УДК 342.9

Діордіца І. В.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і процесу
Національного авіаційного університету

ПОЗИТИВНІ ЧИННИКИ ФОРМУВАННЯ КІБЕРНЕТИЧНОЇ ФУНКЦІЇ ДЕРЖАВИ

POSITIVE FACTORS FOR THE FORMATION OF THE CYBERNETIC FUNCTION OF THE STATE

У статті проаналізовані позитивні чинники формування кібернетичної функції держави. Автором подано систему аргументів щодо формування наукової гіпотези стосовно того, що на сьогоднішньому етапі кібернетична функція держави становить собою окрему, самостійну функцію держави. Виділено низку чинників, що впливають на формування та подальшу реалізацію даної функції. Диференційовано дані чинники на дві загальні групи з метою зосередження та виділення як позитивних, так і негативних чинників. Розглянуто позитивні чинники формування кібернетичної функції.

Ключові слова: *кіберпростір, кібербезпека, кібернетика, кібернетична функція, чинники формування, позитивні чинники.*

В статье проанализированы положительные факторы формирования кибернетической функции государства. Автором представлена система аргументов по формированию научной гипотезы о том, что на сегодняшнем этапе кибернетическая функция государства представляет собой отдельную, самостоятельную функцию государства. Выделен ряд факторов, влияющих на формирование и последующую реализацию данной функции. Дифференцированы данные факторы на две общие группы, с целью сосредоточения и выделения как положительных, так и негативных факторов. Рассмотрены положительные факторы формирования кибернетической функции.

Ключевые слова: *киберпространство, кибербезопасность, кибернетика, кибернетическая функция, факторы формирования, положительные факторы.*

The article analyzes the positive factors of forming the cybernetic function of the state. The author presents a system of arguments for the formation of a scientific hypothesis that at the present stage the cybernetic function of the state is a separate, independent function of the state. There are a number of factors that influence the formation and further implementation of this function. These factors are differentiated into two general groups, in order to focus and distinguish both positive and negative factors. Positive factors for forming a cybernetic function are considered.

Key words: *cyberspace, cyber security, cybernetics, cybernetic function, formation factors, positive factors.*

Мною в моїх роботах подано систему аргументів щодо формування наукової гіпотези стосовно того, що на сьогоднішньому етапі кібернетична функція держави становить собою окрему, самостійну функцію держави.

Звичайно, що даний процес на даному етапі, зважаючи на його швидкість на динамічність, поки не є детально описаним в наукових дослідженнях, водночас це саме і додає наукової новизни моїй роботі. Адже наука передусім має реалізовувати прогностичну функцію, а не тупцювати на одному місці, здійснюючи аналіз подій, які вже відбулись. Поза це доцільним, з урахуванням напрацювань інших дослідників [1–6], офіційних аналітичних доповідей [7–11], чинних нормативно-правових актів, що регулюють суспільні відносини в кібербезпековій сфері, є виділення низки чинників, що впливають на формування та подальшу реалізацію даної функції. Причому я диференціюю дані чинники на дві загальні групи з метою зосередження та виділення як позитивних, так і негативних чинників.

У даній статті я розгляну позитивні чинники формування кібернетичної функції.

До *позитивних чинників формування кібернетичної функції* доцільно включити:

Безпековий блок:

1) *усвідомлення необхідності формування національної системи кібербезпеки* – в грудні 2015 р. – січні 2016 р. Україна отримала чергове підтвердження використання Росією кіберзброї: хакери атакували ПАТ «Прикарпаттяобленерго», внаслідок чого 225 тис. споживачів на години залишилися без світла [12]; належні висновки не були зроблені, і 27 червня 2017 року масштабній кібератаці були піддані вже майже всі центральні органи виконавчої влади в Україні;

2) *фрагментарні спроби щодо формування системних можливостей держави в реалізації кібербезпекової політики* через посилення спроможностей суб'єктів системи національної безпеки для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю;

3) *поглиблення міжнародного співробітництва у сфері реалізації кібербезпекової політики*, яке має відповідати національним інтересам України, ґрунтуватись на Стратегії сталого розвитку і Стратегії національної безпеки України, забезпечити перевагу українських кіберсил принаймні в тактичній перспективі в українському сегменті кіберпростору;

4) реалізація державної кібербезпекової політики через забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення

сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура);

5) доцільність нарощування кібербезпекових можливостей держави, переведення національної системи зв'язку, стратегічних загальнодержавних автоматизованих систем управління, урядових мереж, систем зв'язку і управління зброєю, інформаційно-телекомунікаційних мереж і систем органів військового управління на функціонування в умовах особливого періоду, мобілізації додаткових ресурсів для організації операцій у кіберпросторі;

6) необхідність підвищення ефективності реалізації військово-технічної політики й політики військово-технічного співробітництва у сфері кібероборони в контексті реалізації кібербезпекової політики;

7) здійснення моніторингу стану розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих зі стандартами ЄС та НАТО;

8) кібернетична функція держави тісно пов'язана з безпековою функцією, адже вона, з одного боку, поєднує в собі забезпечення захисту інформації та інформаційної інфраструктури, а з іншого – забезпечує розвиток інформаційного суспільства.

Світоглядний блок:

1) *формування відкритого та вільного кіберпростору*, що розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, нових ринок криптовалюти, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції, в тому числі і через використання механізм блокчейн технологій;

2) трансформація кіберсуспільства випереджує трансформацію світогляду політичних еліт, і відповідно, форм і методів управління, впливає на недостатньо високі темпи впровадження концепції е-урядування;

3) формується і реалізується на тлі зменшення домінуючої ролі держави в ефективному управління соціальними системами і переходом до ліберального управління з більшим залученням кіберспільноти до цих процесів;

4) формується система розумного балансу між *обмежувальними* (для ворожого контенту та деструктивних дій супротивника) і *стимулюючими* (для власного контенту) заходами як стосовно захисту інтересів громадян, суспільства та держави, так і для подальшого розвитку її інформаційного простору;

5) необхідність формування кіберосвіти, що уможливить адекватне та коректне наукове забезпечення та супроводження реалізації кібернетичної функції.

Кібернетичний блок:

1) удосконалення процедури застосування санкцій Національною радою України з питань телебачення і радіомовлення та розширення переліку підстав для переоформлення ліцензії [13], що спрямовано на забезпечення дієвого механізму здійснення нагляду у сфері телебачення та радіомовлення. Кінцевою метою ухвалених змін визначено захист інформаційного простору держави, можливість своєчасного реагування на виявлені загрози та протидія їм;

2) позбавлення російських спецслужб можливостей слідкувати за громадянами України через блокування відповідних сайтів [14] (санкції проти юридичних осіб ВАТ «Яндекс», ВАТ «Мейл.РУ Украина», ВАТ «ВКонтакте», «Одноклассники» та ін.) [15]. У даному аспекті потрібно усвідомлювати, що блокування сайтів і сервісів належить до сфери забезпечення безпеки, а не свободи слова, що і було визнано нашими партнерами з ЄС та міжнародних організацій (НАТО [16]). Особливої значущості ця теза набуває в контексті нещодавніх прикладів використання BigData у виборчому процесі [17];

3) формування в рамках кібербезпеки такого напряму, як *контентна безпека*, в рамках реалізації якої здійснюється комплекс заходів щодо боротьби з деструктивним контентом, який поширюється в кіберпросторі. Складно ігнорувати й ту роль, яку «фабрики тролів», дезінформаційні кампанії в соціальних мережах, створення величезної кількості пропагандистських ресурсів відігравали спочатку під час анексії Криму, а пізніше – для розпалювання сепаратистських настроїв на сході України, під час виборів президентів у більшості європейських країн. Особливо важливо, що сьогодні Україна разом зі світовими урядами починає давати правову оцінку таким діям противника;

4) державні е-ресурси, захищені спільним контуром кіберзахисту, реалізованим Держспецзв'язку в Системі захищеного доступу до Інтернету, а також електронні державні реєстри країни не постраждали й не зазнали несанкціонованих вторгнень, що є свідченням ефективності діяльності суб'єктів кібербезпеки [18];

5) налагоджено системну роботу Національного координаційного центру кіберзахисту при РНБО України (далі – Центр). Зокрема, завдяки діяльності Центру були розроблені організаційно-координаційні рішення щодо співпраці суб'єктів кібербезпеки стосовно ліквідації наслідків кібератак на державні інформаційні ресурси фінансового сектору, подолання наслідків атаки вірусу NotPetya, налагоджено процес розроблення та впровадження узгодженого протоколу спільних дій суб'єктів забезпечення кібербезпеки та власників об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та інших кіберінцидентів, а також при подоланні їхніх наслідків [11, с. 54];

6) продовження робіт із формування Переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави (значного прогресу було досягнуто щодо включення до цього документа операторів мобільного зв'язку).

Інфраструктурний блок:

1) *стрімкий розвиток інформаційних технологій*, що спричинює інформаційну глобалізацію та трансформацію світу інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

2) *необхідність забезпечення розвитку інформаційної інфраструктури держави*;

3) розвиток мережі реагування на комп'ютерні надзвичайні події (*CERT*);

4) розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів, забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак;

5) створення системи підготовки кадрів у сфері кібербезпеки для потреб суб'єктів забезпечення національної безпеки;

6) розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки;

7) розроблення на рівні держави комплексної системи захисту об'єктів критичної інфраструктури та формування на базі консенсусу з бізнес-сектором чітких і зрозумілих правил захисту таких об'єктів.

Блок стратегічних комунікацій:

1) Україна продовжує розвивати комунікативну спроможність органів влади. Доктрина інформаційної безпеки України, визначаючи розвиток системи стратегічних комунікацій пріоритетом, покладає на Міністерство інформаційної політики України завдання з розроблення стратегічного наративу і його імплементації. Практичне виконання завдань, визначених цією Доктриною, відображено в планах дій Уряду України, як річному, так і середньостроковому 22. За ініціативи Міністерства інформаційної політики України планується створити *Координаційну раду з питань стратегічної комунікації*;

2) продовжується реалізація Дорожньої карти Україна – НАТО зі стратегічних комунікацій: наразі відбувається оптимізація організаційної взаємодії державних суб'єктів. Запроваджуються короткотермінові та довго строкові курси зі стратегічних комунікацій для державних службовців та військовослужбовців: від початку 2017 р. проведено 5 навчальних заходів для фахівців сектору безпеки і оборони. Триває робота з виокремлення спеціальності «Комунікація» в «Переліку галузей знань та спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». Зокрема, в 2016 році в ОРІДУ при НАДУ при Президентові України було вперше відкрито магістерську спеціалізацію «стратегічні комунікації». Так само можу акцентувати і на діяльності Інституту стратегічних комунікацій Глобальної організації союзницького лідерства.

Правовий блок:

1) *усвідомлення і легітимація кібербезпеки як окремого напряму державної політики* на рівні концептуальних документів, зокрема в щорічному Посланні Президента України до Верховної Ради, Стратегії кібербезпеки України [19], відтак змістом кібербезпекової політики виступає реалізація *кібернетичної функції держави*;

2) *прийняття у 2016 р. Стратегії кібербезпеки України*, спрямованої на реалізацію до 2020 р. положень Стратегії національної безпеки України, – цей документ визначає уточнені загрози кібербезпеці, вказує пріоритетні напрями забезпечення кібербезпеки (зокрема, розвиток безпечного, стабільного і надійного кіберпростору, кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, кіберзахист критичної інфраструктури, розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки, боротьба з кіберзлочинністю). Стратегія закладає основу формування Національної системи кібербезпеки, визначає її основних суб'єктів;

3) *чітке виділення складових кібербезпекової політики в рамках становлення інформаційного суспільства*: 1) розвиток та безпека кіберпростору; 2) запровадження електронного урядування; 3) гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів;

4) *затвердження* Указом Президента України від 7 червня 2016 року № 242/2016 *Положення «Про Національний координаційний центр кібербезпеки»*;

5) ухвалення Указу Президента України від 13 лютого 2017 р. № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [20];

6) *розвиток та імплементація відповідно положень* Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», а також реформ, передбачених Угодою про асоціацію між Україною та ЄС, ратифікованою Законом України від 16 вересня 2014 року № 1678-VII, і Стратегією сталого розвитку «Україна – 2020», схваленою Указом Президента України від 12 січня 2015 року № 5;

7) ухвалення *Доктрини інформаційної безпеки України* [21], в якій закладено базові підходи до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації, а також функціонування держави в умовах використання агресором інформаційної сфери як ключової арени протиборства. Важливим здобутком Доктрини є чітке визначення механізмів її реалізації, що дозволить зробити цей засадничий документ практично значущим. Окремі напрями реалізації положень Доктрини в контексті реалізації кібербезпекової політики, зокрема щодо обмежень в українському сегменті мережі Інтернет, викликали

широку суспільну дискусію в контексті забезпечення свободи слова [11, с. 48];

8) вирішення проблеми обміну інформацією з обмеженим доступом між Україною та НАТО [22]: створена правова основа та визначено детальні процедури взаємної охорони інформації з обмеженим доступом, яка буде передаватися або створюватися в ході співробітництва [23]. Забезпечення рівноправного, партнерського характеру взаємовідносин у процесі інформаційного обміну сприятиме підвищенню ефективності взаємовигідного співробітництва України з НАТО;

9) припинення дії міжурядових угод із Російською Федерацією про співробітництво у сфері телебачення, радіомовлення та інформації, зумовлене тим, що їх подальша дія не відповідає стану міждержавних відносин і не узгоджується із заходами, яких вживає Україна для забезпечення захисту свого інформаційного поля від негативних інформаційно-психологічних впливів [24];

10) сформованість о сновних правових засад формування та успішної реалізації кібербезпекової політики;

11)формування балансу між збереженням провідної ролі держави як регулятора кібернетичних відносин, централізацією і децентралізацією в управлінні кібернетичною сферою;

12)на виконання Указу Президента України від 13.02.2017 р. № 32/2017, яким було введено в дію рішення РНБО України від 29.12.2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», відбувається стратегічний процес – кардинально оновлюються системні механізми реалізації Національної програми інформатизації, яка тривалий час фактично не виконувалася. Здійснюється контроль за формуванням завдань Національної програми інформатизації на 2018–2020 рр. та поданням відповідних пропозицій на розгляд Верховної Ради України разом із проектом Закону України «Про Державний бюджет України на 2018 рік [11, с. 56].

Фінансово-економічний блок:

1) у 2015 р. за статтею бюджету «Здійснення заходів у сфері захисту національного інформаційного простору» було виділено 2 млн. 800 тис. грн. У 2016 р. в головному фінансовому документі країни такої статті взагалі не було, а в 2017 р. на заходи щодо захисту національного інформаційного простору буде витрачено 33 млн. 600 тис. грн. [25];

2) інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО, для посилення спроможностей України у сфері кібербезпеки;

3) формується як результат оптимального співвідношення державного управління у кіберпросторі та саморегулювання, а також через чітке визначення меж втручання держави в економіку, а також взаємної відповідальності державних інститутів і інститутів громадянського суспільства за реалізацію кібернетичної функції. Розвиток криптовалютного ринку, блокчейн-технологій виступають реальним результатом розвитку недержавної складової кібербезпеки;

4) необхідність реалізації кібербезпекової політики та створення умови до кібернетичного суверенітету формує умови для кардинального збільшення кіберринку вітчизняними продуктами, в тому числі програмним забезпеченням роботами, технологіями, товарами та послугами;

5) необхідність здійснення заходів державної підтримки стратегічно важливих для реалізації державної кібербезпекової політики наукових установ і організацій, в тому числі неурядових. аналітичних організацій, проведення наукових досліджень у галузі кібербезпеки, в тому числі із залученням краудфандінгових компаній, використання можливостей краудсорсінгу для залучення інвестицій і розвитку власної кіберпромисловості, розвитку нових прогресивних технологій та хай-тек промисловості відповідно до реалізації національних інтересів;

6) визначення фінансово-економічного обґрунтування пріоритетів для залучення міжнародної технічної допомоги у сфері забезпечення кібербезпеки, в тому числі й залучення прямих інвестицій;

7) потреба в удосконаленні роботи зі створення конкурентноспроможних високо ефективних вітчизняних програмних продуктів для захисту як державних інформаційних ресурсів, так і для їхнього розповсюдження на світовому кіберринку, зокрема розроблення національної операційної системи, національного антивірусного програмного забезпечення із подальшим виведенням його на світові ринки кіберпродуктів тощо.

Відтак можна стверджувати, що наразі створено всі передумови для інституціоналізації кібернетичної функції держави, формування відповідної організаційно-функціональної структури, а також удосконалення системи стратегічних комунікацій відповідно до нових реалій в кібербезпековій політиці.

Звичайно, що існують і негативні чинники, водночас про них йтиметься в наступній моїй статті.

ЛІТЕРАТУРА:

1. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні: [монографія]. К.: ФОП О. С. Ліпкан, 2015. 664 с.

2. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом: [монографія]. К.: ФОП О.С. Ліпкан, 2013. 344 с.

3. Ліпкан В.А. Консолідація інформаційного законодавства України. К.: ФОП О.С. Ліпкан, 2014. 416 с.

4. Ліпкан В.А. Інкорпорація інформаційного законодавства України: [монографія]. К.: ФОП О.С. Ліпкан, 2014. 408 с.

5. Стратегічні комунікації: [словник]. К.: ФОП О.С. Ліпкан, 2016. 416 с.

6. Климентьєв О.П. Перспективи розвитку інформаційної функції держави. Підприємництво, господарство і право. 2013. № 12. С. 101.

7. Про внутрішнє та зовнішнє становище України в 2013 році: Щорічне Послання Президента України до Верховної Ради України. К.: НІСД, 2013. 576 с.

8. Аналітична доповідь Національного інституту стратегічних досліджень до позачергового Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України у сфері національної безпеки». К.: НІСД, 2014. 148 с

9. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2015 році». К.: НІСД, 2015. 684 с.

10. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році». К.: НІСД, 2016. 688 с.

11. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році». К.: НІСД, 2017. 928 с.

12. Сич О. Під час хакерської атаки на українські обленерго у антивірусів не було шансів. URL: http://www.epravda.com.ua/publications/2016/04/7/588680/.

13. Закон України «Про внесення змін до Закону України «Про телебачення і радіомовлення» від 1 листопада 2016 р. № 1715-VIII URL: http://zakon2.rada. gov.ua/laws/show/1715–19.

14. За даними компанії SimilarWeb, станом на 20 травня 2017 р. відвідуваність соціальної мережі «ВКонтакте» в Україні зменшилася на 3,35 млн. візитів за 5 днів блокування доступу (решта отримали доступ до заблокованого інтернет-ресурсу через VPN); відвідуваність російського інтернет-порталу yandex.ua знизилася приблизно на 2 млн. візитів, мережа «Одноклассники» втратила в середньому 1,67 млн візитів (див.: Відвідуваність ВКонтакте за 5 днів впала на 3 мільйони візитів. URL: http://www.epravda.com.ua/news/2017/05/23/625156/). Одночасно спостерігається зростання відвідуваності альтернативних ресурсів: на другий день після набуття указом чинності відвідуваність українцями мережі Facebook зросла на 40 %, а Google+ – на 85% (див.: Украинская аудитория Facebook выросла на четверть URL: http://ru.golos.ua/suspilstvo/ukrainskaya_auditoriya_acebook_vyirosla_na_chetvert_6261)..

15. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 15 квітня 2017 р. № 133/2017. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/U133_17.html.

16. У НАТО підтримали блокування російських сервісів в Україні. URL: https://ukr.lb.ua/news/2017/05/17/366496_nato_pidtrimali_blokuvannya.html.

17. Расследование Das Magazin: как Big Data и пара ученых обеспечили победу Трампу и Brexit. URL: https://www.facenews.ua/articles/2016/310687/.

18. Кібератака на об'єкти критичної інфраструктури України. Ситуація під контролем URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=278007&cat_id=268448.

19. Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016 Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» від 13 лютого 2017 р. № 32/2017. URL: http://zakon3.rada.gov.ua/laws/show/32/2017.

20. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25 лютого 2017 р. № 47/2017. URL: http://www.president.gov.ua/documents/472017–21374.

21. Розпорядження Кабінету Міністрів України «Про підписання Адміністративних домовле ностей щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного Договору» від 23 серпня 2016 р. № 604-р. URL: http://www.kmu.gov.ua/control/uk/cardnpd?docid=249263938.

22. Проект Закону про ратифікацію Адміністративних домовленостей щодо охорони інформації з обмеженим доступом між урядом України та Організацією Північноатлантичного договору від 18 квітня 2017 р. № 0144. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=61654.

23. Постанова Кабінету Міністрів України «Про припинення дії Угоди між Кабінетом Міністрів України і Урядом Російської Федерації про співробітництво в галузі телебачення і радіомовлення та Угоди між Кабінетом Міністрів України та Урядом Російської Федерації про співробітництво в галузі інформації» від 30 листопада 2016 р. № 1053. URL: http://zakon2.rada.gov.ua/laws/show/1053–2016-%D0 %BF.

24. Закусило М. Держбюджет-2017ф: скільки коштують суспільне, іномовлення, кіно. URL: http://detector.media/infospace/article/122357/2017–01–19-derzhbyudzhet-2017-skilki-koshtuyut-suspilne-inomovlennya-kino/.