Національна безпека

УДК 351.746

Тиква Володимир Леонідович
старший викладач
Національна Академія СБ України
Tykva Volodymyr
Senior Lecturer
National Academy of Security of Ukraine

УКРАЇНСЬКЕ СУСПІЛЬСТВО В УМОВАХ ВІЙНИ: РИЗИКИ ТА ЗАГРОЗИ В ІНФОРМАЦІЙНІЙ СФЕРІ
UKRAINIAN SOCIETY AT WAR: RISKS AND THREATS IN THE INFORMATION SPHERE

Анотація. *У статті автор досліджує стан, ризики та загрози національній безпеці України в інформаційній сфері в умовах військового вторгнення рф в Україну.*

Воєнна безпека держави була і залишається одним із пріоритетних напрямків забезпечення суверенітету України, її територіальної цілісності та недоторканності кордонів. Зміна характеру воєнних загроз на сучасному етапі розвитку військового мистецтва та форм і методів ведення збройної боротьби, гібридний характер дій противника висуває нові вимоги до системи забезпечення воєнної безпеки держави в усіх сферах, в тому числі у сфері інформаційної безпеки.

На основі проведеного аналізу фактів прихованого втручання ззовні в інформаційну сферу нашої держави, вдалого відбиття деструктивних інформаційних впливів з боку країни-агресора, враховуючи позитивний досвід інших країн, для формування власної наступальної інформаційної

політики України автор пропонує розширити та удосконалити заходи спрямовані на мінімізацію наслідків.

Ключові слова: *національна безпека, забезпечення інформаційної безпеки держави, кібербезпека, об'єкти критичної інформаційної інфраструктури, інформаційний простір, система оцінювання ризиків та загроз.*

Summary. *The article is aimed at examining the state, risks and threats to the national security of Ukraine in the information sphere in the conditions of the russian military invasion into Ukraine.*

The military security of the state has always been one of the priority areas of ensuring the sovereignty of Ukraine, its territorial integrity and the inviolability of borders. The change in the nature of military threats at the current stage of the military art development and the forms and methods of conducting armed struggle, the hybrid nature of the enemy's actions puts forward new requirements for the system of ensuring military security of the state in all spheres, including the field of information security.

Based on the analysis of the facts of covert interference from the outside in the information sphere of our state, successful reflection of destructive informational influences from the part of the aggressor country, taking into account the positive experience of other countries, the author proposes to expand and improve measures aimed at minimizing the consequences in order to form Ukraine's own offensive information policy.

Key words: *national security, provision of state information security, cyber security, objects of critical information infrastructure, information space, risk and threat assessment system.*

Постановка проблеми. З початком повномасштабної війни російської федерації проти України, 24 лютого 2022 року, інформаційний та кіберпростори Української держави стали повноцінними театрами

воєнних дій в яких країна-агресор намагається реалізувати свою загарбницьку політику, шляхом поєднання деструктивних дій у кіберпросторі з інформаційно-психологічними операціями різних рівнів.

За таких умов, коли агресія росії в інформаційному і кіберпросторі є однією з основних складових повномасштабної війни проти нашої держави, а численні кібератаки та інформаційно-психологічні операції на інформаційні ресурси – невід`ємною її компонентою, перед Україною з новою актуальністю постає питання пошуку шляхів та механізмів забезпечення інформаційної та кібернетичної безпеки від сучасних викликів та загроз, які виникають.

При цьому, варто акцентувати увагу, що загрози і ризики інформаційної та кібербезпеки не обмежуються територією однієї лише нашої держави, а мають транскордонний характер, що значно ускладнює можливості їх оцінки й нейтралізації та актуалізує питання міжнародної взаємодії та співробітництва світової спільноти. Зазначене потребує прийняття активних та скоординованих заходів реагування суб`єктів міжнародної системи забезпечення інформаційної та кібербезпеки.

Для розробки та реалізації заходів нейтралізації загроз у сфері інформаційної та кібербезпеки України необхідно володіти цілісною картиною суспільних відносин у визначених сферах та особливостями їх правового регулювання. Саме тому, на сьогодні нагальною і вкрай актуальною є проблема аналізу організаційно-правових засад управління інформаційною та кібернетичною безпекою як складових національної безпеки в Україні.

Аналіз останніх досліджень і публікацій. Дослідження складають такі праці фахівців у галузі інформаційної безпеки, як С.В. Белай [1], Д.М. Корнієнко [1], А.В. Войціховський [2], О. М. Косогов [3], Т. О. Гурджій [4], М. А. Дмитренко [5], О.О. Золотар [6], Ю.О. Левченко [7] , Ю. М. Тодика [8].

Формування цілей статті (постановка завдання) – дослідити систему оцінювання ризиків і загроз національній безпеці України в інформаційній сфері України в умовах військового вторгнення та розробити перелік заходів спрямованих на їх мініманізацію наслідків.

Викладення основного матеріалу. Початок військової агресії з боку російської федерації поставив перед нашою країною безліч викликів і загроз, серед яких на перший план виступає посилення захисту в інформаційній сфері. При цьому відсутність жорсткої територіальної прив'язки ключових інформаційних ресурсів дозволяє інформаційно-комунікаційним лідерам опановувати і використовувати будь- яке втручання. Ефективне освоєння чужих територій стає можливим шляхом використання інформаційної локалізації. Небезпеки, що створюються даними загрозами, часто змушують залишати в стороні погодження гострих соціальних проблем в середині України, формують умови фінансово-економічної нестабільності і створюють передумови соціальної та політичної деструкції.

Таким чином, в сучасному світі все більше уваги приділяється захисту в інформаційній сфері. Як і в будь-якому іншому виді діяльності, грамотне планування забезпечення безпеки в інформаційній сфері є найважливішим етапом на шляху до забезпечення безпеки країни в цілому. Організація ефективної системи захисту інформаційної сфери стає критично важливим стратегічним чинником існування України в сучасних умовах, так як, інформація є одним з ключових елементів гібридної війни. При цьому, під інформацією розуміються не тільки статичні інформаційні ресурси (бази даних, поточні налаштування обладнання та інші), а й динамічні інформаційні медіа ресурси.

Кожна країна піддається загрозам безпеки і конфіденційності. Сучасні засоби захисту здатні боротися з атаками кіберзлочинців. Але цього недостатньо, тому держава повинна забезпечити такі умови

внутрішньої політики і поведінки громадян, щоб мінімізувати або значно зменшити ці ризики [1].

Вплив інформації та інформаційних технологій стає одним з передумов формування суспільства. Володіння своєчасними, точними, достовірними даними слугує надзвичайно важливим фактором ефективності прийняття управлінських рішень як на державному рівні, так і на рівні регіонів України.

Система оцінювання ризиків та загроз в інформаційній сфері в умовах війни

Аналізуючи окреслену тематику можна впевнено стверджувати, що до початку збройної агресії з боку рф значно менша увага приділялась питанню безпеки країни, а державні органи управління в інформаційній сфері або не реагували на виклики, а якщо і відбувалась реакція то з запізненням. Але реалії сьогодення доводять, що на даний час успішно формується алгоритми дієвої політики державної безпеки у інформаційному аспекті, розробка механізмів її формування та реалізації, особливо, в умовах гібридних загроз. Так у ст.1 Закону України «Про національну безпеку України» № 2469УІІІ від 21 червня 2018 року (зі змінами та доповненнями) зазначено, що державна безпека — захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру. Разом із тим, зовнішні інформаційні загрози постійно видозмінюються і ставлять перед фахівцями нові питання і примушують шукати нові варіанти вирішення загроз у сфері інформаційної безпеки.

Система оцінювання ризиків і загроз в інформаційній сфері України в умовах ведення гібридної війни забезпечує стратегічне планування у сфері національної безпеки. Зокрема, вона надає можливість українському урядові оцінити широкий спектр ризиків і загроз національним інтересам

та безпеці країни в діапазоні коротко- та довгострокових змін безпекового середовища, визначити стратегічні цілі та пріоритетні завдання щодо забезпечення національної безпеки і стійкості. Система передбачає застосування всеосяжного підходу до проведення оцінювання ризиків і загроз. Для цього підходу властиве об'єднання зусиль максимально широкого кола учасників зазначеного процесу на національному, регіональному та місцевому рівнях. При цьому до оцінювання ризиків залучаються сили й засоби міністерств і відомств, профільних наукових та експертно-аналітичних установ, органів місцевого самоврядування, представників бізнесу, громадянського суспільства та ін. Система функціонує комплексно й послідовно, у єдиному алгоритмі в рамках циклу стратегічного планування у сфері національної безпеки. Під час проведення оцінювання ризиків і загроз в ієрархічній структурі управління системи застосовується принцип «зверху донизу», відповідно до якого загальнонаціональна оцінка ризиків і загроз є основою для розробки відповідних оцінок на регіональному та місцевому рівнях [2].

Передусім існує потреба оцінки загрози національній безпеці українського суспільства в світовому масштабі - міжнародного, воєнного, геоекономічного, геополітичного, техногенного, соціального тощо. При цьому береться до уваги, що в умовах глобалізації міжнародні та внутрішні інформаційні загрози взаємопов'язані.

Основними критеріями для формування певних класів різнотипних ризиків є такі: 1) наслідки; 2) імовірність; 3) ступінь невизначеності; 4) масштабність поширення наслідків інформаційних вкидів; 5) потенціал стійкості/опірності до ризиків; 6) здатність до відновлення; 7) тривалість наслідків; 8) ступінь шкоди правам і свободам громадян, іміджу органів влади; 9) потенціал конфліктності у суспільстві (соціальні хвилювання, психологічні реакції тощо). З урахуванням отриманої інформації у державі

повинні розроблятись програми забезпечення стійкості українського суспільства.

Для зменшення ризиків та загроз в інформаційній сфері проводиться постійний аналіз зовнішніх і внутрішніх чинників. З цією метою визначено, що аналіз загроз — це виявлення ризиків з метою їх зменшення; він має бути процесом постійним і включати:

- аналіз інцидентів небезпек у попередньому періоді та заходів, що приймалися для усунення ризиків;
- аналіз корисності та ефективності заходів протидії, здійснених для усунення ризиків;
- виявлення нових потенційних загроз для суспільних, державних, інформаційних, організаційних процесів тощо;
- аналіз ймовірності ескалації загроз;
- аналіз можливих прямих та непрямих наслідків реалізації загроз;
- визначення ризиків, від яких необхідно забезпечити захист;
- визначення заходів запобігання ризикам, мінімізації шкоди від них;
- оцінювання, чи мінімізований ризик є прийнятним;
- вживання заходів для попередження аналогічних ризиків;
- оцінка, після визначеного періоду, ефективності вжитих заходів; якщо загрози залишаються, слід розробляти і вживати заходи на протидію їм.

В сучасних умовах існування інформаційної сфери вже виник і розвивається ринок інформаційної безпеки світу. З початком збройної агресії інформаційна сфера України стала своєрідним випробувальним майданчиком, де окрім безпосередніх учасників конфлікту, випробовують свій безпековий продукт і інші країни світу.

Можна впевнено говорити, що ринок інформаційної безпеки в Україні існує і розвивається, враховуючи небезпечні фактори що його супроводжують. У нашому розумінні учасники ринкової інформаційної

безпеки окрім користувачів та надання послуг і рішень, також українські та міжнародні регулятори.

Загалом інформаційна сфера в Україні в основному досить успішно бореться з ризиками та загрозами, що виникали з початком збройної агресії. Але, можна виділити основні проблеми для інформаційної сфери в Україні:

- відсталість законодавства в питаннях регулювання її захисту;
- психологічна проблема менеджменту держави (спочатку інформаційний інцидент повинен завдати шкоди і тільки після цього починаються заходи щодо захисту);
- відсутність дієвого механізму оцінки нанесеної шкоди (нездатність оцінити репутаційні ризики).

Щодо загроз в інформаційній сфері, то їх у загальному вигляді визначають як сукупність чинників та умов, що створюють небезпеку певному об'єкту.

О. Косогов розглядає загрозу як родову ознаку безпеки (можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу в межах певної території, спричинити смерть людей чи завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків тощо) [3].

Заходи протидії спрямовуються саме на ризики як об'єкти управління. Визначимо заходи протидії загрозам в інформаційній сфері, що актуальні для України в сучасних умовах війни з Росією. До прикладу, у 2018 році було виявлено, проаналізовано та спростовано у відкритих джерелах ряд фейкових і маніпулятивних повідомлень, які є загрозами національній інформаційній безпеці:

- фейк "Україна включила Естонію до списку офшорів";
- маніпулятивний звіт Amnesty International;

- блокування українських активістів у соціальних мережах через скарги російських тролів;
- фейк "українці радіють смертям у Кемерово";
- публікації "На Харьков" та "Политнавигатора", що розпалюють міжнаціональну ворожнечу;
- фейковий канал ГУР МО в Telegram;
- фейки про Україну від журналістів міжнародних видань у Москві;
- фейк про підрив автомобіля з бійцями НАТО на Донбасі;
- пов'язування України з діяльністю ІДІЛ;
- містифікація про трьох мертвих канадських солдатів в Україні від росЗМІ;
- фейк "Шотландский парламент аплодує візиту українського фашиста";
- публікація архіву з 3 млн твітів російських тролів;
- зміна політики Telegram щодо персональних даних;
- візит "представників громадських організацій США" до Криму.

Захист вітчизняного інформаційного простору потребує забезпечення громадян «чистим» контентом, фільтрованим від сепаратистського, проросійського наповнення. Заборона поширення російської пропаганди на території України немає нічого спільного з придушенням свободи слова і демократії, як говорять про це симпатики «руського міра». Це захист національних інтересів від деструктивних впливів країни-агресора. Тому в Україні має максимально заблоковане мовлення ворожих нам ЗМІ, які віщують як з території Росії, так і з підконтрольних їй українських територій [4].

Саме прийняття закону «Про медіа» унеможливлює поширення неконтрольованого потоку новин сепаратистського спрямування, що розпалює ворожнечу між членами суспільства, які живуть в різних частинах держави. У спеціальному законі визначено порядок ліцензування,

правовий статус, принципи діяльності Інтернет-медіа, їхні права й обов'язки, передбачено відповідальність за пропагандистський / ворожий контент, аж до відібрання ліцензії на діяльність. Як конкретні методи протидії інформаційно психологічним впливам для захисту інформаційного простору фахівцями пропонуються :

- встановлення та перекриття (знешкодження) потенційних каналів проникнення деструктивної інформації в національний інформаційний простір;
- пряме та непряме спростування джерела деструктивного впливу (сумнівність щодо джерела інформації; абсурдність звинувачень; прив'язка джерела інформації до будь якої негативної події; введення ще одного негативного факту, який легко піддається спростуванню);
- відволікання уваги (відволікання ресурсів противника на інший об'єкт шляхом перенаправлення його на іншу діяльність, введення в інформаційний простір нового сенсаційного повідомлення;
- відвертання уваги аудиторії на малозначущий факт у рамках поточної проблеми;
- мовчання у відповідь;
- мінімізація впливу (акцентування на тому, що в повідомленні вказано на деякі правдиві події тощо);
- дискредитація (оприлюднення компромату, негативна "похвала", громадське обурення);
- розмиття негативу (генерація нейтральної або позитивної інформації про об'єкт в об'ємах, що перевищують об'єми негативної інформації) [5].

На державному рівні повинна удосконалюватись інформаційна технологія протидії ворожій російській пропаганді, яку повинні використовувати всі владні структури, відповідальні за інформаційну безпеку в Україні. Вони повинні оперативно реагувати на нові

компромати, що постійно з'являються у вітчизняному інформаційному просторі, який, на жаль, нині не контролюється ефективно державою. Отже, слід створити базу контраргументів російським повідомленням, яку можна було б використовувати не лише постфактум, а й попереджувально.

У контексті сказаного окремо увагу варто звернути на те, що в умовах глобалізації інформаційних процесів, формування світового інформаційного простору, швидкого зростання світового ринку інформації жодна держава, звісно ж, не може функціонувати в інформаційній ізоляції. Саме це й насторожує, бо в цьому разі інформаційні джерела і потоки на території будь-якої країни майже неможливо повністю убезпечити від втручань, нападів, зовнішнього інформаційного впливу й витоку внутрішньої інформації. Вбачається, шо саме цим пояснюється важливість для України (як, до речі, і для буль-якої іншої держави) вирішення проблем у сфері інформаційної безпеки, запобігання поширенню негативних тенденцій і подолання наслідків, які настали через спроби хакерів втрутитися чи провести кібератаку. Більш того, і це головне, приходить усвідомлення того, що необхідно розробити логічно завершену з правової й організаційної точок зору систему формування, розвитку, використання, управління, захисту інформаційних ресурсів, забезпечення національної безпеки, складовою якої є інформаційна безпека. Додамо, що йдеться як про можновладців, так і про пересічних громадян, право яких на недоторканність особистого життя, закріпленого ст. 31,32 Конституції України, захищається державою. Підтвердженням вказаного є рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012, в якому, спираючись на результати системного аналізу положень частин першої, другої статті 24, частини першої статті 32 Конституції України, Суд констатував, що «реалізація права на недоторканність особистого і сімейного життя гарантується кожній особі незалежно від статі, політичних, майнових, соціальних, мовних чи інших ознак» [6].

Наведене набуває неабиякої ваги з огляду на ситуацію, що склалася: зовнішня агресія з боку Росії, анексія Криму, поширення країною-агресором фейків тощо. Звісно, за таких умов для України питання забезпечення безпеки інформаційної сфери як невід'ємної складової національної безпеки стоять особливо гостро. До цього додається й ціла низка інших проблем, які лише на перший погляд є суто технічними. Мова йде про внутрішнє життя української держави, яке сьогодні супроводжується вкрай складними відносинами столичного центру зі східними регіонами, хворобливою соціальною модернізацією, внутрішньою нестабільністю і політичною невпорядкованістю, політичним і соціальним розшаруванням, що інколи доходить до рівня протистояння, кризою економіки та фінансовою дестабілізацією. Як бачимо, саме збройний конфлікт, політична напруженість, інформаційна агресія з боку Росії є тим важелем, який підштовхує Україну до рішучих дій, спрямованих на захист свого суверенітету й незалежності. Зупинимося на цьому трохи детальніше.

Так, згідно аналізу проведеного О. Білорусом, у 2020 році, досліджуючи глобалізацію і національну стратегію України: «Законодавче поле у нас не є взірцеве, завдяки йому в інформаційній сфері працює будь-хто і як захоче. Ми фактично втратили інформаційний суверенітет, бо маємо всього 10% державної частки, коли Франція, Польща, Німеччина - до 40 %, а деякі наші сусіди й 60%. Вони мають по 3-5 державних радіо-, 2-3 телеканали, а у нас особливо в кабельних мережах фактично сидить інша держава». Проте, як відомо, проблема забезпечення безпеки інформаційної сфери як невід'ємної складової стальної національної системи безпеки держави й захисту засад конституційного ладу безпосередньо має вирішуватися державними структурами, до обов'язків яких віднесено забезпечення, додержання й захист Конституції України. Звісно, це логічно, бо з державно-правової точки зору в системі

національної безпеки особливе місце повинні посідати охорона Конституції, забезпечення стабільності конституційного ладу України. Не випадково проф. Ю. М. Тодика вказану проблему розглядав як комплексну політико-правову, яка набуває особливого значення в період становлення державності, економічної, політичної і соціальної нестабільності, формування правової системи держави на концептуально новій основі [7].

Більш того, результати дослідження сучасних підходів до вивчення і розуміння інформаційної безпеки свідчать, що окреслена проблема є багатоаспектною. Проте цій сфері тривалий час не приділялася належна увага, що стало однією з причин посилення внутрішніх протирічь і конфліктів, інспірованих ззовні за допомогою використання передусім інформаційно-комунікаційних засобів.

Як показала історія (світові війни і революції), безпека більше не забезпечується раціональними домовленостями і непорушними державними інститутами. Очевидно, що загрози безпеці сьогодні можуть бути як зовнішніми, так і внутрішніми, саме тому її забезпечення набуває особливої ваги [8].

До наведеного варто додати те, що на думку вітчизняних експертів із проблем безпеки інформаційної сфери, які аналізували іноземний вплив на іноземний медіа- і кіберпростір України, на сьогодні наявні ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції:

- цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;
- активізація критики вищого державного керівництва України;
- здійснення низкою зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- й зовнішньополітичній сферах;

- посилення інформаційних заходів із перешкоджання реалізації Україною її зовнішньополітичного курсу і спонукання до участі в проектах, які в сучасних умовах не вигідні нашій державі;
- дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;
- зростання для України загроз кібернетичних атак, що зумовлено появою нових, більш досконалих зразків кібернетичної зброї.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Усе наведене вище дозволяє зробити висновок про те, що з точки зору інформаційної безпеки на сьогодні Україна продовжує перебувати в зоні ризику, хоча з лютого 2022 року цій сфері стало приділятися набагато більше уваги, що, урешті-решт, і стало однією з причин зменшення внутрішніх протиріч і конфліктів, інспірованих ззовні за допомогою в першу чергу інформаційно-комунікаційних засобів.

Підсумовуючи, слід констатувати, що «інформаційна війна» з росією багато чому нас навчила. Як і раніше, стурбованість викликають і маніпуляції з новинами, походження «конфіденційності джерел», кібератаки і ексцеси в боротьбі з фейковими новинами. Крім того, контрольований сепаратистами схід країни перетворився на закриту зону без критично налаштованих журналістів та іноземних спостерігачів.

Отже, необхідність забезпечення безпеки інформаційної сфери, захисту інформаційного суверенітету, як нами доведено, зумовлено формуванням інформаційного простору, необхідністю забезпечення національної безпеки України в цілому й існуванням загроз в інформаційній сфері держави, які можуть завдавати значної шкоди національним інтересам в комплексі. Як показує досвід провідних країн, розроблення виваженої і чіткої національної інформаційної стратегії сприятиме успішному вирішенню завдань у політичній, економічній,

соціальній та інших сферах життя. Більш того, в умовах ведення теперішнім російським керівництвом агресивної політики щодо України, лише активна (наступальна) позиція могла б вплинути на позитивний хід подій і сприяти зменшенню впливу як внутрішньополітичних, так і зовнішніх факторів. Для своєчасного вирішення цих завдань у правовому, організаційному й організаційно-технічному аспектах Україні ще багато треба зробити. Зокрема, щоб захистити інформаційний простір треба створити системи управління національними інформаційними ресурсами, надійний захист каналів державного управління, протидії інформаційним загрозам.

Література

1. Белай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід`ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ: Національна академія Служби безпеки України, 2018. С. 12.
2. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східно-європейського права. 2018. № 53. С. 28.
3. Косогов О. М. Пріоритетні напрями державної політики щодо забезпечення безпеки національного кіберпростору. Збірник наукових праць Харківського університету Повітряних Сил. 2014. Вип. 3. С. 127-130.
4. Гурджій Т. О. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 18.
5. Дмитренко М. А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 40-41.
6. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. С. 154-155.

7. Левченко Ю.О. Проблеми протидії інформаційній окупації в умовах гібридної війни. Інформаційна безпека в умовах гібридної війни: Міжнар. наук.-практ. конф. (м. Хмельницький, 16-17 лист. 2017 р.). Хмельницький: МВС України, 2017. С. 38.
8. Тодика Ю. М. Народовладдя на трансформаційному етапі розвитку держави і суспільства: монографія. Харків: Право, 2007. 480 с.