УДК 341: 343.34: 316.774

РЕГУЛЮВАННЯ ПИТАНЬ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕЖАХ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ

Грицун О.О., здобувач

Інститут міжнародних відносин
Київського національного університету імені Тараса Шевченка,
вул. Мельникова, 36/1, м. Київ, Україна
olya_markevich@ukr.net

Статтю присвячено дослідженню питань становлення й розвитку проблеми регулювання міжнародної інформаційної безпеки в межах діяльності міжнародних організацій. Предметом дослідження статті є генезис поняття міжнародної інформаційної безпеки в межах Організації Об'єднаних Націй, Міжнародного Союзу Електрозв'язку, Ради Європи, Європейського Союзу, Організації Північноатлантичного Договору та Шанхайської Організації Співробітництва.

Ключові слова: міжнародна інформаційна безпека, кіберпростір, міжнародне право, кібератаки, інформаційно-комунікаційні технології.

РЕГУЛИРОВАНИЕ ВОПРОСОВ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ

Грицун О.А.

Институт международных отношений Киевского национального университета имени Тараса Шевченко,
ул. Мельникова, 36/1, г. Киев, Украина
olya_markevich@ukr.net

Статья посвящается исследованию вопросов становления и развития проблемы регулирования международной информационной безопасности в рамках деятельности международных организаций. Предметом исследования выступает генезис понятия международной информационной безопасности в рамках Организации Объединенных Наций, Международного Союза Электросвязи, Совета Европы, Европейского Союза, Организации Североатлантического Договора и Шанхайской Организации Сотрудничества.

Ключевые слова: международная информационная безопасность, киберпространство, международное право, кибератаки, информационно-коммуникационные технологии.

REGULATION OF INTERNATIONAL CYBER SECURITY WITHIN THE FRAMEWORK OF INTERNATIONAL ORGANIZATIONS

Grytsun O.O.

Institute of International Relations of Taras Shevchenko National University of Kyiv,
str. Melnykov, 36/1, Kyiv, Ukraine
olya_markevich@ukr.net

This article is devoted to the exploring the questions of formation and development of the regulation of international cyber security within the framework of international organizations. The genesis of the concept of international cyber security within the framework of the United Nations, the International Telecommunication Union, the Council of Europe, European Union, North Atlantic Treaty Organization and the Shanghai Cooperation Organization is the subject of the research.

Willingness of the vast majority of states to activate their joint efforts to counter transnational threats of the use of information and communication technologies and other high technology with the aim to solve the problem of international cyber security with maximum regard to the interests of all states resulted in the consideration of this issue both in the framework of the UN political dialogue, and in the other international organizations.

Since 1999, the UN General Assembly adopts an annual resolution named "Developments in the field of information and telecommunications in the context of international security", which emphasized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged and also considered that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes.

International Telecommunication Union as the United Nations specialized agency for information and communication technologies was instructed to assume the coordination of the Action Line C5 “Building confidence and security in the use of ICTs”. In 2007, the Global Cybersecurity Agenda (GCA), as a framework for international cooperation in this area, was adopted. GCA defines main principles, purposes and strategies for developing model legislation in the field of combating cybercrimes.

North Atlantic Treaty Organization (NATO) also pays great attention to security in cyberspace. Thus, in 2014, NATO members agreed a new Cybersecurity Strategy and extended Plan of Action, as mentioned in the Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.

In 2009 was signed the founding document of the SCO information security – Agreement between the Governments of the Member States of the SCO cooperation in ensuring international information security, which defined format, objectives, principles, directions and mechanisms of cooperation among States Parties.

Within the framework of the European Union according to the Decision № 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks the Action plan for a Safer Internet 1999–2004 was adopted. In 2005 the Council adopted a Decision establishing the Safer Internet Plus programme aimed at promoting the safer use of the Internet and new online technologies for 2005–2008. And after it the Safer Internet programme for 2009-2013 was adopted.

The Council of Europe also helps to protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime signed on 23 November 2001 and its Protocol on Xenophobia and Racism, also through the Cybercrime Convention Committee and the technical cooperation Programme on Cybercrime.

Key words: international cyber security, cyberspace, international law, cyber-attacks, information and communication technologies.

У добу інформаційних технологій і цифрового суспільства проблема використання інформаційно-комунікаційних технологій у злочинних цілях окремими особами, групами осіб чи державами набуває все більшого значення та все частіше стає предметом обговорення на міжнародних форумах та в межах міжнародних організацій, оскільки саме вони є найширшою та найдієвішою платформою для активізації спільних зусиль як держав, так і інших зацікавлених сторін діалогу з метою протидії транснаціональним загрозам із застосування інформаційно-комунікаційних технологій.

Окремі аспекти проблеми регулювання міжнародної інформаційної безпеки в межах діяльності міжнародних організацій розглядалися в працях М. Герке, А.В. Крутських, В. Сомерса, М. Грокса, І.Л. Бачило та М. Дюмонтьє. Проте малодослідженим залишилося питання комплексного аналізу основних нормативних документів міжнародних організацій, присвячених цій проблемі. Саме такий аналіз дає змогу краще зрозуміти особливості формування поняття міжнародної інформаційної безпеки та сприйняття його міжнародним співтовариством.

Мета статті – визначити місце та роль діяльності Організації Об’єднаних Націй (далі – ООН), Міжнародного Союзу Електрозв’язку, Ради Європи, Європейського Союзу, Організації Північноатлантичного Договору та Шанхайської Організації Співробітництва у сфері визначення та забезпечення міжнародної інформаційної безпеки.

Завдання статті: аналіз основних нормативних документів вищезазначених організацій щодо питання регулювання міжнародної інформаційної безпеки та визначення їхньої ролі у формуванні єдиного комплексного підходу до розуміння поняття міжнародної інформаційної безпеки.

У межах Організації Об’єднаних Націй питання інформаційної безпеки вперше було винесено на розгляд на 53 сесії Генеральної Асамблеї ООН у 1999 р. Сімдесят сім держав проголосували за Резолюцію 53/73 «Роль науки й техніки в контексті міжнародної безпеки та роззброєння», чим підтвердили готовність більшості держав до активізації зусиль,

спрямованих на унеможливлення використання досягнень науки й техніки у воєнній сферах із метою порушення міжнародного миру та безпеки.

Починаючи з 1999 р. Генеральна Асамблея ООН щорічно приймає резолюції під назвою «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки», у яких підкреслюється занепокоєність міжнародного співтовариства можливістю використання інформаційних технологій та засобів у цілях, несумісних із забезпеченням міжнародного миру та безпеки, а також неправомірним використанням інформаційних ресурсів та можливістю їх використання в протиправних чи терористичних цілях. Відповідно до цих резолюцій держави-члени ООН надають інформацію на ім'я Генерального секретаря щодо загальної оцінки проблем інформаційної безпеки, визначення основних понять інформаційної безпеки, включаючи поняття несанкціонованого втручання чи неправомірного використання інформаційних і телекомунікаційних систем та інформаційних ресурсів, а також доцільність розробки міжнародних принципів із метою зміцнення безпеки глобальних інформаційних і телекомунікаційних систем та боротьби з інформаційним тероризмом та криміналом [1].

З метою реалізації положень цих резолюцій було створено Групу урядових експертів із питань досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки. Під час проведення 68-ї сесії Генеральної Асамблеї ООН було заслухано доповідь про результати роботи групи урядових експертів, що містила перелік загроз у сфері інформаційної безпеки та низку рекомендацій щодо протидії цим загрозам. У вищезазначеному документі рекомендації розділені на три блоки: рекомендації щодо норм, правил та принципів відповідальної поведінки держав; рекомендації щодо заходів посилення довіри та обміну інформацією; рекомендації щодо заходів нарощування потенціалу [2].

Таким чином, ООН наразі залишається найбільшою платформою для обговорення питання інформаційної безпеки з результативного пошуку єдиного підходу до його врегулювання.

Проблема забезпечення міжнародної інформаційної безпеки стала предметом обговорення й у рамках Міжнародного союзу електрозв'язку (далі – МСЕ).

Під час проведення другого етапу Всесвітнього саміту з питань інформаційного суспільства (далі – ВСІС), що відбувся в Тунісі в 2005 р., МСЕ було доручено взяти на себе координацію напряму діяльності С5 «Зміцнення довіри та безпеки при використанні інформаційно-комунікаційних технологій (ІКТ)», оскільки на той момент МСЕ нараховує 191 державу-члена та більше 700 членів секторів та асоційованих членів і має унікальні можливості для того, щоб досягти консенсусу стосовно основ міжнародного співробітництва у сфері міжнародної інформаційної безпеки.

Експертами МСЄ було розроблено визначення терміну «кібербезпека», під якою вони розуміють «набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, а також професійну підготовку, практичний досвід, страхування та технології, що можуть бути використані для захисту кіберпростору, ресурсів організацій та користувачів» [3]. У 2007 р. у межах МСЕ було прийнято Глобальну програму кібербезпеки, що визначила основні принципи, цілі та стратегії розробки моделей законодавства у сфері боротьби з кіберзлочинністю. Глобальна програма кібербезпеки базується на п'яти стратегічних принципах, а саме: 1) правові заходи; 2) технічні та процедурні заходи; 3) організаційні структури; 4) створення потенціалу; 5) міжнародне співробітництво [4].

У межах МСЕ було прийнято низку резолюцій із питань кібербезпеки. Резолюція 50/2004 Всесвітньої асамблеї з питань стандартизації електрозв'язку МСЕ підтвердила нагальність проблеми забезпечення кібербезпеки у світі та доручила директору Бюро стандартизації електрозв'язку підготувати перелік національних, регіональних і міжнародних ініціатив із метою сприяння глобальному погодженню стратегій та підходів до вирішення проблеми

кібербезпеки. Резолюція 174/2010 підкреслила важливість рішень Всесвітнього саміту з питань інформаційного суспільства, зокрема й роль МСЕ. Крім великої кількості резолюцій у межах МСЕ, було прийнято низку рекомендацій, серед яких Рекомендація МСЕ-Т X.509 «Структура сертифікатів відкритих ключів та атрибутів (глобальний стандарт управління ідентифікацією)», Рекомендація МСЕ-Т серії X.8xx «Глобальні стандарти по ключовим аспектам безпеки», Рекомендація МСЕ-R M.1078 «Принципи безпеки для IMT-2000».

Велику увагу МСЕ приділяє проблемі забезпечення кібербезпеки в країнах, що розвиваються. Зокрема, у 2009 р. було запропоновано проект документу під назвою «Поняття кіберзлочинності: інструкція для країн, що розвиваються». Цей документ визначив поняття та типологію кіберзлочинності, статистичні показники кібернетичних правопорушень, основні проблеми боротьби з кіберзлочинністю та її стратегії, а також основні законодавчі підходи до розуміння поняття кіберзлочинності як на міжнародному, так і на регіональному рівнях [5].

Таким чином, Міжнародний союз електрозв'язку як спеціалізована установа Організації Об'єднаних Націй відіграє одну з найважливіших ролей у питаннях уніфікації технічних стандартів та забезпечення зміцнення довіри та безпеки під час використання інформаційно-комунікаційних технологій.

Організація Північноатлантичного договору (далі – НАТО) також приділяє значну увагу питанням безпеки в кіберпросторі. Так, уперше це питання в межах НАТО обговорювалося в листопаді 2002 р. під час Празького саміту. Лідери країн-членів НАТО виявили бажання посилювати свої можливості щодо протидії інформаційним атакам. У цей же час було створено Агентство НАТО з питань обслуговування комунікаційних та інформаційних систем. Це бажання ще раз було підтверджено під час Ризького саміту в 2006 р.

Після серії кібератак, спрямованих на урядові та неурядові установи Естонії в 2007 р., НАТО визнала кібератаки стратегічними загрозами, й у 2008 р. під час проведення саміту в Бухаресті міністрами оборони країн-членів НАТО була схвалена офіційна політика НАТО у сфері кібероборони.

Крім цього, важливим кроком у сфері боротьби з кібератаками стало створення в 2008 р. Управління з питань забезпечення кібероборони, що покликано координувати дії в разі кібератаки на когось із держав-членів та Центру експертизи з питань кооперативної кібероборони (CCDCOE) у Таллінні.

У червні 2011 р. було прийнято Доктрину кібербезпеки НАТО та відповідний план дій. Ці документи деталізували практичні кроки НАТО у сфері підвищення кібербезпеки. Основними елементами нового підходу стали такі: усвідомлення того, що кібероборона є необхідною вимогою для реалізації НАТО завдань колективної оборони; забезпечення кібероборони та централізованого захисту власних мереж НАТО; визначення мінімальних технічних вимог до національних інформаційних систем, що мають вирішальне значення для виконання основних завдань НАТО; допомога союзникам задля досягнення мінімального рівня кіберзахисту та зменшення вразливості національних критичних інфраструктур; удосконалення засобів попередження та попереднього реагування на інциденти в кіберпросторі [6].

У 2013 р. експертами Центру експертизи з питань кооперативної кібероборони (CCDCOE) у Таллінні було оприлюднено документ під назвою Талліннська інструкція з питань міжнародного права, що застосовуються до кібервійни (The Tallinn Manual on the International Law Applicable to Cyber Warfare). Цей документ не є офіційним документом ні CCDCOE, ні НАТО, лише відображає окрему точку зору експертів. Однак, не дивлячись на це, він надзвичайно цікавий з точки зору трактування існуючих норм міжнародного права та можливості їх застосування до ведення війни в інформаційному просторі. До основних ключових висновків авторів цього документа можна віднести такі: держави несуть

відповідальність за кібероперації проти інших держав, які здійснюються з їх території, навіть у тому випадку, якщо такі операції проводяться не спецслужбами цієї держави, а наприклад, залученими хакерами; заборона застосування сили, включаючи застосування сили в кіберпросторі [7].

Під час проведення Уельського саміту 4-5 вересня 2014 р. країни-члени НАТО ухвалили нову розширену політику кібероборони та новий план дій, про що йшлося в Декларації Уельського саміту глав держав та урядів, які брали участь у засіданні Північноатлантичної ради в Уельсі. Ця політика підтверджує принципи неподільності безпеки союзників та визначає, що міжнародне право, у тому числі міжнародне гуманітарне право та Статут ООН, застосовується в кіберпросторі, а рішення про те, що кібернапад призведе до застосування ст.5 Вашингтонського договору НАТО про колективну оборону буде прийматися Північноатлантичною радою на індивідуальній основі в кожному конкретному випадку.

У цілому аналіз діяльності Організації Північноатлантичного договору у сфері інформаційної безпеки засвідчує її намагання створити ефективні механізми, що дозволять оперативно реагувати на загрози в кіберпросторі.

Шанхайська організація співробітництва у своїх роботі також приділяє значну увагу питанням міжнародної інформаційної безпеки. У 2007 р. було створено групу експертів держав-членів Шанхайської організації співробітництва (далі – ШОС) та підготовлено План дій із забезпечення міжнародної інформаційної безпеки. Він стосувався нових викликів у галузі міжнародної інформаційної безпеки та передбачав проведення спільних заходів у сфері забезпечення інформаційної безпеки. У 2009 р. було підписано основоположний документ ШОС у сфері інформаційної безпеки – Угоду між урядами держав-членів ШОС про співробітництво у сфері забезпечення міжнародної інформаційної безпеки (далі – Угода), що визначила формат, цілі, принципи, напрями та механізми співробітництва держав-учасниць. Крім цього, в угоді надавалася класифікація загроз у сфері забезпечення міжнародної інформаційної безпеки. До них, зокрема, віднесено такі: розробка та застосування інформаційної зброї, підготовка та ведення інформаційної війни; інформаційний тероризм; інформаційна злочинність; 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. Додаток 1 до Угоди містив визначення таких базових понять, як «інформаційна безпека», «інформаційна війна», «інформаційний тероризм», «інформаційна зброя» та інші [8].

Ще одним важливим внеском ШОС у дослідження проблеми міжнародної інформаційної безпеки стало внесення 4-а державами-учасницями (Росією, Китаєм, Узбекистаном та Таджикистаном) на розгляд Генеральному секретарю ООН документу під назвою «Правила поведінки в сфері забезпечення міжнародної інформаційної безпеки». Цей документ було доопрацьовано та винесено на обговорення під час 66-ї сесії Генеральної Асамблеї ООН. Основною метою цього документу було визначення прав та обов'язків держав в інформаційному просторі, стимулювання їх відповідальної поведінки та посилення співробітництва [9].

Загалом країни-члени ШОС активно напрацьовують нормативну базу та понятійний апарат у сфері міжнародної інформаційної безпеки та спрямовують свої зусилля для втілення власних ініціатив та поглядів у межах ООН.

Разом з активізацією співробітництва між країнами Європейського Союзу в політичній, соціально-економічній, науково-технічній та культурній сферах, створенням єдиних інформаційних систем у фінансовій, банківській, страховій та інших сферах, а також створенням цифрових банків даних виникла проблема захисту персональних даних.

Тимчасовим вирішенням проблеми стало прийняття Директиви 95/46/ЄС Європейського парламенту та Ради «Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних» від 24 жовтня 1995 р. та Директиви 97/66/ЄС Європейського парламенту та Ради «Про обробку персональних даних і захист права на невтручання в особисте життя осіб у телекомунікаційному секторі». У цій директиві було визначено необхідність гармонізувати законодавства країн-членів з метою належного захисту персональних даних у телекомунікаційному секторі та забезпечення їхнього вільного обміну [10].

Наступним важливим кроком стало прийняття Європейським парламентом і Радою Рішення про багаторічний план дій Співтовариства зі сприяння безпечному використанню Інтернету шляхом боротьби із незаконним і шкідливим змістом у глобальних мережах № 276/1999/ЄС від 25 січня 1999 р. [11]. Ця програма отримала назву «План дій «Безпечний Інтернет» (1999-2004 рр.)». Вона покликана була сприяти формуванню сприятливого середовища для розвитку Інтернету в межах ЄС, прийняття кодексу поведінки глобальних мереж та можливої гармонізації правової термінології. У подальшому були прийняті відповідні програми «Безпечний Інтернет Плюс» на 2005–2008 рр. та «Безпечний Інтернет на 2009-2013 роки». Крім того, у межах ЄС було прийнято низку програм для вирішення проблем кіберзлочинності, зокрема такі: «Електронна Європа», «План дій щодо Інтернету», «Технології інформаційного суспільства». З метою формування нормативно-правової бази у сфері інформаційної безпеки було прийнято Директиву Європейського парламенту та Ради 2202/21/ЄС від 7 березня 2002 р. про загальну нормативно-правову базу для електронних комунікаційних мереж і послуг та Директиви 2002/20/ЄС, 2002/22/ЄС та 2002/58/ЄС. Директиви 2000/31/ЄС та 2002/19/ЄС у свою чергу врегулювали питання посилення безпеки суспільних інформаційних послуг та електронної комерції.

У березні 2004 р. було створено Європейське агентство з мережевої та інформаційної безпеки з метою забезпечення високого рівня захисту даних, формування культури кібербезпеки та сприяння підвищенню рівня поінформованості громадян.

Програми ЄС «Попередження й боротьба зі злочинністю» передбачали ключові моменти співробітництва у сфері протидії кіберзлочинності. Загалом у ЄС питання інформаційної безпеки зводиться до вирішення лише кримінальних аспектів, пов'язаних із використанням інформаційно-комунікаційних технологій.

Питання міжнародної інформаційної безпеки постали на порядку денному Ради Європи ще із середини 1970-х рр. Проте визначальним у межах Ради Європи став 2001 р., протягом якого було прийнято Європейську конвенцію про правовий захист послуг, що надаються на основі обумовленого доступу або які полягають у наданні обумовленого доступу від 24 січня 2001 р., що визначила кримінальну, адміністративну та іншу відповідальність винних осіб за несанкціонований доступ до захищених послуг та Конвенцію про кіберзлочинність від 23 листопада 2001 р. Відповідно до положень Конвенції про кіберзлочинність на держави покладається обов'язок вживати законодавчі й інші заходи, необхідні для встановлення кримінальної відповідальності відповідно до внутрішнього законодавства. Злочини в 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 р. до цього переліку було додано п'яту групу правопорушень – правопорушення, пов'язані з діями расистського та ксенофобського характеру, вчинених через комп'ютерні системи [12].

Ще одним важливим документом у межах Ради Європи стала Декларація Комітету міністрів про принципи управління Інтернетом від 21 вересня 2011 р. Ця декларація визначила намір держав-членів дотримуватися викладених принципів управління Інтернетом та використовувати їх як основи для розробки національної й міжнародної політики. До таких принципів увійшли права людини, демократія та верховенство закону; багатостороннє

управління; відповідальність держав; розширення прав і можливостей інтернет-користувачів; універсальність Інтернету; цілісність Інтернету; децентралізоване управління; архітектурні принципи; відкрита мережа; культурне й мовне різноманіття.

Також Радою Європи було прийнято Стратегію з управління Інтернетом на 2012-2015 рр. Цей правовий інструмент покликаний сприяти урядам, приватному сектору та громадянському суспільству в захисті та повазі прав людини, принципів верховенства закону й демократії в Інтернеті. Цією стратегією було визначено основні цілі Ради Європи в мережі Інтернет на чотири роки. До них віднесено, зокрема, такі: захист універсальності, цілісності та відкритості Інтернету; максимальне розширення прав користувачів Інтернету; захист персональних даних та приватного життя; взаємодія в боротьбі з кіберзлочинністю; захист та розширення прав дітей та молоді; максимізація потенціалу Інтернету для розвитку демократії.

Таким чином, проаналізувавши основні нормативні документи Організації Об'єднаних Націй, Міжнародного Союзу Електрозв'язку, Ради Європи, Європейського Союзу, Організації Північноатлантичного Договору та Шанхайської Організації Співробітництва у сфері визначення та забезпечення міжнародної інформаційної безпеки, можна стверджувати, що наразі не існує єдиного підходу до термінології та понятійного апарату в цій сфері та єдиного підходу до розуміння самого поняття міжнародної інформаційної безпеки. Тому кожна міжнародна організація спрямовує власні сили на врегулювання лише окремих аспектів міжнародної інформаційної безпеки: кримінального, технічного, терористичного.

ЛІТЕРАТУРА

1. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности : Резолюция Генеральной Ассамблеи ООН A/RES/69/28 [Електронний ресурс]. – Режим доступу : http ://www.un.org/ru/documents/ods.asp?m=A/RES/69/28.
2. Доклад группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности A/68/98 [Електронний ресурс]. – Режим доступу : http ://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF
3. Резолюція МСЕ 130/2006 [Електронний ресурс]. – Режим доступу : http ://www.itu.int/osg/spu/cybersecurity/ituevents.html.
4. Глобальна програма кібербезпеки МСЕ [Електронний ресурс]. – Режим доступу : http ://www.ifap.ru/pr/2008/080908aa.pdf.
5. Герке М. Понимание киберпреступности : руководство для развивающихся стран [Електронний ресурс] / М. Герке. – Режим доступу : www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.
6. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon 19–20 November 2010 [Electronic resource]. – Access mode : http ://www.nato.int/cps/uk/natohq/official_texts_68580.htm?selectedLocale.
7. The Tallinn Manual on the International Law Applicable to Cyber Warfare [Electronic resource]. – Access mode : https ://ccdcoe.org/249.html.
8. Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 р. [Електронний ресурс]. – Режим доступу : http ://base.spinform.ru/show_doc.fwx?rgn=28340
9. Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединённых Наций от 12 сентября 2011 г. на имя

Генерального секретаря ООН [Електронний ресурс]. – Режим доступу : http ://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF.

10. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector // Official Journal. – 1998. – L. 24. – P. 1.

11. Decision 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks // Official Journal. – 1999. – L. 12. – P. 11.

12. Європейська конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу : http ://zakon2.rada.gov.ua/laws/show/994_575/page.

REFERENCES

1. UNGA Resolution A/RES/69/28 “Developments in the field of information and telecommunications in the context of international security” [Electronic resource]. – Access mode : http ://www.un.org/ru/documents/ods.asp?m=A/RES/69/28..

2. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of international security A/68/98 [Electronic resource]. – Access mode : http ://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF .

3. ITU Resolution 130/2006 [Electronic resource]. – Access mode : http ://www.itu.int/osg/spu/cybersecurity/ituevents.html.

4. ITU Global Cybersecurity Agenda [Electronic resource]. – Access mode : http ://www.ifap.ru/pr/2008/080908aa.pdf.

5. Gerke M. “Understanding Cybercrime : A Guide for Developing Countries” [Electronic resource] / M. Gerke. – Access mode : www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

6. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon 19-20 November 2010 [Electronic resource]. – Access mode : http ://www.nato.int/cps/uk/natohq/official_texts_68580.htm?selectedLocale.

7. The Tallinn Manual on the International Law Applicable to Cyber Warfare [Electronic resource]. – Access mode : https ://ccdcoe.org/249.html.

8. Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security of June 16, 2009 [Electronic resource]. – Access mode : http ://base.spinform.ru/show_doc.fwx?rgn=28340.

9. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the UN Secretary General [Electronic resource]. – Access mode : http ://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF.

10. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector // Official Journal. – 1998. – L 24. – P. 1.

11. Decision 276/1999 / EC of the European Parliament and of the Council of 25 January 1999 adopting multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks // Official Journal. – 1999. – L 12. – P. 11.

13. European Convention on Cybercrime [Electronic resource]. – Access mode : http ://zakon2.rada.gov.ua/laws/show/994_575/page.

УДК 347.77 (477)

ПРАВОВЕ РЕГУЛЮВАННЯ ІНТЕЛЕКТУАЛЬНИХ РЕСУРСІВ В УКРАЇНІ

Мандзюк О.А., голова

Інститут стратегічних ініціатив Глобальної організації союзницького лідерства
вул. Жилянська 43, м. Київ, Україна
mandzyk@ukr.net

У роботі досліджене правове регулювання інтелектуальних ресурсів в Україні. Досліджено роль і місце правового регулювання в реалізації пріоритетних напрямів державної політики України з розвитку інтелектуальних ресурсів. Визначено основні напрями вдосконалення правового регулювання інтелектуальних ресурсів в Україні, серед яких окрему увагу приділено таким: удосконаленню правового регулювання формування правової політики держави щодо інтелектуальних ресурсів і напрямів реалізації такої політики; удосконаленню правового регулювання інтеграції наукових та освітніх ресурсів в умовах побудови інноваційної економіки; удосконаленню правового регулювання системи наукового й технологічного прогнозування; удосконаленню правового регулювання відповідальності у сфері інтелектуальних ресурсів. Визначено перспективні напрями розвитку положень цього дослідження, якими слід вважати проведення аналізу ролі інтелектуальних спільнот у державотворчому процесі.

Ключові слова: державна політика, правове регулювання, інтелектуальний ресурс, інновації, науково-освітній потенціал.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ РЕСУРСОВ В УКРАИНЕ

Мандзюк О.А.

Институт стратегических инициатив Всемирной организации союзнического лидерства
ул. Жилянская 43, г. Киев, Украина
mandzyk@ukr.net

В работе исследовано правовое регулирование интеллектуальных ресурсов в Украине. Рассмотрены роль и место правового регулирования в реализации приоритетных направлений государственной политики Украины по развитию интеллектуальных ресурсов. Определены основные направления совершенствования правового регулирования интеллектуальных ресурсов в Украине, среди которых особое внимание уделено следующим: совершенствованию правового регулирования формирования правовой политики государства в отношении интеллектуальных ресурсов и направлений реализации такой политики; совершенствованию правового регулирования интеграции научных и образовательных ресурсов в условиях построения инновационной экономики; совершенствованию правового регулирования системы научного и технологического прогнозирования; совершенствованию правового регулирования ответственности в сфере интеллектуальных ресурсов. Определены перспективные направления развития положений этого исследования, которыми следует считать проведение анализа роли интеллектуальных сообществ в государственном процессе.

Ключевые слова: государственная политика, правовое регулирование, интеллектуальный ресурс, инновации, научно-образовательный потенциал.

LEGAL REGULATION OF INTELLECTUAL ASSETS IN UKRAINE

Mandziuk O.A.

Institute of strategic initiatives Global organization of allied leadership, str. Zhylyanska, 43, Kyiv, Ukraine
mandzyk@ukr.net

The article examines the regulation of intellectual resources in Ukraine. The role and place of legal regulation in the implementation of the priorities of Ukraine’s state policy on development of intellectual