УДК: 341(045):004.056

ЗАБАРА І.М., *кандидат юридичних наук, доцент,*
кафедра міжнародного права Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

ІНСТИТУТ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРАВОВІ АСПЕКТИ

Анотація. *Стаття присвячена аналізу складових елементів інституту міжнародної інформаційної безпеки. Автор розглядає ключові аспекти, принципи і підходи з позицій міжнародного права.*

Ключові слова: *інформація, міжнародна інформаційна безпека, кіберзлочинність, інформаційно-комунікаційні технології, міжнародно-правове регулювання.*

Аннотация. *Статья посвящена анализу составных элементов института международной информационной безопасности. Автор рассматривает ключевые аспекты, принципы и подходы с позиций международного права.*

Ключевые слова: *информация, международная информационная безопасность, киберпреступность, информационно-коммуникационные технологии, международно-правовое регулирование.*

Summary. *The article analyzes the components of the international institute of information security. The author considers the key issues, principles, elements from the standpoint of international law.*

Keywords: *information, international information security, cybercrime, information and communication technology, international legal regulation.*

Постановка проблеми. В міжнародному праві проблема міжнародної інформаційної безпеки постала в якості самостійної наукової проблеми у дев’яностих роках XX сторіччя. Вона була викликана зростаючою кількістю проявів використання інформаційно-комунікаційних технологій в цілях, несумісних із задачами забезпечення міжнародної безпеки і стабільності в цивільній і військовій сферах.

Проблема використання інформаційно-комунікаційних технологій привернула до себе увагу і тим, що ці технології виявились здатними здійснювати негативний вплив як на цілісність державних інфраструктур, так і реалізацію основних прав і свобод людини.

Проблематика міжнародної інформаційної безпеки, як одного з ключових елементів системи міжнародної безпеки, є доволі широкою і для міжнародного права продовжує залишатись актуальною. Варто зазначити, що у перших доктринальних дослідженнях, пов’язаних із тематикою міжнародної інформаційної безпеки, превалювали питання, пов’язані із її кримінальною та військовою складовими. Це пояснюється тим, що на виокремлення саме цих питань в достатній мірі вплинули національні концепції інформаційної безпеки, прийняті в різних державах.

Однак, поява нових негативних проявів використання інформаційно-комунікаційних технологій посилила увагу до цієї теми як з практичної, так і з теоретичної точок зору. Окремі питання почали дедалі частіше розглядатися з позицій вирішення окремих проблем і у рамках міжнародних організацій.

Аналіз останніх досліджень і публікацій свідчить, що серед представників доктрини значна увага проблемам міжнародної інформаційної безпеки була приділена в роботах А. Балера, І. Бачило, Ю. Батурина, В. Василенка, А. Волеводз, А. Жодзішського,

С. Гормана, М. Грокса, М. Дюмонтьє, Р. Кларка, В. Кіютіна, Р. Кнейка, С. Комова, С. Короткова, А. Крутських, В. Машликіна, Т. Морера, А. Новікова, С. Расторгуєва, Д. Робинсона, А. Сегала, П. Сінгера, А. Смирнова, В. Сомерса, А. Стрельцова, В. Талімончик, А.Федорова, К. Форда та інших. Окремі аспекти інформаційної безпеки досліджували О. Баранов, Д. Біго, М. Герке, К. Гирс, В. Гавловський, Н. Ємельянова, І. Кванталіані, Б.Кормич, В. Фурашев та інші.

Серед розглянутих авторами були теоретичні питання щодо міжнародно-правових проблем інституту міжнародної інформаційної безпеки, питання співробітництва в рамках міжнародних організацій та окремих аспектів боротьби із кіберзлочинністю. Певною мірою були досліджені питання щодо ролі міжнародних організацій у формуванні норм інституту міжнародної інформаційної безпеки.

В той же час, одним з малодосліджених в науці міжнародного інформаційного права є саме поняття міжнародної інформаційної безпеки, її складових та концептуальних підходів. Ці питання епізодично розглядались у іноземній та вітчизняній доктрині міжнародного права. Між тим тема міжнародної інформаційної безпеки виступає в якості одного з напрямків міжнародного співробітництва, має достатній для аналізу обсяг правового матеріалу і викликає не тільки теоретичний, але й практичний інтерес.

Метою статті є визначення складу інституту міжнародної інформаційної безпеки у міжнародному праві.

Виклад основного матеріалу. При розгляді питання щодо складу інституту міжнародної інформаційної безпеки за критерій, на нашу думку, варто взяти відносини держав в інформаційній сфері, що підлягають регулюванню, оскільки поняття міжнародної інформаційної безпеки в міжнародно-правовій термінології не є усталеним. Причина полягає у відсутності єдиних методологічних засад, на базі яких можуть бути визначені сутність цього інституту, ступінь необхідності використання і межі застосування. На жаль, ці методологічні засади і до сьогодні не розроблено, що має виразний прояв не тільки в доктрині міжнародного права, але й у текстах міжнародно-правових документів, в тому числі низки міжнародних організацій. На нашу думку, складнощі із методологічними засадами викликані різними доктринальними поглядами як на тематику і проблематику, пов’язану із міжнародною інформаційною безпекою, так і на концептуальні шляхи вирішення окремих проблем.

Аналіз наукових досліджень та міжнародно-правових актів надає можливість стверджувати, що зазначені відносини держав в інформаційній сфері можна структурувати на підставі трьох складових.

Перша складова міждержавних відносин в інформаційній сфері полягає у необхідності забезпечення належного і стійкого балансу між правоохоронними інтересами і повагою до основних прав і свобод людини.

В доктрині до цієї складової відносять всі прояви використання інформаційно-комунікаційних технологій на шкоду основним правам і свободам людини, що реалізуються в інформаційній сфері.

Ці прояви можуть виражатися через використання інформаційної інфраструктури для здійснення неправомірного доступу до інформації; неправомірного поширення інформації; порушення конфіденційності, цілісності та доступності інформації, комп’ютерних даних і систем; протизаконного використання програм та баз даних, що є об’єктами авторського права; поширення інформації, що розпалює міжнаціональну, міжрасову та міжконфесійну ворожнечу, расистських та ксенофобських писемних матеріалів, зображень або будь-якої іншої демонстрації ідей або теорій, які пропагують, сприяють або підбурюють до ненависті, дискримінації, насильству проти будь-якої особи

або групи осіб, якщо в якості приводу до цього використовуються фактори, що ґрунтуються на расі, кольору шкіри, національному та етнічному походженні та релігії.

Цю складову в доктрині міжнародного права визначають в якості кримінального аспекту міжнародної інформаційної безпеки (відповідно і термінологія, яка використовується – “транскордонна комп’ютерна злочинність”, “кіберзлочинність”, “комп’ютерні злочини”, “високотехнологічні злочини”, “злочини у сфері комп’ютерної інформації”, “кіберзлочини”, “інформаційні злочини” тощо) [1 – 2].

Кримінальний аспект міжнародної інформаційної безпеки став одним з досліджених в доктрині і, як наслідок, знайшов відображення в кількох міжнародних угодах. В якості прикладу, вважаємо за необхідне звернути увагу на зобов’язання держав, пов’язані із боротьбою з кримінальними злочинами в інформаційній сфері. Так, *Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами у сфері комп’ютерної інформації* від 1 червня 2001 року [3] покладає на держави зобов’язання щодо визнання у відповідності з національним законодавством в якості кримінальних злочинів:

“а) здійснення неправомірного доступу до комп’ютерної інформації, що охороняється законом, якщо це потягло знищення, блокування, модифікацію або копіювання інформації, порушення роботи електронно-обчислювальних машин (далі – ЕОМ), систем ЕОМ або їхньої мережі;

б) створення, використання або поширення шкідливих програм;

в) порушення правил експлуатації ЕОМ, системи ЕОМ або їхньої мережі особою, що має доступ до ЕОМ, системи ЕОМ або їхньої мережі, що потягло знищення, блокування або модифікацію інформації ЕОМ, що охороняється законом, якщо це спричинило суттєву шкоду або тяжкі наслідки;

г) протизаконне використання програм для ЕОМ та баз даних, що є об’єктами авторського права, так само як і присвоєння авторства” (ст. 3) [3].

В свою чергу, положеннями *Конвенції про кіберзлочинність* від 23 листопада 2001 року [4] та *Додатковим протоколом до Конвенції про кіберзлочинність* від 28 січня 2003 року, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп’ютерні системи, що були прийняті в рамках Ради Європи, на держави покладаються зобов’язання щодо вживання законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності згідно до її внутрішнього законодавства за наступні, класифіковані за групами злочини:

перша група передбачає кримінальну відповідальність за вчинення правопорушень проти конфіденційності, цілісності та доступності комп’ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями) (ст. 2 – 6) [4];

друга група передбачає відповідальність за правопорушення, пов’язані з комп’ютерами (підробка, пов’язана з комп’ютерами; шахрайство, пов’язане з комп’ютерами) (ст. 7, 8) [4];

третя група містить правопорушення пов’язані зі змістом інформації (правопорушення, пов’язані з дитячою порнографією) (ст. 9) [4];

четверта група містить правопорушення, пов’язані із порушеннями авторських і суміжних прав (ст. 10) [4];

п’ята група містить правопорушення, пов’язані з діями расистського та ксенофобського характеру, вчинених через комп’ютерні системи (ст. 3 – 7 Додаткового протоколу) [4].

Шанхайська організація співробітництва (далі – ШОС) запропонувала дещо інший підхід. На відміну від попередніх *Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки* від 16 червня 2009 року [5] передбачає новий концептуальний підхід до питань забезпечення міжнародної інформаційної безпеки. Його суть полягає у комплексному забезпеченні міжнародної інформаційної безпеки держав від усіх інформаційних загроз, в тому числі і від кримінальних, що можуть бути спричинені злочинним використанням інформаційно-комунікаційних технологій. Виходячи з цих позицій, інформаційна злочинність визнана сторонами Угоди ШОС в якості основної загрози в області забезпечення міжнародної інформаційної безпеки.

Джерелом цієї загрози, відповідно до Угоди ШОС, є особи або організації, що здійснюють неправомірне використання інформаційних ресурсів або несанкціоноване втручання в такі ресурси у злочинних цілях.

Ознаками інформаційної злочинності є:

проникнення в інформаційні системи для порушення цілісності, доступності і конфіденційності інформації;

навмисне виготовлення і поширення комп’ютерних вірусів та інших шкідливих програм;

здійснення DOS-атак (відмова в обслуговуванні) та інших негативних впливів;

заподіяння шкоди інформаційним ресурсам;

порушення законних прав і свобод громадян в інформаційній сфері , в тому числі права інтелектуальної власності і недоторканності приватного життя;

використання інформаційних ресурсів і методів для скоєння таких злочинів як шахрайство, крадіжка, вимагання, контрабанда, незаконна торгівля наркотиками, поширення дитячої порнографії тощо.

З метою протидії інформаційній злочинності, сторони Угоди ШОС погодились співпрацювати і проводити свою діяльність у інформаційному просторі таким чином, щоб така діяльність сприяла соціальному і економічному розвитку і була сумісною з задачами підтримки міжнародної безпеки і стабільності, відповідала загальновизнаним принципам міжнародного права. Така діяльність повинна бути сумісною з правом кожної сторони Угоди ШОС шукати, отримувати і поширювати інформацію з урахуванням можливих обмежень з причин захисту інтересів національної та суспільної безпеки.

Міжнародне співробітництво, в цілях протидії правопорушенням в інформаційній сфері, передбачає прийняття державами законодавчих і організаційних заходів, а також проведення спільних дій в цілях запобігання правопорушенням в інформаційній сфері.

Законодавчі заходи полягають у встановленні кримінальної відповідальності осіб за соціально небезпечні діяння в інформаційній сфері та застосуванні відповідних заходів покарання. Організаційні заходи спрямовуються на протидію неправомірному використанню інформаційно-комунікаційних технологій (поширенню інформації, порушенню конфіденційності, цілісності і доступності інформації тощо).

До цього варто додати і запропонований новий концептуальний підхід, що привертає увагу. Так, проведення спільних дій, принаймні, як це передбачається *проектом універсальної Конвенції про забезпечення міжнародної інформаційної безпеки* 2011 року [6] передбачає, що держави забезпечать встановлення, виконання та застосування процедур з метою проведення кримінального розслідування та судового розгляду за фактами скоєння в інформаційному просторі соціально небезпечних діянь у відповідності з їх національним законодавством, що забезпечуватиме належний захист прав і свобод людини. На держави покладається обов’язок прийняття заходів щодо

встановлення юрисдикції щодо соціально небезпечних діянь в інформаційному просторі, що здійснюються на її території, на борту судна, літака та літального апарату, зареєстрованого відповідно до її законодавства (ст. 11) [6]. В разі виникнення питань щодо юрисдикції, держави використовуватимуть процедуру консультацій, з метою визначення найбільш відповідної юрисдикції для здійснення судового переслідування.

Друга складова міждержавних відносин в інформаційній сфері полягає у протидії використанню інформаційного простору у терористичних цілях [7].

В доктрині до цієї складової відносять всі прояви використання інформаційно-комунікаційних технологій державними і недержавними структурами, організаціями, групами і окремими особами в терористичних, екстремістських та інших злочинних діях (ст. 3) [6]. Прояви можуть виражатися через використання інформаційної інфраструктури для розміщення інформаційних ресурсів, що пропагують насильницькі дії з метою залякування, пригнічення та нав’язування певної лінії поведінки; поширення закликів до проведення екстремістських та терористичних актів (в тому числі і в інформаційному просторі); повідомлень про скоєні або заплановані акти (в тому числі і в інформаційно-комунікаційних мережах); руйнування даних, що призводить до порушень суспільного порядку; перешкоджання трансляції каналами масової інформації тощо.

Цю складову в доктрині міжнародного права визначають в якості терористичного аспекту міжнародної інформаційної безпеки (відповідно і термінологія яка використовується – “інформаційний тероризм”, “кібертероризм” [7] тощо). На відміну від попереднього кримінального аспекту, терористична діяльність в інформаційному просторі проводиться в політичних цілях.

Визначення інформаційного тероризму в якості загрози в області забезпечення міжнародної інформаційної безпеки здійснено в *Угоді між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки* від 16 червня 2009 року [5].

Джерелом цієї загрози, відповідно до її положень виступають терористичні організації та особи, які причетні до терористичної діяльності, що здійснюють протиправні дії шляхом або у відношенні інформаційних ресурсів (інформаційної інфраструктури, інформації та потоків інформації) (п. 2) [8]. Ознаками інформаційного тероризму, відповідно до положень цієї Угоди, є:

використання інформаційних мереж терористичними організаціями для здійснення терористичної діяльності і залучення до своїх лав нових послідовників;

деструктивний вплив на інформаційні ресурси, що призводять до порушень громадського порядку;

контролювання або блокування каналів передачі масової інформації;

використання мережі Інтернет або інших інформаційних мереж для пропаганди тероризму, створення атмосфери страху і паніки у суспільстві, а також інший негативний вплив на інформаційні ресурси (п. 2) [8].

Питання міжнародного співробітництва в цілях протидії використанню інформаційного простору в терористичних цілях досить вдало деталізуються положеннями *проекту універсальної Конвенції про забезпечення міжнародної інформаційної безпеки* 2011 року і передбачають проведення державами спільних дій та прийняття законодавчих і інших заходів.

Вони полягають у розробці єдиних підходів до припинення функціонування Інтернет-ресурсів терористичного характеру і спрямування; обміні інформацією щодо ознак, фактів, методів і засобів використання інформаційно-комунікаційних систем в терористичних цілях, а також спрямованості і діяльності терористичних організацій в

інформаційному просторі; обміні досвідом щодо моніторингу інформаційних ресурсів інформаційно-комунікативних мереж, пошуку та відстеженні змісту сайтів терористичного спрямування; проведенні спільних комп’ютерних криміналістичних експертиз (ст. 9) [6].

Держави, як це передбачається проектом, спрямовуватимуть свої зусилля на прийняття заходів законодавчого характеру з метою надання компетентним органам можливості проводити слідчі, розшукові та інші процесуальні заходи, спрямовані на попередження, припинення і ліквідацію наслідків проведення терористичних дій в інформаційному просторі, а також покарання винних осіб. Крім цього держави зможуть визначити у законодавстві заходи щодо гарантованого доступу на території держави до окремих частин інформаційно-комунікаційної інфраструктури, щодо яких є підстави вважати, що вони використовуються для діяльності терористичних актів або діяльності терористичних організацій, груп або окремих терористів (ст. 9) [6].

Варто зазначити, що терористичний аспект міжнародної інформаційної безпеки окремі представники доктрини іноді розглядають разом із кримінальним аспектом, що, на нашу думку, невиправдано призводить до їх ототожнення.

Третя складова міждержавних відносин в інформаційній сфері полягає у попередженні військових конфліктів з використанням інформаційно-комунікативних технологій, а також підготовки та ведення інформаційної війни.

В доктрині до цієї складової відносять всі прояви використання інформаційно-комунікаційних технологій для здійснення ворожих дій і актів агресії; цілеспрямованого деструктивного впливу в інформаційному просторі на критично важливі структури іншої держави; дії в інформаційному просторі з метою підриву політичної, економічної, соціальної систем іншої держави, поширення інформації, що дестабілізує суспільство; транскордонного поширення інформації, що суперечить принципам і нормам міжнародного права, а також національному законодавству держав; інформаційної експансії, отримання контролю над національними інформаційними ресурсами іншої держави (ст. 4) [6].

Цю складову в доктрині міжнародного права визначають в якості військового (іноді – військово-політичного) аспекту міжнародної інформаційної безпеки (відповідно і термінологія, яка використовується – “інформаційні війни”, “інформаційні операції” [9] тощо).

Військовий аспект міжнародної інформаційної безпеки виступає в якості одного із вагомих з тієї причини, що здатен безпосередньо впливати на міжнародний світ і безпеку. Однак, варто зазначити, що сприйняття військового аспекту в якості складової міжнародної інформаційної безпеки в міжнародному праві не є безперечним.

Необхідність розробки спільних заходів щодо розвитку норм міжнародного права в області обмеження розробки, поширення і застосування інформаційної зброї, підготовки і введення інформаційної війни передбачає *Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки* від 16 червня 2009 року [5].

Джерелом цієї загрози, відповідно до цієї угоди, є створення і розвиток інформаційної зброї, що представляє загрозу для критично важливих структур держави, що може привести до нової гонки озброєнь і представляє загрозу в галузі міжнародної безпеки. Її ознаками є застосування інформаційної зброї в цілях підготовки і ведення інформаційної війни, а також вплив на системи та об’єкти оборони, в результаті чого держава втрачає обороноздатність (п. 2) [8].

Міжнародне співробітництво, з метою протидії використанню інформаційного простору у військових цілях, може передбачати комплекс заходів.

Найбільш широко вони представлені у проекті універсальної Конвенції про забезпечення міжнародної інформаційної безпеки 2011 року. Так, згідно з її положеннями, міжнародне співробітництво в цілях протидії використання інформаційної сфери у інформаційних війнах та інформаційних операціях та військових конфліктах включає заходи щодо випереджувального виявлення та попередження потенціальних конфліктів у інформаційному просторі та мирного врегулювання спорів.

Передбачається, що для цього держави спрямовуватимуть зусилля на підтримку співробітництва в сфері забезпечення міжнародної інформаційної безпеки для підтримки миру і безпеки, сприяння стабільності і прогресу. Для досягнення цієї мети держави будуть вживати необхідних заходів для попередження деструктивного інформаційного впливу зі своєї території або з використанням інформаційної інфраструктури, що знаходиться під юрисдикцією держави; будуть утримуватись від розробки та прийняття планів, доктрин, здатних спровокувати зростання загроз у інформаційному просторі, а також викликати напруженість у відносинах між державами та виникнення “інформаційних війн”; будуть утримуватись від будь-яких дій, спрямованих на повне або часткове порушення цілісності інформаційного простору інших держав; будуть утримуватись у міжнародних відносинах від загрози силою або її застосування проти інформаційного простору будь-якої держави задля його порушення або в якості заходу розв’язання конфліктів; будуть вживати заходів щодо обмеження поширення “інформаційної зброї” та технологій її створення; візьмуть зобов’язання не використовувати інформаційно-комунікаційні технології для втручання у внутрішні справи держав; утримуватимуться від організації або сприяння організації будь-яких іррегулярних сил для здійснення неправомірних дій в інформаційному просторі іншої держави; утримуватимуться від наклепницьких тверджень, а також від образливої або ворожої пропаганди для здійснення інтервенції або втручання у внутрішні справи інших держав (ст. 6) [6].

Передбачається, що розв’язання конфліктів у інформаційному просторі держави вирішуватимуть, у першу чергу, шляхом переговорів, обстежень, посередництва, примирення, арбітражу, судового розгляду, звернення до регіональних органів або іншими мирними заходами на свій розсуд таким чином, щоб не піддавати загрозі міжнародний мир і безпеку. Пропонується, в разі міжнародного конфлікту закріпити право держави, що знаходиться в конфлікті, обирати методи і засоби ведення “інформаційної війни”, обмежене застосовними нормами міжнародного гуманітарного права (ст. 7) [6].

Отже, є обґрунтованим твердження про те, що міждержавні відносини у питанні безпеки в інформаційній сфері можна структурувати на підставі зазначених трьох складових. Використання їх в сукупності забезпечить захист інтересів особи, держави і світового співтовариства в інформаційній сфері.

Висновки.

Таким чином, розглянувши питання, пов’язані із складовими елементами інституту міжнародного інформаційного права у міжнародному праві, можна зазначити наступне:

- інститут міжнародної інформаційної безпеки розглядається в доктрині міжнародного права в якості одного з ключових елементів системи міжнародної безпеки;
- до складу міжнародної інформаційної безпеки в доктрині міжнародного права відносять кримінальний, терористичний та військовий елементи;

- розвиток інституту міжнародної інформаційної безпеки відбувається в рамках регіональних організацій;

- правові основи співробітництва держав у забезпеченні міжнародної інформаційної безпеки на регіональному рівні відбуваються з урахуванням різних концептуальних підходів щодо його кримінальної, терористичної та військової складових;

– спільна діяльність держав в сфері правового регулювання міжнародної інформаційної безпеки виступає в якості суттєвого додаткового фактору розвитку міжнародних інформаційних відносин.

Використана література

1. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях : международный опыт : монография / А.Л. Осипенко – М. : Норма, 2004. – 432 с.

2. Шнайдер Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайдер. – СПб. : Питер, 2003. – 368 с.

3. Борьбе с преступлениями в сфере компьютерной информации : Соглашение о сотрудничестве государств-участников Содружества Независимых Государств от 01.06.01 г. // Московский журнал международного права. – 2008. – № 4(72). – С. 244-250.

4. Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. – Режим доступу : //www.zakon2.rada.gov.ua/laws/show/994_575

5. Про співробітництво в області забезпечення міжнародної інформаційної безпеки : Угода між урядами держав-членів ШОС від 16.06.09 р. – Режим доступу : //www.base.spinform.ru/show_doc.fwx?rgn=28340

6. Проект Конвенции об обеспечении международной информационной безопасности. – Режим доступа : //www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/42df9e13d28e06ec3257925003542c4!Open Document

7. Касьяненко М.А. Правовые проблемы при использовании Интернет в транснациональном терроризме / М.А. Касьяненко // Информационное право. – 2012. – №1(28). – С. 21-25.

8. О сотрудничестве в области обеспечения международной информационной безопасности : Приложение 2 к Соглашению между правительствами государств-членов Шанхайской организации сотрудничества. – Режим доступа : //www.base.spinform.ru/show_doc.fwx?rgn=28340

9. Информационная война и международное право. Право и информатизация общества : сб. науч. тр. РАН ИНИОН ; отв. ред. И.Л. Бачило. – М., 2002. – 223 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~