністю єдиного понятійного апарату у сфері регулювання міжнародної інформаційної безпеки та фрагментарністю існуючих міжнародних документів, присвячених цій проблемі.

Аналіз досліджень та публікацій. Частково питання міжнародної інформаційної безпеки висвітлювались у працях В.І. Мунтіяна, І.Л. Бачило, І.М. Рассолова, О.О. Стрельцова, В.М. Лопатіна, А.О. Малюка, А.В. Крутських, С. Гормана, Р. Кнейки, Т. Мерера, М. Герке, К. Форда та інших. Питтям безпеки в інформаційному просторі також присвячені дослідження А.Д. Єлякова, А.А. Яковенко, В.О. Плешакова та О.Ю. Шумилова. Водночас концептуальні підходи до розуміння міжнародної інформаційної безпеки та її складових елементів залишились малодослідженими та потребують подальшого наукового висвітлення.

Мета статті – проаналізувати існуючі документи міжнародних та регіональних організацій, національні доктрини та концептуальні проекти, присвячені питанням міжнародної інформаційної безпеки, та визначити основні підходи до розуміння цього поняття світовим співтовариством.

Виклад основного матеріалу. Стрімкий розвиток інформаційно-комунікаційних технологій та виникнення загроз, пов'язаних із кіберзлочинністю, кібертероризмом та інформаційними війнами, призвели до формування в різних державах окремих стратегій забезпечення інформаційної безпеки, за допомогою яких вони закріплюють своє бачення

відповідного поняття, визначають загрози в інформаційний сфері та вектори національних зусиль і міжнародного співробітництва з метою протистояння інформаційним загрозам.

Так, постановою Уряду Фінляндії від 25 січня 2013 року було прийнято «Стратегію кібербезпеки Фінляндії», яка визначила основні терміни, ключові цілі та керівні принципи, що використовуються для реагування на загрози в кіберпросторі і забезпечують його функціонування. Відповідно до вищезазначеної стратегії під «кібербезпекою» розуміється «бажаний кінцевий стан, в якому забезпечується її належне функціонування та надійність кіберпростору» [1]. Кібербезпека включає в себе заходи для функціонування необхідної для суспільства критичної інфраструктури, стійкої до кіберзагроз та їх наслідків. Бачення кібербезпеки зводиться до таких чинників: держава здатна захистити свої життєво важливі функції від кіберзагроз у всіх ситуаціях; громадяни, державні органи та комерційні компанії можуть ефективно користуватись безпечним кіберпростором та компетенцією, що випливає із заходів кібербезпеки як у державному, так і в міжнародному масштабі. Виходячи з цього бачення у Фінляндії було розроблено стратегічні керівні принципи кібербезпеки, що покликані посилити державно-приватне співробітництво у сфері регулювання питань кібербезпеки.

До переліку таких принципів увійшли такі: «створення ефективної моделі співробітництва між органами державної влади та іншими суб'єктами з метою посилення кібербезпеки та кіберзахисту; посилення національної кібербезпеки шляхом активної участі у діяльності міжнародних організацій та форумів співробітництва, присвячених питанням кібербезпеки; забезпечення ефективних заходів кіберзахисту через національне законодавство; визначення завдань, пов'язаних із кібербезпекою, моделей обслуговування та загальних стандартів управління кібербезпекою, а також реалізація стратегії кібербезпеки держави» [1].

Таким чином, стратегія кібербезпеки Фінляндії визначила напрями внутрішньої безпеки, воєнного потенціалу, міжнародного співробітництва, функціонування економіки та інфраструктури держави, а також напрями державно-приватного партнерства в питаннях протистояння кіберзагрозам.

У червні 2013 року Республіка Індія також прийняла документ під назвою «Національна політика кібербезпеки». У цьому документі наголошується, що основним завданням політики кібербезпеки визнано «захист інформації та інформаційної інфраструктури в кіберпросторі, збільшення потенціалу для попередження кіберзагроз та реагування на них, а також зменшення вразливості та збитків від кіберзлочинів шляхом поєднання інституціональних структур, людей, процесів, технологій та співробітництва» [2].

Основними напрямами національної політики визначено: створення безпечної екосистеми кіберпростору; вдосконалення нормативно-правової бази; створення механізмів попереднього сповіщення про загрози для безпеки, управління вразливістю та реагуванням на загрози безпеці; забезпечення безпеки послуг електронного управління; захист стійкості критичної інформаційної інфраструктури; сприяння науково-дослідним та дослідно-конструкторським роботам у сфері кібербезпеки; забезпечення поінформованості про кібербезпеку; створення ефективного державно-приватного партнерства та обмін інформацією і співробітництво [2]. Таким чином, Індія спрямовує всі свої зусилля на побудову захищеного та стійкого кіберпростору для громадян, приватного сектора та безпосередньо держави. Значна увага в документі приділяється також питанню формування культури кібербезпеки та недоторканності приватного життя.

У 2003 році Сполученими Штатами Америки було прийнято «Національну стратегію кібербезпеки США», що визначила загрози у кіберпросторі, основні принципи національної політики в цій сфері та пріоритети національної кібербезпеки. До 5 національних пріоритетів входять: формування системи протидії інформаційним загрозам, розробка програми зі зниження вразливості та загроз національній кібербезпеці, розробка тренінгів та навчальних програм з метою підвищення обізнаності про кіберзагрози; посилення інформаційної безпеки уряду, а також принципи національної безпеки та міжнародного співробітництва у кіберпросторі [3].

Крім того, у 2011 році США прийняли «Міжнародну стратегію щодо кіберпростору. Процвітання, безпека та відкритість мережевого світу». Цей документ визначив керівні принципи, яких необхідно дотримуватись для створення безпечного та відкритого інформаційного простору. Основним принципом відповідно до цієї стратегії визнано міжнародне співробітництво. Крім нього, до основоположних принципів увійшли такі: захист основних свобод людини і громадянина, захист права власності, повага до приватного життя, захист від кіберзлочинців, право на самооборону держав у разі агресії в кіберпросторі, повага до свободи поширення інформації в національних мережах, гарантування надійного доступу до мережі Інтернет, багатостороннє управління Інтернетом та принцип відповідальності держав за захист власних інформаційних інфраструктур [4]. Варто додати, що у своїй доповіді, поданій на ім'я Генерального Секретаря ООН на виконання резолюцій «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки», США зазначили, що до числа основних суб'єктів, які є загрозою для надійного функціонування кіберпростору, входять держави, злочинці, терористи та посередники, у такий спосіб наголосивши на тому, що держави повинні поглиблювати безпеку інформаційного простору незалежно від джерела загрози [5].

В українському законодавстві поняття інформаційної безпеки закріплено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Відповідно до положень цього закону «інформаційна безпека – це

стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [6].

Крім того, Законом України «Про основи національної безпеки України» визначено перелік загроз національним інтересам і національній безпеці України в інформаційній сфері, до них увійшли такі: «прояви обмеження свободи слова та доступу до публічної інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації» [7].

Варто зауважити, що 8 липня 2009 Указом Президента України було затверджено «Доктрину інформаційної безпеки України». Відповідно до положень цього документу інформаційну безпеку визнано невід'ємною складовою кожної зі сфер національної безпеки та важливою самостійною сферою забезпечення національної безпеки [8]. Доктрина інформаційної безпеки закріпила життєво важливі інтереси в інформаційній сфері, розподіливши їх на окремі блоки залежно від об'єкту – особи, суспільства та держави. Також у документі перераховано реальні та потенційні загрози інформаційній безпеці України та напрями державної політики у сфері інформаційної безпеки України в таких сферах: зовнішньополітичній, воєнній, внутрішньополітичній, економічній, соціальній та гуманітарній, у науково-технічній, екологічній та у сфері державної безпеки [8]. Цей документ втратив чинність 30 червня 2014 року, а нова редакція опрацьовується Державним комітетом телебачення і радіомовлення України.

Досліджуючи поняття інформаційної безпеки, російська наукова школа інформаційного права стоїть на позиції визначення інформаційної безпеки як «стану захищеності національних інтересів держави в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства та держави, в яку входять чотири основні складові національних інтересів держави, а саме: дотримання конституційних прав і свобод людини і громадянина у сфері отримання інформації та користування нею, збереження моральних цінностей суспільства, культурного та наукового потенціалу країни; інформаційне забезпечення державної політики щодо надання достовірної інформації про державну політику, офіційну позицію держави щодо соціально значимих подій як усередині країни, так і за кордоном із забезпеченням доступу громадян до відкритих державних інформаційних ресурсів; розвиток сучасних інформаційних технологій, індустрії засобів інформатизації, телекомунікації та зв'язку, забезпечення потреб внутрішнього ринку її продукцією та вихід цієї продукції на світовий ринок, забезпечення накопичення, збереження та ефективного використання інформаційних ресурсів; а також захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних та телекомунікаційних систем» [9]. Відповідно до вищезазначених складових національних інтересів, російська доктрина класифікує загрози інформаційній безпеці на такі види: загрози конституційним правам та свободам людини і громадянина у сфері духовності та в інформаційній діяльності, індивідуальній, груповій та суспільній свідомості; загрози інформаційному забезпеченню державної політики; загрози розвитку індустрії інформатизації, телекомунікації та зв'язку та загрози безпеці інформаційних та телекомунікаційних засобів і систем [9].

Міжнародне співтовариство також приділяє значну увагу питанням міжнародної інформаційної безпеки. Питання забезпечення безпеки в кіберпросторі піднімаються в рамках Організації Об'єднаних Націй, Міжнародного Союзу Електрозв'язку, Ради Європи, Європейського Союзу, Організації Північноатлантичного Договору, Шанхайської Організації Співробітництва, Співдружності Незалежних Держав, Організації з безпеки та співробітництва в Європі та низки інших міжнародних та регіональних організацій.

Уперше питання забезпечення міжнародної інформаційної безпеки на регіональному рівні були закріплені в Угоді про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації від 01 червня 2001 року. Угода держав-учасниць СНД визначила перелік діянь в інформаційній сфері, що тягнуть за собою кримінальну відповідальність, порядок призначення компетентних органів держав-учасниць, форми співробітництва держав, врегулювала питання порядку надання запитів про сприяння, виконання таких запитів, питання конфіденційності інформації та порядок вирішення спорів. Відповідно до положень Угоди умисними діяннями, що тягнуть за собою кримінальну відповідальність, визнано такі: «здійснення неправомірного доступу до комп'ютерної інформації, що охороняється законом, якщо таке діяння призвело до знищення, блокування, модифікації чи копіювання інформації, порушення роботи ЕОМ, систем ЕОМ чи їх мереж; створення, використання чи поширення шкідливих програм; порушення правил експлуатації ЕОМ, систем ЕОМ чи їх мереж особою, що мала до них доступ, і якщо таке діяння спричинило суттєву шкоду чи тяжкі наслідки; незаконне використання програм для ЕОМ та баз даних, що є об'єктами авторського права, привласнення авторства, якщо таке діяння спричинило суттєві збитки» [10]. До основних форм співробітництва держав відповідно до Угоди віднесено: обмін

інформацією про злочини у сфері комп'ютерної інформації, про форми і методи розслідування злочинів у даній сфері та про національне законодавство та міжнародні договори, що регулюють ці питання; виконання запитів про проведення оперативно-пошукових заходів та процесуальних дій у цій сфері; планування та проведення скоординованих заходів щодо попередження, виявлення та розслідування комп'ютерних злочинів, надання сприяння в підготовці підвищення кваліфікації кадрів; створення інформаційних систем, що забезпечують виконання завдань щодо виявлення, запобігання та розслідування комп'ютерних злочинів; проведення спільних наукових досліджень у цій сфері; обмін нормативно-правовими актами та інші форми співробітництва [10]. Незважаючи на те, що Угода держав-членів СНД врегулювала лише кримінальний аспект міжнародної інформаційної безпеки, вона стала першим кроком до врегулювання цього питання на рівні міжнародних організацій.

Наступним документом у сфері забезпечення інформаційної безпеки стала Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року. Як і Угода держав-членів СНД, Конвенція Ради Європи включила до сфери свого регулювання лише кримінальний аспект міжнародної інформаційної безпеки. Злочини у конвенції класифіковано на чотири групи: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем; правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані зі змістом інформації; правопорушення, пов'язані з порушенням авторських і суміжних прав. Додатковим протоколом від 2003 року до цього переліку було додано п'яту групу правопорушень – правопорушення, пов'язані з діями расистського та ксенофобського характеру, вчиненими через комп'ютерні системи [11].

Наступним кроком у сфері регулювання питань міжнародної інформаційної безпеки стало прийняття в рамках Шанхайської Організації Співробітництва Угоди між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року. На противагу двом вищезгаданим міжнародним документам Угода держав-членів ШОС регулює три аспекти міжнародної інформаційної безпеки – кримінальний, терористичний та військово-політичний, а також визначає формат, цілі, принципи, напрями та механізми співробітництва держав-учасниць. У Додатку 1 до Угоди закріплено визначення терміна «міжнародна інформаційна безпека», під якою розуміють «стан міжнародних відносин, що виключає порушення стабільності у світі та створення загрози безпеці держав та світового співтовариства в інформаційному просторі» [12]. Крім цього, в угоді надається класифікація загроз у сфері забезпечення міжнародної інформаційної безпеки відповідно до її поділу на три аспекти. Так, до військово-політичних загроз відповідно до Угоди віднесено: «розробку та застосування інформаційної зброї, підготовку та ведення інформаційної війни; використання домінуючого становища в інформаційному просторі з метою нанесення шкоди інтересам та безпеці інших держав; поширення інформації, що наносить шкоду суспільно-політичному, соціально-економічному, духовному, моральному та культурному середовищу інших держав; загрози безпечному та стабільному функціонуванню глобальних та національних інформаційних інфраструктур». Головною терористичною загрозою визнано інформаційний тероризм, а кримінальною – інформаційну злочинність [12].

У рамках дослідження поняття міжнародної інформаційної безпеки доцільно було б згадати і концептуальні підходи до розуміння цього поняття, що закріплені у відповідних проектах та концепціях окремих законодавців та науковців.

Своє розуміння інформаційної безпеки Російська Федерація запропонувала міжнародному співтовариству у проекті Конвенції із забезпечення міжнародної інформаційної безпеки (концепція) у 2011 році. Варто звернути увагу на те, що запропонована концепція повністю відтворює визначення міжнародної інформаційної безпеки, закріплене в Угоді держав-членів ШОС, хоча дещо розширює загальний перелік термінів, додаючи до нього визначення доступу до інформації, інформаційної системи, інформаційно-комунікаційних технологій, оператора інформаційної системи, правопорушення в інформаційному просторі, а також надання та поширення інформації. Проект Конвенції, запропонований Російською Федерацією, суттєво розширив коло військово-політичних загроз у сфері міжнародної інформаційної безпеки та визначив основні принципи забезпечення інформаційної безпеки. Заходи протидії загрозам в інформаційній сфері розподілено окремими розділами на три блоки: заходи щодо попередження та вирішення воєнних конфліктів в інформаційному просторі, заходи протидії використанню інформаційного простору в терористичних цілях та заходи протидії правопорушенням в інформаційній сфері відповідно. Крім цього, концепція Конвенції передбачає заходи щодо забезпечення організації кримінального процесу, напрями міжнародного співробітництва держав, консультативну допомогу та заходи довіри у сфері воєнного використання інформаційного простору [13]. Таким чином, проект Конвенції загалом відтворює підхід держав-членів ШОС до розуміння міжнародної інформаційної безпеки, але деталізує та суттєво розширює її положення.

Крім цього, у 2011 році професори Штайн Шольберг та Соланж Гернуті-Елі опублікували друге видання робочого проекту «Загального договору з питань кібербезпеки та кіберзлочинності» [14].

Документ складається з преамбули та трьох частин. У преамбулі договору йдеться про напрацювання всіх міжнародних та регіональних організацій у сфері кібербезпеки, зокрема про проведену роботу в рамках ООН, Міжнародного Союзу Електрозв'язку та конвенцію Ради Європи про кіберзлочинність 2001 року. Основна частина документу складається з трьох частин: заходи у сфері кримінального права; заходи у сфері процесуального права та у сфері

кримінального переслідування; заходи в глобальній юрисдикції.

До заходів у сфері кримінального права автори проекту відносять незаконний доступ, незаконне прослуховування, незаконний доступ до комп'ютерних даних, незаконний доступ до комп'ютерної системи, злочинне використання пристроїв, комп'ютерні підробки, комп'ютерне шахрайство, злочини, пов'язані з дитячою порнографією, крадіжка інформації, масові та скоординовані атаки проти інформаційно-комунікаційних інфраструктур, запобігання тероризму та іншим серйозним кібератакам та підготовчі дії.

У наступній частині документу, що присвячена заходам у сфері процесуального права та у сфері кримінального переслідування, йдеться про: сферу застосування процесуальних положень, умови та гарантії, забезпечення цілісності збережених комп'ютерних даних, забезпечення цілісності та частковий доступ до інформації про трафік, інформаційні запити, пошук та конфіскація збережених комп'ютерних даних, збір інформації про трафік у реальному часі та перехоплення даних контенту.

Відповідно до заключної частини проекту договору держави повинні вжити всіх необхідних законодавчих та інших заходів з метою визначення юрисдикції щодо будь-якого злочину, зазначеного в договорі, якщо такий злочин скоєно: «на її території; на борту судна, що плаває під прапором цієї держави; на борту повітряного судна, зареєстрованого відповідно до законодавства цієї держави; одним із громадян цієї держави, якщо злочин тягне за собою покарання згідно з кримінальним законом держави, де воно було скоєно, або якщо злочин скоєно за межами територіальної юрисдикції будь-якої держави» [14].

Таким чином, Проект договору Штайна Шольберга та Соланж Гернуті-Елі можна сміливо назвати доктринальним досягненням, що претендує на глобальні нововведення в питаннях міжнародно-правового регулювання кібербезпеки.

Висновки. Проаналізувавши підходи до регулювання питань міжнародної інформаційної безпеки в законодавстві окремих країн, у документах міжнародних та регіональних організацій, а також розглянувши концептуальні напрацювання в цій сфері, приходимо до висновку, що питання посилення інформаційної безпеки, визначення основних загроз в інформаційному просторі та розробка напрямів співробітництва, безперечно, є пріоритетним напрямом діяльності як окремих держав, так і міжнародних організацій. Формування системи міжнародної інформаційної безпеки відбувається на основі двох основних поглядів. Прихильники першого з них обмежуються розумінням міжнародної інформаційної безпеки як забезпечення кримінального покарання за злочини в інформаційному просторі, прихильники ж другого погляду наполягають на розширеному розумінні міжнародної інформаційної безпеки як протидії інформаційному тероризму, інформаційним війнам та кіберзлочинам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Finland's Cyber Security Strategy [Електронний ресурс]. – Режим доступу : http://www.yhteiskunnanturvallisuus.fi/en/materials.

2. India National Cyber Security Strategy [Електронний ресурс]. – Режим доступу : http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss.

3. The National Strategy to Secure Cyberspace [Електронний ресурс]. – Режим доступу : https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

4. International Strategy for Cyberspace [Електронний ресурс]. – Режим доступу : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

5. Резолюция ГА ООН A/RES/66/24 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Електронний ресурс]. – Режим доступу : http://www.un.org/ru/documents/ods.asp?m=A/RES/66/24.

6. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – С. 102.

7. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351. Зі змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – С. 116.

8. Указ Президента України «Про Доктрину інформаційної безпеки України» [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/514/2009/card5#Links.

9. Доктрина інформаційної безпеки Російської Федерації від 09.09.2000 [Електронний ресурс]. – Режим доступу : http://www.scrf.gov.ru/documents/6/5.html.

10. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 года // Московский журнал международного права. – 2008. – № 4 (72). – С. 244–250.

11. Конвенція про кіберзлочинність від 23 листопада 2001 року [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_575.

12. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года [Електронний ресурс]. – Режим доступу : http://base.spinform.ru/show_doc.fwx?rgn=28340.

13. Конвенция об обеспечении международной информационной безопасности (концепция) [Електронний ресурс]. – Режим доступу : http://www.mid.ru/bdomp/nsosndoc.nsf/e2f289bea6297f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument.

14. A Global Treaty on Cybersecurity and Cybercrime [Електронний ресурс]. – Режим доступу : http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.