Політологія

УДК 321.01

Дубов Дмитро Володимирович
кандидат політичних наук,
старший науковий співробітник,
завідувач відділу інформаційної безпеки
та розвитку інформаційного суспільства
Національного інституту стратегічних досліджень
e-mail: shamus123@mail.ru

"ЦИФРОВИЙ СУВЕРЕНІТЕТ" У СУЧАСНОМУ СВІТІ: ВИКЛИКИ ТА МОЖЛИВОСТІ ДЛЯ УКРАЇНИ

Стаття присвячена проблемі забезпечення "цифрового суверенітету". Аналізуються ключові проблеми розбудови "цифрового суверенітету" української держави та необхідні для цього передумови, а також два сценарії побудови "цифрового суверенітету" в Україні: перший (умовно) заснований на об'єктно-орієнтованому підході та реалізації класичної вестфальської системи в цифровому світі; другий – на понятті "акціонованого суверенітету" та зорієнтований на формування необхідних інституційних, організаційних та економічних механізмів. Зроблено висновок, що стратегічно доцільною є розбудова "цифрового суверенітету" України на базі другого сценарію.

Ключові слова: цифровий суверенітет, вестфальська система, інновації, акціонований суверенітет.

Дубов Дмитрий Владимирович, *кандидат политических наук, старший научный сотрудник, заведующий отделом информационной безопасности и развития информационного общества Национального института стратегических исследований*

"Цифровой суверенитет" в современном мире: вызовы и возможности для Украины

Статья посвящена проблеме обеспечения "цифрового суверенитета". Анализируются ключевые проблемы построения "цифрового суверенитета" украинского государства и необходимые для этого условия, а также два сценария построения "цифрового суверенитета": первый (условно) основан на объектно-ориентированном подходе и реализации классической вестфальской системы в цифровом мире; второй – на понятии "акционированного суверенитета" и ориентирован на формирование необходимых институциональных, организационных и экономических механизмов. Сделан вывод, что стратегически целесообразным является построение "цифрового суверенитета" Украины на базе второго сценария.

Ключевые слова: цифровой суверенитет, вестфальская система, инновации, акционированный суверенитет.

Dubov Dmitro, *Ph.D. in political science, senior scientific officer Head of Department of information security and the development of the information society The National Institute for Strategic Studies*

"Digital sovereignty" in the modern world: challenges and opportunities for Ukraine

The article deals with providing "digital sovereignty." The article analyzes the key problems of building a "digital sovereignty" of the Ukrainian state and the necessary conditions for this. Were analyzed by two dominant scenario of building a "digital sovereignty". First, conditionally, based on the object-oriented approach and the implementation of the classical Westphalian system in the digital world. The second – is based on the concept of "corporatized sovereignty" and is focused on the formation of the necessary institutional, organizational and economic mechanisms. It is concluded that it is appropriate to strategically build "digital sovereignty" Ukraine on the basis of the second scenario.

Keywords: digital sovereignty, Westphalian system, innovation, corporatized sovereignty.

Державний суверенітет – невідчужувана юридична якість незалежної держави, яка символізує її політико-правову самостійність, вищу відповідальність і цінність як первинного суб'єкта міжнародного права. Суверенітет означає, що всі правила на території даної держави встановлюються тільки нею самою й ніким іншим. З точністю "до навпаки": держава несуверенна не є самостійною, а перебуває під зовнішнім управлінням, тобто є колонією, напівколонією або ж складовою іншої держави.

Україна особливо гостро зіткнулась із проблемою захисту та відстоювання свого суверенітету в 2014 р., і цей виклик ще довгий час буде залишатись актуальним для нашої держави. При чому це буде стосуватись всіх аспектів державного суверенітету і не в останню чергу – цифрового, який є складовою інформаційного.

Деструктивні щодо української державності дії РФ, розпочаті у березні 2014 року, наочно продемонстрували роль й значення інформаційної безпеки держави у сучасному світі, оскільки масові компанії з дезінформації та пропаганди, подання викривлених новин та тенденційних оцінок – все це стало тлом протистояння між Україною та РФ й, озброєними керівництвом цієї держави, сепаратистами. Протягом усього цього часу Україна принаймні декілька разів стикалась із загрозами інформацій-

но-технологічного характеру, починаючи від вже традиційних DDos-атак та спам-розсилок і закінчуючи зламом (спробами зламу) урядових систем. Останнє (виклики та загрози інформаційно-технологічного характеру) стають все більш значущими та небезпечними для України.

Це обумовлюється тим, що залежність ефективного розвитку будь-якого сучасного суспільства від ІКТ стає визначним фактором суспільного розвитку. Виразний безперервний інноваційний характер ІКТ з одного боку створює все нові можливості для подальшого економічного та соціального зростання, а з іншого – створює нові виклики для безпеки людей та держави, на які вони не завжди можуть відповісти.

Іншою проблемою стає те, що весь цей розвиток відбувається у класичних умовах суперництва держав між собою та їх бажання використати ІКТ для забезпечення необхідної переваги для себе в глобалізованому світі. При цьому розуміється і необхідність захистити себе від негативних впливів на/через ІКТ від сторонніх гравців.

Все це змушує держави активніше звертатись до проблеми вироблення принципово нового розуміння свого місця (завдань, можливостей, засобів) в нових реаліях і до того, наскільки взагалі держава зберігає свою суверенність у цифровому просторі. І для України ця проблема, актуальна як ніколи. Відповідно, метою роботи є визначення ключових викликів та можливостей на шляху утвердження цифрового суверенітету України.

Питаннями забезпечення цифрового суверенітету та кібермогутності держав займались такі дослідники як Ф. Крамер, С. Старр, Л.Вентц [2], Лі Жанг [4], А. Клімбург [3], а серед українських – М. Ожеван, Д. Дубов [6], В.Гапотій [9], А.Череп [10].

Можливості забезпечення Україною власного інформаційного/цифрового суверенітету досить неоднозначні. Передусім – через вкрай складні військово-політичні та економічні умови, в яких існує наша держава, а тим більше – зовнішньої агресії проти неї. Крім того, оглядаючи потенціал України крізь призму методологічних рамок східно-азійських дослідників [6] можна зробити висновок, що за майже кожним із принципових пунктів, можливості України досить обмежені. Передусім це стосується економічного аспекту питань, зокрема інноваційного характеру української економіки. На жаль, ми і досі навіть наближено не підійшли до середньо світових показників частки інновацій у ВВП держави. В кращому випадку ми маємо безперервну "модернізацію навздогін", яка до інноваційного розвитку відношення майже не має. Це стабільний шлях до своєрідного неоколоніалізму.

І важливою частиною цієї проблеми є не лише традиційне небажання потужних фінансових груп розвивати високотехнологічні сектори, але й те, що Україною досі не були сформовані образи "бажаного майбутнього". Лише в Стратегії розвитку інформаційного суспільства [11] від 2013 року частково про це згадується – чого ми власне хочемо досягти. Однак за всі роки незалежності в Україні так і не були проведені цілісні форсайтні дослідження, які дали б змогу хоча б теоретично уявити, якою Україна бачить себе через 10, 20 років? Які на її думку технології будуть затребувані? Без цього ми не спроможні сформулювати найбільш виграшні стратегії розбудови технологічного сектору, весь час рухаючись у фарватері інших гравців.

Не менш складно стоїть питання із спроможностями держави ефективно конкурувати на міжнародних цифрових ринках, передусім – через власні ІТ-корпорації. Цілком зрозуміло, що штучно їх створити навряд чи можливо, однак саме держава має створити умови для їх появи. Показовою в цьому сенсі є Росія, яка хоч і має, вочевидь, неефективну економічну модель газової/нафто залежності, однак зрозуміла важливість реального входження своїх гравців на міжнародний ІТ-ринок і для цього сприяла побудові таких компаній як Yandex, Mail.ru чи "Лабораторія Касперського". І хоча окремі їх спроби "вигадати велосипед" у вигляді власних мобільних телефонів [1], планшетів тощо нам видаються дивними, а подекуди і кумедними, однак стратегічно це правильний шлях, хоча і обираються при цьому не зовсім вірні тактичні засоби.

Без потужних ІТ-компаній Україна ніколи не буде мати національних операційних систем, антивірусів, пошуковиків тощо. Відповідно різноманітні рішення державних органів (на кшталт Рішення РНБО від 28 квітня 2014 року [12]) так і будуть залишатись "на папері", оскільки не мають реальної інфраструктури реалізації. Тим більше, що такі завдання мають виникати у вигляді довгострокових і продуманих завдань, коли зрозуміла реальна мета та можливості.

В цьому контексті державі взагалі варто серйозно переглянути своє відношення до проблеми співвідношення "державного" та "національного", оскільки ці два поняття часто ототожнюються. Ефективна стратегія держави в цьому питання – напрацювання реального механізму тісної співпраці із приватним сектором та налагодження державно-приватного партнерства. В цьому сенсі пріоритетною є ґрунтовна реформа законодавства як в сфері державно-приватного партнерства, так і того законодавства, що впливає на розвиток ІТ-сектору. В чинних економічних умовах держава буде довгий час просто не в змозі приймати на себе додаткові фінансові зобов'язання із великих проектів, тим більше, що далеко не завжди є ефективні механізми їх реалізації. В тому числі – по відношенню до ІТ-сектору.

Важливим є і те, якою мірою Україна буде розвивати власний ІТ-ринок. Сьогодні ми маємо дійсно серйозний цифровий розрив між Києвом та більшістю регіонів. Провайдери майже вичерпали ресурс міст-мільйонників та навіть міст з населенням більше 100 тис. при цьому йти у менші міста для них часто економічно не доцільно. Частково цю проблему може вирішити 3G зв'язок, однак це питання в кращому випадку року-півтора [5]. При цьому більшість провідних держав світу вже розпочинають

будівництво 5G мереж [13] і відповідно, навіть після впровадження 3G ми знов постанемо перед проблемою технологічного відставання

Ще одне важливе питання – зовнішня політика України щодо майбутнього кіберпростору. Україна бере участь у роботі Міжнародного союзу електрозв'язку, взаємодіє з ICANN однак досі ми не маємо чіткої та послідовної позиції держави щодо того, яким Україні бачиться "майбутнє інтернету"? Навіть державні органи не завжди можуть вияснити, що Україна підписує в межах тих чи інших заходів і що це означає для держави та її громадян. Не можна не відмітити досить пасивну позицію МЗС України в цьому питанні, в тому числі – на рівні ООН.

На жаль, Україна майже не бере участі у роботі спеціальних груп ООН, які виробляють підходи в сфері глобальної інформаційної безпеки. (У 2009 р. Відповідно до резолюції 60/45 Генасамблеї ООН була створена група урядових експертів ООН з міжнародної інформаційної безпеки. Група створена з 15 експертів з таких країн: Білорусь, Бразилія, КНР, Естонія, Франція, Німеччина, Індія, Ізраїль, Італія, Катар, Південна Корея, РФ, Південно-Африканська Республіка, Велика Британія та США. Керівником групи став представник РФ Андрій Крутських.) Так само, Україна майже не виступає із міжнародними ініціативами щодо мережі інтернет та того, в якому напрямку мережа має розвиватись. Слід визнати, що на даному етапі ми залишаємось пасивними спостерігачами глобальних процесів, а сама позиція держави щодо цих питань у кращому випадку реактивна, однак точно не проактивна.

Крім того, до останнього часу незрозуміле, яким державі бачиться майбутнє українського домену, які перспективи його розвитку та низка інших суто внутрішніх проблем.

Важливим є розвиток військової складової цифрового суверенітету. Ми лише частково підійшли до даного питання, і навіть в середині Міністерства оборони є лише досить умовний консенсус щодо того, хто і як має займатись питаннями кібербезпеки, хоча не можна не відмітити і певні позитивні кроки. Наприклад, вже розроблюються перші дослідницькі кіберполігони [8], відбуваються процеси реформування та оптимізації системи управління цією сферою. Варто особливо відзначити, що багато в чому завдяки тісній співпраці та узгодженості позицій профільних державних структур (зокрема, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації, Міністерства внутрішніх справ, підрозділів Міністерства оборони, Служби зовнішньої розвідки) та низки науково-експертних організацій (в тому числі – Національного інституту стратегічних досліджень) розуміння кібербезпекової складової національної безпеки сьогодні вже не виникає таких дискусій, як це було навіть 3-4 роки тому.

Вкрай неоднозначним питанням залишається і українська система нормативно-правових документів, що впливають на формування інформаційного/цифрового суверенітету. В цьому сенсі складно не відмітити майже повну недієвість всього комплексу документів, що функціонують в цій сфері починаючи від Національної програми інформатизації [7] і закінчуючи прийнятою у 2013 році Стратегією розвитку інформаційного суспільства.

Важливо відмітити, що все вищезазначене мало впливає на суспільну дискусію відносно цифрового суверенітету держави. Більше того, спостерігаються очевидні взаємопротилежні інтенції, щодо того, як саме держава має будувати свій цифровий суверенітет. Домінуючими є два, досить умовних, сценарії.

Перший з них базується на тому, що Україна має розбудовувати свій цифровий суверенітет в межах повернення до базових концепцій вестфальського світоустрою, де суверенітет є майже абсолютним. Прихильники такого підходу зазвичай вимагають від держави вже найближчим часом створити національну операційну систему, національну систему мобільного зв'язку, національного телекомоператора, національну пошукову систему, національний мобільний термінал та багато іншого "національного". Фактично ж це заклик до негайної розбудови російсько-китайської моделі в Україні.

На нашу думку, реалізація такого сценарію у режимі "тут і зараз" мало реальна. Слід розуміти, що на сьогоднішній день (а швидше за все і у віддаленій перспективі) Україна не буде мати змогу реалізувати більшість таких "важких" проектів. Більше того, в багатьох випадках це і недоцільно, оскільки сприяє не стільки утвердженню суверенітету, скільки нецільовому використанню бюджетних коштів. Адже більшість з цих проектів будуть потребувати значних вливань з державного бюджету, що нереально в умовах тотальної бюджетної економії.

Крім того, далеко не завжди вдається зрозуміти доцільність створення тих чи інших елементів саме з огляду на їх необхідність та потрібність на поточному етапі розвитку Української держави. Так, розробка "національної операційної системи" виглядає абсолютно беззмістовною, оскільки незрозуміла ані технологічна платформа її створення, ані кінцева мета, ані реальна причина. У випадку ж відновлення різноманітних "національних" телекомунікаційних операторів виникають ризики іншого характеру, в тому числі – монопольного положення на ринку, ефективності управління ними і знов так – кінцевої мети.

Знов таки, у своїй більшості прихильники такого сценарію розвитку стають на стратегічно неперспективну позицію відштовхування від потреб певних "елементів". Як вже зазначалось раніше, за цього підходу існують ризики того, що якісь важливі елементи будуть пропущені та невраховані.

Натомість другий сценарій передбачає багатоступеневу систему планування, кінцевою метою якого і буде отримання реального цифрового суверенітету.

Перш за все увага має бути акцентована на створенні можливостей (механізмів), які дозволять в подальшому створити будь-який з потрібних "елементів". Загальною методологічною рамкою у про-

цесі реальної розбудови цифрового суверенітету має стати методологічна рамка, запропонована східноазійськими дослідниками [4]. Цей підхід базується на більш сучасних розумінням суверенітету, що актуальні саме для глобалізованого світу. Мова йде про теорії "акціонування" суверенітету, коли кожна держава має чітко визначені "квоти" реального суверенітету, поступаючись водночас на засадах вільного вибору своїми повноваження міжнародним або наднаціональним структурам у вирішенні питань, які ця країна самостійно вирішити неспроможна.

За таких умов маємо більш-менш чітке розуміння того, що потрібно розвивати, аби і у стратегічній перспективі залишатись убезпеченими та технологічно розвинутими, однак при цьому – не виснажувати "безпековим" дискурсом державу. Це, передусім:

- посилення інноваційної складової української економіки;
- сприяння розвитку ІТ-сектору (з особливим акцентом на формування потужних ІТ-ТНК);
- розвиток внутрішнього ринку та інформаційної інфраструктури;
- формулювання чітких позицій щодо майбутнього мережі інтернет як на міжнародній арені, так і в середині країни із подальшим активним відстоюванням їх;
- сприяння поширенню української культури у Всесвітній Мережі;
- акцент на необхідності більш інтенсивної підготовки Збройних Сил України та взагалі державних органів до кібервійн;
- адекватна нормативно-правова політика щодо розвитку інформаційного суспільства та інформаційного/цифрового суверенітету.

Саме у цих питаннях держава не тільки може, але й має здійснювати активну діяльність, навіть користуючись виключно наявним економічним та організаційним потенціалом.

Крім того, маємо зрозуміти, що потрібна нова та зрозуміла система різнорівневих цілей, яких бажає досягнути держава на шляху утвердження власного цифрового суверенітету. На сьогоднішній день ця сфера є або слабо визначеною, або визначеною надмірно загально. При чому ця багаторівнева система може включати в себе і завдання першого сценарію, однак виключно на рівні певних віддалених цілей, для досягнення яких буде потрібно здійснити абсолютно зрозумілі та реальні кроки. В цілому така система різнорівневих цілей має підпорядковуватися такій логіці:

- умовний "ідеальний рівень", досягнення якого хоча і є бажаним, однак виглядає малодосяжним навіть у віддаленій перспективі (наприклад, малоймовірно, що в осяжній перспективі ми дійсно зможемо створювати власні операційні системи чи розбудувати ІТ-корпорацію світового рівня). Водночас слід враховувати, що дійсно цілісна постановка завдань буде потребувати низки системних форсайтних досліджень, які дозволять принаймні в загальному сенсі зрозуміти, про перспективи найближчих 10-20 років;
- "стратегічний рівень", який виділяє ті показники "ідеального рівня", які можуть бути досягнуті в разі послідовної реалізації цілісної державної політики в перспективі 5-7 років (умовно, завдання формування національних ІТ-корпорацій потребує прийняття відповідного законодавства, налагодження приватно-державного партнерства, розвитку технопарків тощо);
- "тактичний рівень", який передбачає залучення наявних, накопичених, збережених чи нещодавно створених ресурсів, які можуть бути і мають бути використані у розвитку складових інформаційного суверенітету за умови повноцінної підтримки державою подібної інвестиційної політики.

Відповідно до такого розподілу майже будь-яка складова цифрового суверенітету може і має бути розкладена на окремі елементи та в подальшому знайти своє відображення у Плані дій чи Стратегії.

Отже, на сьогоднішній день концепція "цифрового суверенітету" щодо України все ще може розглядатись виключно як певна стратегічна конструкція, яка в практичній площині майже не реалізується. Це зумовлено низкою об'єктивних складнощів економічного розвитку, станом нормативно-правової бази та браком цілеспрямованої політики держави та окремих профільних структур. Водночас згадана концепція потребує подальших наукових та практичних розробок, що дасть змогу більш цілісно підійти до питань довгострокового розвитку України, в тому числі в безпековому аспекті.

Література

1. "Ростехнологии" создадут свой мобильный телефон [Електронний ресурс] // Lenta.ru. – Режим доступу: http://lenta.ru/news/2010/09/13/telefon.
2. Kramer F. Cyberpower and National Security / Franklin D. Kramer, Stuart H. Starr, Larry Wentz. – Washington, D.C: Potomac Books, 2009. – 642 p.
3. The Whole of Nation in Cyberpower [Електронний ресурс] / Alexander Klimburg // Austrian Institute for International Affairs. – Режим доступу: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/News/The_Whole_of_Nation_in_Cyberpower_AK.pdf.
4. Zhang Li. A Chinese perspective on cyber war / Li Zhang // International Review of the Red Cross. New Technologies and Warfare. – Jun 2012. – P. 801-807.
5. Беседа Я. Зв'язок нового покоління [Електронний ресурс] / Яна Беседа, Дарія Ісакова // Forbes.ua. – Режим доступу: http://forbes.ua/ua/magazine/forbes/1380616-zvyazok-novogo-pokolinnya.
6. Дубов Д. В. Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні / Дмитро Дубов // Вісник національної академії керівних кадрів культури і мистецтв. – 2014. – №1. – С.233-238.

7. Закон України "Про Національну програму інформатизації" [Електронний ресурс] // Верховна Рада України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/74/98.

8. Івахів С. Де взяти армію майбутнього? [Електронний ресурс] / Степан Івахів // ВолиньPost. – Режим доступу: http://www.volynpost.com/blogs/1230-de-vziaty-armiyu-majbutnogo.

9. Інформаційне суспільство та інформаційний суверенітет: теоретико-правовий аспект [Електронний ресурс] / В. Д. Гапотій, А. А. Письменицький // Науковий вісник Дніпропетровського державного університету внутрішніх справ. – 2012. – № 2. – С. 24-33.

10. Інформаційний, культурний та економічний суверенітет в умовах сучасної глобалізації [Електронний ресурс] / А. В. Череп, А. Р. Шевченко // Економічний простір. – 2013. – № 76. – С. 40-48.

11. Стратегія розвитку інформаційного суспільства в Україні // Урядовий кур'єр. – № 105.

12. Указ Президента України (№ 449/2014) "Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" [Електронний ресурс] // Рада національної безпеки і оборони України. – Режим доступу: http://www.rnbo.gov.ua/documents/347.html.

13. Широкосмуговий доступ до мережі Інтернет як важлива передумова інноваційного розвитку України: аналіт. доп. / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2013. – 112 с.

References

1. "Rostekhnologii" sozdadut svoi mobil'nyi telefon [Elektrolinii resurs] // Lenta.ru. – Rezhim dostupu: http://lenta.ru/news/2010/09/13/telefon.

2. Kramer F. Cyberpower and National Security / Franklin D. Kramer, Stuart H. Starr, Larry Wentz. – Washington, D.C: Potomac Books, 2009. – 642 p.

3. The Whole of Nation in Cyberpower [Elektronnyi resurs] / Alexander Klimburg // Austrian Institute for International Affairs. – Rezhym dostupu: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/News/The_Whole_of_Nation_in_Cyberpower_AK.pdf.

4. Zhang Li. A Chinese perspective on cyber war / Li Zhang // International Review of the Red Cross. New Technologies and Warfare. – Jun 2012. – R. 801-807.

5. Beseda Ya. Zviazok novoho pokolinnia [Elektronnyi resurs] / Yana Beseda, Dariia Isakova // Forbes.ua. – Rezhym dostupu: http://forbes.ua/ua/magazine/forbes/1380616-zvyazok-novogo-pokolinnya.

6. Dubov D. V. Problemy normatyvno-pravovoho zabezpechennia informatsiinoho suverenitetu v Ukraini / Dmytro Dubov // Visnyk natsionalnoi akademii kerivnykh kadriv kultury i mystetstv. – 2014. – № 1. – S.233-238.

7. Zakon Ukrainy "Pro Natsionalnu prohramu informatyzatsii" [Elektronnyi resurs] // Verkhovna Rada Ukrainy. – Rezhym dostupu: http://zakon4.rada.gov.ua/laws/show/74/98.

8. Ivakhiv S. De vziaty armiiu maibutnoho? [Elektronnyi resurs] / Stepan Ivakhiv // VolynPost. – Rezhym dostupu: http://www.volynpost.com/blogs/1230-de-vziaty-armiyu-majbutnogo.

9. Informatsiine suspilstvo ta informatsiinyi suverenitet: teoretyko-pravovyi aspekt [Elektronnyi resurs] / V. D. Hapotii, A. A. Pysmenytskyi // Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav. – 2012. – № 2. – S. 24-33.

10. Informatsiinyi, kulturnyi ta ekonomichnyi suverenitet v umovakh suchasnoi hlobalizatsii [Elektronnyi resurs] / A. V. Cherep, A. R. Shevchenko // Ekonomichnyi prostir. – 2013. – № 76. – S. 40-48.

11. Stratehiia rozvytku informatsiinoho suspilstva v Ukraini // Uriadovyi kurier. – № 105.

12. Ukaz Prezydenta Ukrainy (№ 449/2014) "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 roku "Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy" [Elektronnyi resurs] // Rada natsionalnoi bezpeky i oborony Ukrainy. – Rezhym dostupu: http://www.rnbo.gov.ua/documents/347.html.

13. Shyrokosmuhovyi dostup do merezhi Internet yak vazhlyva peredumova innovatsiinoho rozvytku Ukrainy: analit. dop. / D. V. Dubov, M. A. Ozhevan. – K. : NISD, 2013. – 112 s.