

ПРОБЛЕМАТИКА ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ В СУЧАСНІЙ СВІТОВІЙ ПОЛІТИЦІ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

НОВИЦЬКИЙ Віталій Ярославович - науковий співробітник, Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

<https://orcid.org/0000-0001-7386-1221>

УДК 342.6:342.922(477)

DOI 10.32782/EP.2021.2.14

У статті визначено проблематику міжнародно-правового аспекту правового регулювання інформаційної та кібернетичної безпеки. У статті ми обстоюємо точку зору, що тріаду інформаційної та кібернетичної безпеки можна представити наступним чином: безпека держави, безпека суспільства, безпека особи. При цьому безпека особи, суспільства та держави може гарантуватися як на національному, регіональному, так і міжнародному рівні, як і будь-який інший рівень, рівень міжнародного регулювання містить проблематику. Обрання як предмет дослідження саме міжнародний аспект пов'язано із транскордонністю інформаційних відносин і неможливістю виняткового національного регулювання. Така транскордонність суспільних відносин у сфері гарантування інформаційної та кібернетичної безпеки є однією із проблемних аспектів, оскільки видається вкрай складним створення єдиних нормативних актів, до яких зможуть приєднатися всі або більшість країн. Проблематика правового регулювання кібербезпеки в сучасній світовій політиці пов'язана із динамічністю цієї сфери міжнародного права, яка характеризується постійним і бурхливим розвитком, а також відсутністю досвіду комплексного правового регулювання багаторівневих транснаціональних відносин в Інтернеті. Також проблема полягає у відсутності консенсусу на міждер-

жавному рівні, у глобальному характері, багаторівневій і багатосторонній участі у формуванні правового регулювання відносин в Інтернеті. Проблематикою правового регулювання кібербезпеки є також факт відсутності міжнародно-правових договорів між багатьма країнами-учасницями щодо врегулювання зазначеної сфери суспільних відносин.

У статті ми виділили декілька нормативних актів у сфері правового регулювання гарантування інформаційної та кібернетичної безпеки: Конвенція про інформаційне та правове співробітництво стосовно Інформаційних суспільних послуг, Конвенція про кіберзлочинність та Додатковий протокол до Конвенції, Резолюція Ради ООН з прав людини в Інтернеті, Декларація про принципи управління Інтернетом, Політична декларація і Резолюція «Свобода Інтернету», Резолюції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки», «Боротьба із злочинним використанням інформаційних технологій», «Посилення програм ООН із запобігання злочинності та кримінального судочинства, зокрема їх технічної спроможності» тощо.

Ключові слова: інформаційна безпека, кібернетична безпека, міжнародно-правове регулювання, кіберзлочин, інформаційно-комунікаційні засоби і технології, Рада Європи, Організація Об'єднаних Націй.

Вступ

Невпинний розвиток науково-технічного прогресу впливає на форми взаємодії між людьми. Наразі безспірним є твердження, що основою формою спілкування стало невербальне віддалене спілкування за допомогою передачі інформації технічними засобами. За таких умов особливого значення набуває гарантування інформаційної та кібернетичної безпеки.

Актуальність обраної теми обумовлена постійними процесами глобалізації. Відбуваються постійні процеси зближення інформаційних систем окремих країн і формування на їх основі єдиного інформаційного простору, впровадження інформаційних технологій у всі сфери життя особи. Глобальний процес інформатизації охопив усі сучасні країни світу, тому гарантування інформаційної безпеки особи стає одним із найважливіших напрямків державної політики. Адже цілком правильним буде твердження, що сьогодні людини без інформації не існує. Тому гарантування інформаційної безпеки кожної особи має стати невід'ємною частиною інформатизації світу в цілому. За таких умов особливого наукового значення набуває дослідження міжнародно-правового аспекту правового регулювання інформаційної та кібербезпеки.

Аналіз останніх досліджень і публікацій

Слід зауважити, що існують численні публікації щодо дослідження правових питань гарантування інформаційної безпеки особи в Україні. Що стосується міжнародно-правового аспекту правового регулювання інформаційної та кібербезпеки, варто зазначити, що вказана тематика недостатньо досліджена в сучасній правовій науці. Так, К.С. Шахбазян здійснив дослідження міжнародно-правових основ регулювання відносин у мережі Інтернет [1]. І.М. Забара аналізував різні аспекти означеної проблематики: правове регулювання міждержавного обміну інформацією, правове регулювання обміну інформацією в діяльності міжнародних організацій системи ООН тощо [2; 3; 4; 5]. А.В. Пазюк у дисертаційній роботі дослідив теоретичні і практичні аспекти міжнародно-правового

регулювання інформаційної сфери [6]. З.О. Кукіна присвятила своє дослідження правовим стандартам і практиці регулювання діяльності засобів масової інформації в міжнародному праві [7]. Окремими аспектами міжнародного співробітництва України у сфері кібербезпеки займається Т. Станіславський [8]. А.Ю. Нашинець-Наумова присвятила свою роботу питанням правового регулювання інформаційної безпеки [9]. Різними питаннями у сфері гарантування інформаційної безпеки займається Б.А. Кормич, який присвятив дослідженню організаційно-правових основ політики інформаційної безпеки України свою докторську дисертацію [10]. Вказані праці мають велике наукове та практичне значення, однак зміни в суспільстві, настання епохи інформаційного суспільства потребують нового наукового пошуку.

Метою статті є визначення проблематики міжнародно-правового аспекту правового регулювання інформаційної та кібербезпеки.

Виклад основного матеріалу

Тріаду інформаційної та кібернетичної безпеки можна представити наступним чином: безпека держави, безпека суспільства, безпека особи. При цьому безпека особи, суспільства та держави може забезпечуватися як на національному, регіональному, так і міжнародному рівні. Нас цікавить питання гарантування інформаційної та кібернетичної безпеки на міжнародному рівні, зокрема, правові аспекти їх забезпечення. Такий інтерес обумовлений конституційним положенням про те, що «чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України» [11]. Таким чином, в Україні забезпечується верховенство міжнародного регулювання суспільних відносин. Враховуючи територіальне місце розташування України, науковий інтерес становить дослідження гарантування інформаційної та кібернетичної безпеки в рамках європейського простору. Також обрання саме міжнародного аспекту пов'язано із транскордонністю інформацій-

них відносин і неможливістю суто національного регулювання.

Україна бере активну участь у діяльності Ради Європи, а діяльність Ради Європи має значний вплив на українську політику. Так, у 2001 р. була прийнята Конвенція про інформаційне та правове співробітництво стосовно Інформаційних суспільних послуг», яка має за мету створення юридичної інформаційної системи співробітництва у сфері нових комунікаційних служб шляхом поширення застосування Директиви 98/48/ЕС за межами Європейського Союзу [12]. Це дозволило Раді Європи виконувати функцію координаційного центру з розробки законодавства у сфері «інформаційних суспільних послуг» на загальноєвропейському рівні.

У цілях покращення міжнародного співробітництва з питань боротьби із злочинами у сфері Інформаційно-комунікаційних засобів і технологій Рада Європи у 2001 р. у Будапешті приймає Конвенцію про кіберзлочинність. У ній приділяється увага чотирьом видам злочинів, що вчиняються у кіберпросторі та з використанням Інформаційно-комунікаційних засобів і технологій: правопорушенням проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушенням, пов'язаним з комп'ютерами; правопорушенням, пов'язаним зі змістом; правопорушенням, пов'язаним з порушенням авторських та суміжних прав.

Конвенція про кіберзлочинність є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва [13].

Додатковий протокол до Конвенції (Страсбург, 2003) розширює перелік кіберзлочинів за рахунок таких протиправних діянь: поширення расистського та ксенофобного матеріалу через комп'ютерні системи, погроза та образа з расистських та ксенофобних мотивів через комп'ютерну систему. Також криміналізуються: розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до матеріалу, який заперечує, значно мінімізує, схвалює або виправдовує дії, які є геноцидом або злочинами проти людства відповідно до міжнародного права. Конвенція передбачає надання повноважень, достатніх для ефективної боротьби із зазначеними кримінальними правопорушеннями, шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню на внутрішньодержавному і на міжнародному рівнях, укладення домовленостей щодо швидкого і надійного міжнародного співробітництва.

Як зазначають учені, окрім європейських нормативних актів, до міжнародно-правового гарантування інформаційної та кібернетичної безпеки, можна з упевненістю віднести всі універсальні принципи міжнародного права: принцип вирішення міжнародних спорів мирними засобами; принцип обов'язку держав співпрацювати одна з одною; принцип рівноправності і самовизначення народів; принцип суверенної рівності держав; принцип сумлінного виконання зобов'язань; принцип непорушності державних кордонів і територіальної цілісності держав; принцип поваги прав людини та основних свобод [6, с. 74-75]. Також у науці пропонується поширювати на міжнародно-правові інформаційні відносини дію ряду спеціальних принципів. До спеціальних принципів відносять: 1) право держав на здійснення чи санкціонування радіо і телевізійного трансграничного мовлення; 2) обов'язок держав запобігати або припиняти поширення ідей, засуджених світовою спільнотою; 3) обов'язок держав забезпечувати вільний доступ населення до джерел інформації; 4) право держав на протидію поширенню на своїй території ідей, які заборонені міжнародним співтовариством і несуть загрозу державній безпеці, громадському

порядку, здоров'ю та моралі населення тощо [14, с. 4–5]. Наведені наукові положення свідчать, що правове регулювання інформаційної та кібербезпеки на рівні міжнародного права здійснюється в рівній мірі як нормативними актами, там і виробленими наукою і практикою положеннями – принципами міжнародного інформаційного права.

Окремо слід зазначити, що розвиток міжнародно-правового регулювання гарантування інформаційної безпеки нерозривно пов'язаний із формуванням «нових» інформаційних прав людини, які доповнюють сучасну систему загально визнаних прав і свобод людини, тим самим розвиваючи міжнародне право захисту прав людини. Яскравим прикладом є право на захист персональних даних, яке традиційно сприймалося як елемент права на повагу до приватного життя, але набуло самостійного значення і визнання як фундаментальне інформаційне право людини в ході його інституційного розвитку.

Серед відносно «нових» прав людини в розвинених країнах світу отримало своє визнання право на доступ в Інтернет. Наприклад, парламент Естонії в законодавстві, прийнятому в 2000 р., проголосив доступ в Інтернет як право людини [15]. Конституційна рада Франції визнала доступ в Інтернет як фундаментальне право людини в 2009 р., а Конституційний суд Коста-Ріки дійшов такого ж висновку в 2010 р. [16].

Із поняттям «право на доступ в Інтернет» тісно пов'язані терміни кібербезпека та кіберпростір. У нормативних актах загальний доступ до кіберпростору визначається як рівноправний доступ для всіх людей за доступними цінами до інформаційної інфраструктури (зокрема, до Інтернету), до інформації та знань, необхідних для розвитку суспільства та особистості [17].

У 2012 р. Рада ООН з прав людини вперше ухвалила резолюцію, присвячену правам людини в Інтернеті, у якій: «... 2. Визнає глобальний і відкритий характер Інтернету, який є однією з рушійних сил прискорення прогресу по шляху розвитку в його різних формах» [18]. У Резолюції з аналогічною назвою у 2014 р. цей підхід був підтверджений ще раз [19].

Розгляд кібербезпеки саме у міжнародному плані пов'язаний із такою властивістю кіберпростору, як транснаціональність. Така властивість ускладнює регулювання кіберпростору і забезпечення кібербезпеки. Йдеться про розширення сучасної сфери міжнародно-правового регулювання, поширення її на відносини в глобальному інформаційному суспільстві та його віртуальне віддзеркалення – кіберпростір.

Із термінами кібербезпека та кіберпростір тісно пов'язане поняття кіберправо. Наразі кіберправо – уособлена галузь права, що постійно розвивається та формується у самостійну групу суспільних відносин. Кіберправо може бути як підгалуззю міжнародного права, так і самостійною внутрішньодержавною галуззю.

Якщо говорити, наприклад, про таку галузь права, як цивільне право або кримінальний процес, то зрозуміло, що мова йде про національну галузь права. Якщо ж говорити про кіберправо та кібербезпеку, то слід вести мову про наднаціональний автономний правовий режим правового регулювання.

Проблематика правового регулювання кібербезпеки в сучасній світовій політиці пов'язана із динамічністю цієї сфери міжнародного права, яка характеризується постійним і бурхливим розвитком, а також відсутністю досвіду комплексного правового регулювання багаторівневих транснаціональних відносин в Інтернеті. Також проблема полягає у відсутності консенсусу на міждержавному рівні, у глобальному характері, багаторівневій і багатосторонній участі у формуванні правового регулювання відносин в Інтернеті.

Проблематикою правового регулювання кібербезпеки є також факт відсутності міжнародно-правових договорів щодо врегулювання зазначеної сфери суспільних відносин.

Що стосується врегулювання означеного аспекту на європейському рівні, слід зазначити наступні нормативні акти. Комітет Міністрів Ради Європи у вересні 2011 р. затвердив Декларацію про принципи управління Інтернетом. У цьому документі сформульовано десять принципів управління

Інтернетом та наголошується, що «Інтернет забезпечує простір свободи шляхом сприяння реалізації та користуванню основоположними правами, активній участі та демократичним процесам, соціальній та комерційній діяльності» [20].

Також слід зазначити Політичну декларацію і Резолюцію «Свобода Інтернету», які ухвалені на Конференції міністрів, відповідальних за медіа та інформаційне суспільство, під егідою Ради Європи у Белграді 2013 р. У них проголошується тверде прагнення до свободи Інтернету, під якою розуміється «спільна відповідальність», що включає «забезпечення відкритої архітектури Інтернету, підтриманої та посиленої відкритими стандартами, процесами розвитку, та просування інновацій у висхідний децентралізований багатосторонній спосіб, що довів свою успішність для швидкої еволюції та поширення доступу до Інтернету, його відповідних технологій та пристосувань» [21].

Наведені нормативні акти регулюють окремі аспекти піднятої тематики. Кожен із них регулює окрему самостійну групу суспільних відносин. Така розрізненість нормативного регулювання становить собою окрему проблематику визначеної тематики. Також слід зазначити про відсутність спеціальних універсальних міжнародно-правових норм, спрямованих на впорядкування відносин у кіберпросторі, невизначеність стосовно практики держав у кіберпросторі, а також проблемність у визначенні дії міжнародних звичаїв для суб'єктів міжнародного права за аналогією з іншими міжнародно-правовими режимами, вимагають розробки міжнародно-правових інформаційних норм та принципів.

Окремо слід звернути увагу, що Організація Об'єднаних Націй відіграє провідну роль у розвитку діалогу між державами-членами з метою вироблення спільного розуміння безпеки в галузі використання Інформаційно-комунікаційних засобів і технологій.

У 2002 р. Генеральна Асамблея ООН ухвалила резолюцію «Створення глобальної культури кібербезпеки» [22], що потім доповнювалася за результатами Женевського (2003) та Туніського (2005) етапів Все-

світній саміт інформаційного суспільства і приймалася у нових редакціях у 2003 [23] та 2009 [24] роках. Резолюція 2002 р. передбачає дотримання всіма «учасниками» (державні органи, підприємства, інші організації та індивідуальних користувачів, які розробляють ці інформаційні системи і мережі, володіють, поставляють їх, управляють ними, обслуговують і використовують їх) правил, що охоплені в Додатку до резолюції за назвою «Елементи для створення глобальної культури кібербезпеки». Налічується дев'ять таких елементів, що мають забезпечити кібербезпеку: а) обізнаність; б) відповідальність; в) реагування; г) етика; д) демократія; е) оцінка ризику; ж) проектування та впровадження засобів гарантування безпеки; з) управління гарантування безпеки; и) перегляд.

Організація Об'єднаних Націй у сфері боротьби з кіберзлочинністю прийняла Резолюції Генеральної Асамблеї: «Боротьба із злочинним використанням інформаційних технологій», схвалені у 2000 [25] та 2001 роках [26]; «Посилення програм ООН із запобігання злочинності та кримінального судочинства, зокрема їх технічної спроможності» [27] тощо.

Висновки

У статті нами обстоюється точка зору, що триаду інформаційної та кібернетичної безпеки можна представити наступним чином: безпека держави, безпека суспільства, безпека особи. При цьому безпека особи, суспільства та держави може забезпечуватися як на національному, регіональному, так і міжнародному рівні. Як і будь-який інший рівень, рівень міжнародного регулювання містить проблематику. Обрання як предмет дослідження саме міжнародний аспект пов'язано із транскордонністю інформаційних відносин і неможливістю суто національного регулювання. Така траскордонність суспільних відносин у сфері гарантування інформаційної та кібернетичної безпеки є однією із проблемних аспектів, оскільки видається вкрай складним створення єдиних нормативних актів, до яких зможуть приєднатися всі або більшість країн. Проблема права правового регулювання кібербезпеки

в сучасній світовій політиці пов'язана із динамічністю цієї сфери міжнародного права, яка характеризується постійним і бурхливим розвитком, а також відсутністю досвіду комплексного правового регулювання багаторівневих транснаціональних відносин в Інтернеті. Також проблема полягає у відсутності консенсусу на міждержавному рівні, у глобальному характері, багаторівневій і багатосторонній участі у формуванні правового регулювання відносин в Інтернеті. Проблематикою правового регулювання кібербезпеки є також факт відсутності міжнародно-правових договорів між багатьма країнами-учасницями щодо врегулювання зазначеної сфери суспільних відносин.

У статті ми виділили декілька нормативних актів у сфері правового регулювання гарантування інформаційної та кібернетичної безпеки: Конвенція про інформаційне та правове співробітництво стосовно Інформаційних суспільних послуг, Конвенція про кіберзлочинність та Додатковий протокол до Конвенції, Резолюція Ради ООН з прав людини в Інтернеті, Декларація про принципи управління Інтернетом, Політична декларація і Резолюція «Свобода Інтернету», Резолюції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки», «Боротьба із злочинним використанням інформаційних технологій», «Посилення програм ООН із запобігання злочинності та кримінального судочинства, зокрема їх технічної спроможності» тощо.

Література

1. Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет: дис. ... канд. юрид. наук: 12.00.11; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2009. 219 с.
2. Забара І. М. Правове регулювання міждержавного обміну інформацією у багатосторонніх договорах. *Інформація і право*. 2013. № 1(7). С. 50–56.
3. Забара І. М. Міжнародно-правове регулювання обміну інформацією. *Інформація і право*. 2013. № 2(8). С. 56–62.
4. Забара І. М. Правове регулювання обміну інформацією в діяльності міжнародних

організаційсистеми ООН. *Український часопис міжнародного права*. 2012. №1. С. 113–120.

5. Забара І. М. Міжнародно-правове регулювання поширення інформації: теоретичні і практичні аспекти. *Форум права*. 2012. № 4. С. 362–366.

6. Пазюк А.В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти): дис. ... д.ю.н., Київ, 2016. 465 с.

7. Кукіна З. О. Правові стандарти і практика регулювання діяльності засобів масової інформації в міжнародному праві: автореф. дис ... канд. юрид. наук: 12.00.11; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2013. 18 с.

8. Станіславський Т. Розвиток міжнародного співробітництва України у сфері кібербезпеки. *Актуальні проблеми державного управління*. 2019. № 3. С. 58-67.

9. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

10. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис. ... док. юрид. наук: 12.00.07. Одеса, 2004. 427 с.

11. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

12. Convention on Information and Legal Co-operation concerning «Information Society Services», 2001, CETS № 180. URL: <http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?CL=ENG&CM=0&NT=180> (дата звернення 19.04.2021).

13. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 19.04.2021).

14. Ермичева Е. В. Международно-правовые аспекты деятельности средств массовой информации: дис. ... канд. юрид. наук: 12.00.10; Дипломат. акад. МИД Рос. Федерации. М., 2003. 177 с.

15. Woodard, C. Estonia, where being wired is a human right. Colin Woodard. *Christian Science Monitor*. URL: <http://www.csmonitor.com/2003/0701/p07s01-woeu.html> (дата звернення 19.04.2021).

16. Report of the Special Rapporteur on the promotion and protection of the right to free-

dom of opinion and expression, Frank La Rue, Human Rights Council Seventeenth session, 16 May 2011 URL: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (дата звернення 19.04.2021).

17. Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace / Records of the General Conference 32nd Session Paris, 29 September to 17 October 2003, Volume 1, Resolutions. URL: http://portal.unesco.org/en/ev.php-URL_ID=17717&URL_DO=DO_TOPIC&URL_SECTION=201.html (дата звернення 19.04.2021).

18. Resolution 20/8. The promotion, protection and enjoyment of human rights on the Internet, United Nations Human Rights Council, 5 July 2012. URL: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8 (дата звернення 19.04.2021).

19. Resolution 26/ The promotion, protection and enjoyment of human rights on the Internet, A/HRC/26/L.24, United Nations Human Rights Council, 20 June 2014 URL: <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G14/059/67/PDF/G1405967.pdf?OpenElement> (дата звернення 19.04.2021).

20. Declaration by the Committee of Ministers on Internet governance principles (adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies). URL: <https://wcd.coe.int/ViewDoc.jsp?id=1835773> (дата звернення 19.04.2021).

21. Resolution No. 1 Internet Freedom / Political Declarations and Resolutions [Freedom of Expression and Democracy in the Digital Age: Opportunities, rights, responsibilities], (Belgrade, 7–8 November 2013). URL: http://www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted_en.pdf (дата звернення 19.04.2021).

22. Resolution 57/239 Creation of a global culture of cybersecurity, UN GA, 2002. ITU: URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf (дата звернення 19.04.2021).

23. Resolution 58/199 Creation of a global culture of cybersecurity and the protection of critical information infrastructures, UN GA, 23

December 2003 URL: <http://onlinelibrary.wiley.com/doi/10.1002/9780470087923.hhs567/abstract/> (дата звернення 19.04.2021).

24. Resolution 64/211 Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, UN GA, 21 December 2009. URL: <http://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx> (дата звернення 19.04.2021).

25. Resolution 55/63 Combating the criminal misuse of information technologies, UN GA, 4 December 2000. URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (дата звернення 19.04.2021).

26. Resolution 56/121 Combating the criminal misuse of information technologies, UN GA, 19 December 2001. URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf (дата звернення 19.04.2021).

27. Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular, its technical cooperation Capacity: UN GA Resolutions 63/195 (18 December 2008), 64/179 (18 December 2009), and 65/232 (21 December 2011).

Novytskyi Vitalii, Researcher The Ukrainian scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine

LEGAL REGULATION OF INFORMATION AND CYBER SECURITY IN MODERN WORLD POLICY: INTERNATIONAL LEGAL ASPECT

The article identifies the issues of international legal aspect of legal regulation of information and cyber security. In the article we defend the view that the triad of information and cyber security can be represented as follows: security of the state, security of society, security of the person. At the same time, the security of the individual, society and the state can be ensured at the national, regional and international levels. Like any other level, the level of international regulation contains issues. The choice of the international aspect as a subject of research is connected with the cross-border information relations and the impossibility of exclusive national regulation. This cross-border nature of

public relations in the field of information and cyber security is one of the problematic aspects, as it seems extremely difficult to create uniform regulations to which all or most countries can join. The issue of legal regulation of cybersecurity in modern world politics is associated with the dynamism of this area of international law, which is characterized by constant and rapid development, as well as the lack of experience in comprehensive legal regulation of multilevel transnational relations on the Internet. Another problem is the lack of consensus at the interstate level, in the global nature, multilevel and multilateral participation in the formation of legal regulation of relations on the Internet. The problem of legal regulation of cybersecurity is also the fact that there are no international legal agreements between many member states to regulate this area of public relations.

In the article we have identified several regulations in the field of legal regulation of information and cyber security: Convention on Information and Legal Co-operation concern-

ing «Information Society Services», Convention on Cybercrime, Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace, Resolution 20/8 The promotion, protection and enjoyment of human rights on the Internet, United Nations Human Rights Council, Resolution 26/ The promotion, protection and enjoyment of human rights on the Internet, Declaration by the Committee of Ministers on Internet governance principles, Resolution No. 1 Internet Freedom / Political Declarations and Resolutions, Resolution 64/211 Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, Resolution 55/63 Combating the criminal misuse of information technologies, Resolution 56/121 Combating the criminal misuse of information technologies, etc.

Keywords: information security, cyber security, international legal regulation, cybercrime, information and communication means and technologies, Council of Europe, United Nations.