УДК 341.45:004

Калмикова Олександра Сергіївна –
кандидат юридичних наук,
асистент кафедри міжнародного права
Національного юридичного університету
імені Ярослава Мудрого

Alexandra S . Kalmykova –
candidate of juridical sciences,
assistant of department of international law
Yaroslav Mudryi National Law University
(77 Pushkinska str., Kharkiv, Ukraine)

Волчкова Майя Ігорівна –
студентка 3 курсу 5 групи
факультету адвокатури
Національного юридичного університету
імені Ярослава Мудрого

Maya I. Vochkova –
3rd year Bachelor's student of
Barristers' Faculty,
Yaroslav Mudriy National Law University
(77 Pushkinska str., Kharkiv, Ukraine)

Міжнародна співпраця у сфері боротьби з кіберзлочинністю

У статті автори продемонстрували переконливе розуміння того факту, що питання боротьби з кіберзлочинністю на даний час у світі постало дуже гостро і це є актуальною проблемою для більшості країн. Досліджено проблемні питання здійснення міжнародного співробітництва у боротьбі з кіберзлочинністю, досліджено міжнародно-правові та організаційні форми даної співпраці. Авторами наголошено на необхідності врегулювання українського законодавства відповідно до норм міжнародного права.

Ключові слова: *кіберзлочин, кіберзлочинність, міжнародне кримінальне право, уніфікація міжнародно-правових норм.*

В статье авторы продемонстрировали убедительное понимание того факта, что вопрос борьбы с киберпреступностью в настоящее время в мире является актуальной проблемой для большинства стран. Исследовано проблемные вопросы осуществления международного сотрудничества в борьбе с киберпреступностью, исследованы международно-правовые и организационные формы данного сотрудничества. Авторами отмечена необходимость урегулирования украинского законодательства в соответствии с нормами международного права.

Ключевые слова:*, киберпреступление, киберпреступность, международное уголовное право, унификация международно-правовых норм.*

A.S. Kalmykova, M.I. Vochkova International Cooperation in the Field of Combating Cybercrime

In the article, the authors demonstrated a compelling understanding of the fact that the issue of combating cybercrime is now very acute in the world and is a pressing problem for most countries. The authors analyze the historical origins of solving this problem in international law. Problems of international cooperation in the fight against cybercrime are investigated, international legal and organizational forms of this cooperation are investigated. The following international legal acts are analyzed: the Geneva Declaration of Principles, the

Convention on Information Technology Crime of the Council of Europe Cybercrime League, the CIS Commonwealth Cooperation Agreement on Crime and Crime in the Sphere of Crime. The definition of "cybercrime" is given, which follows from the analysis of the above acts, although no definition of "cybercrime" is enshrined in any universal international legal act. In addition to the main international legal acts regulating the fight against cybercrime, the rules of soft law are also analyzed. The problems of regulation in the Ukrainian legislation on combating cybercrime are reflected, one of them is that the authorities and divisions, which are entrusted with the duties to combat cybercrime, are deprived of the opportunity to promptly and timely process the requests of law enforcement authorities of other countries to collect evidence the location of suspects under the Cybercrime Convention. The authors agree with VF Antipenko's opinion, whose work has also been analyzed, that the criminalization of activities in the international sphere does not correspond to the realities of the present and requires significant corrections. In particular, this discrepancy can be observed in the field of high technology.

The authors emphasized the need to regulate the current Ukrainian legislation in accordance with the rules of international law.

Keywords: *cybercrime, cybercrime, international criminal law, unification of international legal norms.*

Постановка проблеми. Розвиток та ускладнення суспільних відносин, посилення транскордонної злочинності, а також досягнення у сфері технологій спричинили появу такого явища, як кіберзлочинність. Тривалий час ця сфера практично не була врегульована міжнародним правом, але на сьогоднішній день вироблено ряд норм, що мають за мету боротьбу з високотехнологічною злочинністю. Однак, наявне міжнародно-правове поле не достатньо ефективне, оскільки відсутня єдність та одноманітність правового регулювання зазначеної сфери. Це проявляється, перш за все, в застосуванні різної термінології та категоріально-понятійного апарату. Таким чином, вироблення загального уніфікованого визначення поняття «кіберзлочинність» – перший крок на шляху до кримінально-правової боротьби із нею.

В силу специфічної природи цього виду злочинів, внутрішнє законодавство про боротьбу з ними має прийматись відповідно до спеціальних міжнародних документів, оскільки ефективна протидія кіберзлочинності в межах однієї держави, без міжнародного співробітництва, в даний час не можлива [1, с. 8]. Проте, в умовах відсутності загальновизнаного на міжнародному рівні понятійно-категоріального апарату у зазначеній сфері національне правове поле може включати або «мертві» законодавчі норми, або такі, що неможливо використати на практиці, що ще раз підкреслює актуальність та необхідність вироблення єдиних міжнародно-правових стандартів.

Аналіз останніх досліджень і публікацій. Вивченням питання врегулювання міжнародних відносин у сфері боротьби з кіберзлочинністю займалися і розглядали в своїх роботах багато вчених, зокрема: О. Є. Користін, В. М. Бутузов, В.В. Василевич, В. Ф. Антипенко, О. О. Йона, Д. В. Швець, Є. С. Дурнов, О.В Махницький, О.О. Косиченко та інші.

Невирішені раніше проблеми. На сьогодні з’явилася необхідність в більш комплексній регламентації в чинне українське законодавство норм міжнародного права щодо боротьби з кіберзлочинністю. Тому, необхідно терміново підготувати і внести зміни до чинного законодавства щодо виконання зобов’язань України, узятих у зв’язку з ратифікацією «Конвенції про кіберзлочинність».

Метою статті є комплексний аналіз форм міжнародної співпраці у сфері боротьби з кіберзлочинністю. Дослідити та узагальнити поняття кіберзлочинності.

Виклад основного матеріалу. Дослідження та узагальнення поняття «кіберзлочин» є важливим кроком на шляху до формування концепції «кіберзлочинності» у міжнародному праві, створення загальних підходів до криміналізації такого роду протиправних діянь. У той же час, уніфікація міжнародно-правових норм у сфері боротьби із кіберзлочинністю є засобом розвитку галузі міжнародного кримінального права, а також об’єктивним процесом в рамках загальної уніфікації міжнародного права, зумовленої глобалізацією. Можна прослідкувати взаємозв’язок глобалізації, кіберзлочинності та

уніфікації міжнародно-правових норм. З однієї сторони, глобалізація, як характерна риса сучасного етапу розвитку суспільних відносин, призводить до виникнення та посилення транскордонної злочинності, а за рахунок технологічних досягнень – кіберзлочинності. З іншої сторони, наслідком глобалізації є уніфікація норм міжнародного права. Таким чином, уніфікація міжнародного права у сфері боротьби із кіберзлочинністю цілком об'єктивний, обумовлений вимогами сучасності процес, першим етапом якого повинна стати уніфікація відповідної термінології.

Разом із тим, не можливо не погодитись з думкою В. Ф. Антипенка, щодо того, що криміналізація діянь у міжнародній сфері не відповідає реаліям сучасності та потребує суттєвих коректив. Зокрема, таку невідповідність можна спостерігати і у сфері високих технологій. Міжнародне нормотворення повинно вчасно реагувати на виклики сучасності, в тому числі на зародження тенденцій до виникнення нових асиметричних джерел сили, серед яких і кібернетичні можливості впливу [2, с. 10] .

Міжнародне співтовариство неодноразово висловлювало занепокоєння тим, що новітні технології потенційно можуть використовуватися в цілях, несумісних із завданнями щодо забезпечення міжнародної стабільності та безпеки, і в змозі негативно впливати на цілісність інфраструктури держав, порушуючи їх безпеку як в цивільній, так і у військовій сферах. Генеральна Асамблея ООН також проголосила за необхідне запобігти використанню інформаційних ресурсів чи технологій в злочинних або терористичних цілях. (Резолюції ГА ООН 66/24 від 13.12.2011 [3], 67/27 від 11.12.2012 року [4]).

Женевська Декларація принципів «Побудова інформаційного суспільства: глобальна задача в новому тисячолітті», також підкреслюючи безмірний вплив інформаційних та комунікаційних технологій (далі – ІКТ) практично на всі аспекти нашого життя (А, п.8), визначила за необхідне формувати, розвивати і впроваджувати глобальну культуру кібербезпеки у співробітництві з усіма зацікавленими сторонами і компетентними міжнародними органами [5]. У рамках цієї глобальної культури важливо підвищувати безпеку і забезпечувати захист даних і недоторканість приватного життя. Разом із цим, було висловлено підтримку діяльності Організації Об'єднаних Націй, та підкреслено необхідність запобігати використанню інформаційних ресурсів і застосуванню інформаційних технологій у злочинних і терористичних цілях, дотримуючись при цьому прав людини [5]. У Женевській Декларації принципів прямо не застосовано термін «кіберзлочинність», однак із наведених положень випливає, що боротьба із кіберзлочинністю є важливою складовою глобальної культури кібербезпеки.

Розвинувши положення Женевської декларації принципів «Побудова інформаційного суспільства: глобальна задача в новому тисячолітті», Женевський план дій «С5. Зміцнення довіри і безпеки при використанні ІКТ» передбачив зобов'язання для державних органів та приватного сектору попереджати, виявляти і реагувати на прояви кіберзлочинності і зловживання ІКТ шляхом розробки керівних принципів, які враховують неперервні зусилля у цій сфері; обдумування законодавства, що дає змогу ефективно розслідувати і переслідувати зловживання; сприяння ефективним зусиллям взаємодопомоги; посилення на міжнародному рівні інституційної підтримки запобіганню, виявленню і ліквідації наслідків таких інцидентів; а також заохочення освіти і підвищення рівня інформованості [6]. Необхідність стимулювання, розвитку та впровадження глобальної культури кібербезпеки, а також кримінального переслідування кіберзлочинності визначила і Туніська програма для інформаційного суспільства [7].

Водночас, у жодному універсальному міжнародно-правовому акті не закріплено визначення кіберзлочинності. Більш того, експерти, що входять до групи Усестороннього дослідження проблеми кіберзлочинності та відповідних заходів зі сторони держав-членів міжнародного співтовариства і приватного сектору відповідно до Резолюцій 65/230 і 67/189 Генеральної Асамблеї ООН (UNODOC/CCPCJ/EG.4/2013/2 23.01.2013), наголошують на відсутності необхідності формування такого єдиного узагальнюючого поняття. Зазначається, що: «Визначення діапазону спеціальних слідчих повноважень та можливостей в галузі міжнародного

співробітництва не потребує «пошуку широкого, штучного визначення концепції «кіберзлочинності»» [8].

Разом із тим, відповідно до положень названого документу правомірно говорити про поняття кіберзлочинності у вузькому та широкому значеннях. Так, у першому випадку кіберзлочинність пов'язується лише із «обмеженою кількістю діянь, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних даних чи систем» [8]. Саме ці діяння складають основу досліджуваного поняття. Якщо трактувати його у широкому2. значенні, то кіберзлочинність можна визначити, як: «сукупність діянь, які передбачають використання комп'ютера в цілях отримання особистої чи фінансової вигоди або вчинення особистої чи фінансової шкоди, включаючи форми злочинів, пов'язаних з використанням персональних даних та діяння пов'язані з інформацією, що зберігається в комп'ютері» [8]. Однак, незважаючи на те, що Усестороннє дослідження кіберзлочинності не є міжнародно-правовим договором, тобто немає відповідної юридичної сили, вважаємо, що положення, які в ньому містяться можуть лягти в основу єдиного уніфікованого визначення поняття «кіберзлочинності». 3.

За умов відсутності універсального міжнародно-правового акту в сфері боротьби із кіберзлочинністю важливим кроком у згаданій сфері міжнародно-правового регулювання стало прийняття регіональних договорів. Аналізуючи їх положення варто зазначити, що в них використовується різний понятійно-категоріальний апарат, так:

Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. містить термін «кіберзлочинність» (cybercrime), однак його дефініція відсутня. Фактично, у документі перелічені окремі види4. діянь, які логічно необхідно віднести до кіберзлочинності. Також в преамбулі визначається наступне: «Ця Конвенція 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…»; «… Конвенція має на меті доповнення цих конвенцій для підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину в електронній формі» [9]. Таким чином, логічно узагальнивши наведені положення можна стверджувати, що кіберзлочин – це кримінальне правопорушення в електронній формі, спрямоване проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними.

Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21.12.2010 р. застосовує термін «злочини у сфері інформаційних технологій» (information technology offences), визначення якого в тексті договору також відсутнє [10]. Водночас, виходячи із контексту ст. 2 можна стверджувати, що злочини у сфері інформаційних технологій – це злочини пов'язані з будь-якими матеріальними чи віртуальними засобами або групами засобів, що використовуються для зберігання, сортування, організації, отримання, обробки, розробки та обміну інформацією відповідно до команд та інструкцій.

Угода про співробітництво держав-членів Співдружності Незалежних Держав у боротьбі із злочинністю в сфері комп'ютерної інформації від 01.06.2001 р. визначає «злочин в сфері комп'ютерної інформації» (преступление в сфере компьютерной информации), як кримінально каране діяння, предметом посягання якого є комп'ютерна інформація, а саме така інформація, що знаходиться в пам'яті комп'ютера, на машинних чи інших носіях у формі, доступній сприйняттю ЕОМ (електронно-обчислювальна машина) чи передається по каналах зв'язку [11].

Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16.06.2009 р. (вступила в силу з 05.01.2012) містить термін «інформаційна злочинність», що тлумачиться як використання інформаційних ресурсів та (або) вплив на них в інформаційному просторі в протиправних цілях [12].

Окремої уваги потребують і норми soft law, що були вироблені міжнародним співтовариством з метою боротьби із високотехнологічною злочинністю.

Найважливішими із них, вважаємо: Висновки Організації економічного співробітництва та розвитку «Злочини пов'язані з комп'ютером: аналіз правової політики» 1985 р.; Рекомендацію № R89 (9) Комітету міністрів держав-членів Ради Європи про злочини, які пов'язані з комп'ютерами 1989 р.; Рекомендацію, прийняту на VIII Конгресі ООН з попередження злочинності та поводження з правопорушниками 1990 р.; Рекомендацію про керівні принципи забезпечення безпеки інформаційних систем 1992 р.; Довідник ООН із запобігання і контролю злочинності, пов'язаної з комп'ютерами 1995 р.; Десять принципів боротьби з високотехнологічними злочинами, прийняті на зустрічі міністрів внутрішніх справ та міністрів юстиції Великої Вісімки 1997 р.; План дій про боротьбу із злочинами, пов'язаними з використанням високих технологій та комп'ютерів Комісії з попередження злочинності та кримінального правосуддя 2001 р.

У зазначених джерелах на рівні із поняттям «кіберзлочинність» застосовуються такі поняття як «злочини пов'язані з комп'ютерами», «злочини, пов'язані з використанням комп'ютерних технологій», «високотехнологічні злочини». Норми, що містяться в джерелах soft law не мають обов'язкової юридичної сили, але повинні бути враховані при створенні універсальної концепції кіберзлочинності.

Кіберзлочинність є міжнародною проблемою, оскільки об'єкти її посягання знаходяться в кіберпросторі, який необмежений державними кордонами.

У протидію з цим негативним явищем міжнародного характеру залучені всі держави світу, незалежно від рівня їх технічного розвитку і національного законодавства. При цьому менш розвинені в технічному відношенні країни мають можливість використовувати досвід розвинених країн для запобігання і розслідування комп'ютерних злочинів.

З уведенням в дію нового Кримінально-процесуального кодексу України 19 листопада 2012 р. значно ускладнилася процедура отримання інформації від провайдерів телекомунікаційних послуг. Якщо раніше отримання такої інформації здійснювалося на підставі положень про «Конвенцію про кіберзлочинність» і Закону України «Про міліцію», то зараз така інформація віднесена до категорії документів, що містять комерційну таємницю, яка охороняється законом (Глава 46 Цивільного Кодексу України).

Таким чином, органи і підрозділи, на які покладені обов'язки по боротьбі з кіберзлочинністю, позбавлені можливості оперативно і своєчасно обробляти запити правоохоронних органів інших країн по збору доказів про кіберзлочини і встановлення місцезнаходження підозрюваних у рамках «Конвенції про кіберзлочинність».

З метою ефективної боротьби з кіберзлочинністю на національному і міжнародному рівнях, необхідно давати адекватну оцінку змінам процесуальних норм ведення розслідування і переслідування в судовому порядку, а також враховувати вимоги часу і потреби практики.

Сьогодні рівень і темпи зростання кіберзлочинності вимагають адекватного реагування, у тому числі і на законодавчому рівні. Тому, враховуючи вищевикладене, необхідно терміново підготувати і внести зміни до чинного законодавства про порядок і підстави виконання запитів, отриманих від правоохоронних органів країн у рамках виконання зобов'язань України, узятих у зв'язку з ратифікацією «Конвенції про кіберзлочинність».

Для ефективної протидії кіберзлочинності необхідний інтегрований підхід, який можна забезпечити лише колективними зусиллями міжнародної спільноти через тісну взаємодію державних інститутів.

Висновки. Підсумовуючи вищесказане, ми пропонуємо таке визначення: «кіберзлочинність - це незаконне кримінальне правопорушення, вчинене за допомогою комп'ютерних даних, комп'ютерів, їх систем та мереж».

В рамках та відповідно до універсальної концепції кіберзлочинності слід розробити концепцію стратегії реалізації державної політики боротьби з кіберзлочинністю в Україні. На сьогодні така стратегія ще не сформована. У кримінальному законі жоден із вивчених термінів відсутній, незважаючи на те, що глава XVI Кримінального кодексу присвячена протидії злочинам у використанні електронних комп'ютерів (комп'ютерів), систем та комп'ютерних мереж та телекомунікаційних мереж. Ми відзначаємо доцільність внесення

відповідних змін до законодавства України, включаючи застосування терміна "кіберзлочинність".

Список використаних джерел:

1. Користін О. Є., Бутузов В. М., Василевич В.В. Протидія кіберзлочинності в Україні: правові та організаційні /за заг. ред. В. В. Коваленка. Київ: Видавничий дім «Скіф», 2012.728 с.
2. Антипенко В. Ф. Проблеми ефективності міжнародного права. *Проблеми ефективності міжнародного права:* матеріали міжнародної науково-практичної конференції. Київ, 2013. С. 10-11.
3. Резолюция ГА ООН № 66/24 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности от 13.12.2011 р. URL: http://daccess-ddsny.un.org/doc/UNDOC/GEN/N11/460/28/PDF/N1146028 (дата звернення: 21.11.2019).
4. Резолюция ГА ООН № 67/27 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности от 11.12.2012 р. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N12/480/24/PDF/N1248024. (дата звернення: 21.11.2019).
5. Женевська Декларація принципів «Побудова інформаційного суспільства: глобальна задача в новому тисячолітті від 12.12.2003 р. URL: http://www.nkrz.gov.ua/uk/1324628380 /1337763264/1337766423(дата звернення: 21.11.2019).
6. Женевський план дій від 12.12.2003 р. URL: http://www.nkrz.gov.ua/uk/ 1324628380/1337763264/1337765310 (дата звернення: 23.11.2019).
7. Туніська програма для інформаційного суспільства від 18.11.2005 р. URL: http://www.nkrz.gov.ua/uk/1324628380/1337763264/1337767389/(дата звернення: 23.11.2019).
8. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора 23-28.02.2013. URL: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата звернення: 25.11.2019).
9. Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. URL: http://zakon4.rada.gov.ua/laws/show/994_575 (дата звернення: 25.11.2019).
10. Arab Convention on Combating Information Technology Offences 21.12.2010. URL: http://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd. (дата звернення: 25.11.2019).
11. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. URL: http://zakon4.rada.gov.ua/laws/show/997_353 (дата звернення: 28.11.2019).
12. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества О сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 г. URL: http://base.spinform.ru/show_doc.fwx?rgn=28340 (дата звернення: 28.11.2019).

References:

1. Korystin O. Ye., Butuzov V. M., Vasylevych V.V. Protydiia kiberzlochynnosti v Ukraini: pravovi ta orhanizatsiini /za zah. red. V. V. Kovalenka. Kyiv: Vydavnychyi dim “Skif”, 2012.728 s.
2. Antypenko V. F. Problemy efektyvnosti mizhnarodnoho prava. *Problemy efektyvnosti mizhnarodnoho prava*: materialy mizhnarodnoi naukovo-praktychnoi konferentsii. Kyiv, 2013. S. 10-11.
3. Rezoliutsyia HA OON № 66/24 Dostyzhenyia v sfere ynformatyzatsyy y telekommunykatsyi v kontekste mezhdunarodnoi bezopasnosty ot 13.12.2011 r. URL: http://daccess-ddsny.un.org/doc/UNDOC/GEN/N11/460/28/PDF/N1146028 (data zvernennia: 21.11.2019).
4. Rezoliutsyia HA OON № 67/27 Dostyzhenyia v sfere ynformatyzatsyy y telekommunykatsyi v kontekste mezhdunarodnoi bezopasnosty ot 11.12.2012 r. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N12/480/24/PDF/N1248024. (data zvernennia: 21.11.2019).

5. Zhenevska Deklaratsiia pryntsypiv “Pobudova informatsiinoho suspilstva: hlobalna zadacha v novomu tysiacholitti” vid 12.12.2003 r. URL: http://www.nkrz.gov.ua/uk/1324628380 /1337763264/1337766423(data zvernennia: 21.11.2019).

6. Zhenevskyi plan dii vid 12.12.2003 r. URL: http://www.nkrz.gov.ua/uk/ 1324628380/1337763264/1337765310 (data zvernennia: 23.11.2019).

7. Tuniska prohrama dlia informatsiinoho suspilstva vid 18.11.2005 r. URL: http://www.nkrz.gov.ua/uk/1324628380/1337763264/1337767389/(data zvernennia: 23.11.2019).

8. Vsestoronnee yssledovanye problemi kyberprestupnosty y otvetnikh mer so storoni hosudarstv-chlenov, mezhdunarodnoho soobshchestva y chastnoho sektora 23-28.02.2013. URL: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (data zvernennia: 25.11.2019).

9. Konventsiia Rady Yevropy pro kiberzlochynnist vid 21.11.2001 r. URL: http://zakon4.rada.gov.ua/laws/show/994_575 (data zvernennia: 25.11.2019).

10. Arab Convention on Combating Information Technology Offences 21.12.2010. URL: http://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd. (data zvernennia: 25.11.2019).

11. Sohlashenye o sotrudnychestve hosudarstv-uchastnykov Sodruzhestva Nezavysymikh Hosudarstv v borbe s prestuplenyiamy v sfere kompiuternoi ynformatsyy ot 01.06.2001 h. URL: http://zakon4.rada.gov.ua/laws/show/997_353 (data zvernennia: 28.11.2019).

12. Sohlashenye mezhdu pravytelstvamy hosudarstv-chlenov Shankhaiskoi orhanyzatsyy sotrudnychestva O sotrudnychestve v oblasty obespechenyia mezhdunarodnoi ynformatsyonnoi bezopasnosty ot 16.06.2009 h. URL: http://base.spinform.ru/show_doc.fwx?rgn=28340 (data zvernennia: 28.11.2019).