

Методи, засоби та заходи організаційно-правового захисту інформації з обмеженим доступом

Анотація. В основу написання данної научної статті покладено аналіз законодавчої бази України та погляди учених на проблематику в сфері, котра стосується комерційної тайни суб'єктів господарювання. Проблематика заключається в тому, що немає Закону України «Про комерційну тайну», де повинні бути записані правила доступу до комерційної тайни правоохоронних органів та відповідальність цих контролюючих органів за розкриття свідомості, що складає комерційну тайну, як це передбачено в Законі України «Про банки та банківську діяльність».

Проведений аналіз свідчить, що в Україні рішенням проблематики, пов'язаної з комерційною тайною, повинна стати прийняття Закону України «Про комерційну тайну».

Ключові слова: інформація з обмеженим доступом, комерційна тайна, захист комерційної тайни, конфіденційна інформація, корпоративна безпека.

Abstract. This scientific article is based on the analysis of the legal framework of Ukraine and scientists' views on the issues of trade secrets entities. The range of problems consists in the absence of the Law of Ukraine «On Trade Secret», where the rules of law enforcement authorities access to trade secret must be prescribed and also there must be spelled out the responsibility of these controlling authorities for disclosure the information considered as a trade secret, as it is provided in the Law of Ukraine «On Banks and banking».

The analysis has shown that in Ukraine the solution of the trade secrets issues should be the adoption of the Law of Ukraine «On Trade Secrets».

Key words: classified information, trade secrets, the protection of trade secrets, confidential information, corporate security.

УДК 342.3+351:659.3

ПОЛЕВИЙ Володимир Іванович

ВИЗНАЧЕННЯ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ СКЛАДОВОЇ ДЕРЖАВНОГО СУВЕРЕНІТЕТУ

Постановка проблеми. В умовах неоголошеної агресії РФ проти України, характерною особливістю якої є активне інформаційне протистояння сторін, особливої актуальності набуває забезпечення інформаційної складової державного суверенітету.

Аналіз останніх досліджень і публікацій. Вивченням питання про

інформаційний суверенітет у різний час займалися зарубіжні та вітчизняні науковці. С. Краснер досліджував контроль над інформацією в контексті глобалізації; І. Панарін та І. Ашманов відстоюють у своїх працях концепцію інформаційного суверенітету як контроль держави за інформацією та інформаційною політикою; Д. Дубов,

Methods, means and measures for organizational and legal protection of classified information

О. Литвиненко, В. Петров, В. Панченко, Г. Почепцов розглядають суверенітет крізь призму категорії безпеки.

Мета статті – подальший дискурс щодо змісту поняття інформаційного суверенітету в сучасних умовах, а її завданням є визначення інформаційної складової державного суверенітету.

Тобто шукатимемо відповіді на такі запитання: чи можемо розглядати інформаційний суверенітет як складову суверенітету держави?; чи коректно говорити про верховенство та незалежність влади держави над інформацією в сучасному суспільстві?; чи потрібно наділяти державу владою над інформацією та в яких межах?

Виклад основного матеріалу. За класичного підходу суверенітет (від фр. *souveraineté* – верховна влада) передбачає верховенство, самостійність та повноту державної влади у всіх її вимірах всередині держави та незалежність і рівноправність держави у зовнішніх відносинах (див. Декларацію про державний суверенітет України).

Питання організаційного і правового забезпечення державного суверенітету вітчизняними науковцями розглядається переважно в політико-правовій площині. Це «верховенство влади всередині країни та її незалежність від влади будь-якої іншої держави», «повна незалежність держави від інших держав у її внутрішніх справах і зовнішніх відносинах» [1; 2]. При визначенні суверенітету наголошується на тому, що це є «...сукупність повновладдя нації і прав, які

гарантують незалежність особи. Суверенітет нації реалізується насамперед у можливостях її вільного політичного самовизначення, в правах на територію, що історично склалася і яку вона займає споконвіку, її природні ресурси і копалини, а також у верховенстві її законодавства та обраної державної влади, у національному громадянстві...» [3].

Статті 17 та 5 Конституції України визначають, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. При цьому носієм суверенітету і єдиним джерелом влади в Україні є народ. Принцип державного суверенітету отримав міжнародно-правове визнання (ст. 2 Статуту ООН 1945 року, Заключний акт НБСЄ 1975 року), але ніколи не був реалізований в його чистому вигляді. Як міжнародна, так і внутрішня політика реалізується внаслідок компромісів, взаємних поступок між сторонами та групами впливу, які суттєво обмежують «повноту та незалежність» влади.

У сучасних умовах суверенітет держави зіткнувся з викликами глобалізації: вільним рухом товарів, грошей, трудовою міграцією, інформаційними технологіями. Разом з цим слушною є теза Стівена Краснера, що «глобалізація не підриває фундаментальні основи суверенітету держав. Глобалізація – це виклик ефективності державного контролю» [4]. Причому виклик не новий за змістом. Питання про захист власної ідентичності в історії постає щоразу, коли

Методи, засоби та заходи організаційно-правового захисту інформації з обмеженим доступом

спільнота починає взаємодіяти з новою (часто більш ефективною) системою, яка їй не підконтрольна. Таке траплялося в часи великої міграції народів, географічних відкриттів, розвитку морської торгівлі, створення транснаціональних корпорацій. Сьогодні це виклик комунікаційних технологій.

В умовах демократії державний суверенітет також обмежується принципом верховенства прав і свобод людини, який встановлює рамки для нормативно-правового регулювання [5]. З огляду на зазначені обмеження автору імпонує думка В. Горового, що без ефективних інструментів забезпечення силового захисту від зовнішнього впливу розмови про інформаційний суверенітет є демагогією [6].

За класичного підходу до поняття «суверенітет» суверенітет інформаційний мав би передбачати контроль держави над поширенням інформації на своїй території та незалежність від впливів ззовні [7]. Таку концепцію, зокрема, намагаються реалізувати в деяких країнах Азії і Близького Сходу (КНДР, Китай, Іран) та в РФ.

І. Ашманов, наприклад, вважає, що інформаційний суверенітет у сучасних умовах є базисом для суверенітету державного [8]. Це право та можливість суб'єкта визначати свою інформаційну політику та інформаційні пріоритети самостійно. З І. Ашмановим погоджується Д. Дубов, В. Петров та інші дослідники, які вважають, що спроможність приймати суверенні рішення повинна базуватися на відповідному технологічному рівні інформаційно-комунікаційних

систем, контролі над власними big data, на власних незалежних медіа та інших виробниках контенту. Росіяни, щоправда, додають, що необхідними елементами суверенітету є також чітко сформульована державна ідеологія та система пропаганди.

У часи теоретичного та правового становлення концепції інформаційного суверенітету в РФ (І. Панарін, І. Ашманов) в Україні було прийнято Закон України «Про національну програму інформатизації» (1998 р.), який закріпив, що інформаційний суверенітет держави – це здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави [9].

Проте необхідно вказати, що значена здатність до контролю ніколи не була досягнута. Серед головних причин цього, по-перше, відкритість українського інформаційного простору до російського впливу. Так, наприклад, відповідно до міждержавних угод між Урядами України та РФ про співробітництво в галузі інформації, телебачення та радіомовлення передбачалося «створення сприятливих правових, організаційних та економічних умов для забезпечення трансляції та поширення програм російських телерадіомовних організацій на території України» [10] та «створення сприятливих умов для широкого та вільного взаємного розповсюдження інформації» [11]. По-друге, прямиий конфлікт із конституційним принципом свободи слова та доступу до інформації (ст. 34 Консти-

Methods, means and measures for organizational and legal protection of classified information

туції України), на сторожі якого стоять комерційно незалежні ЗМІ та неурядові організації із зарубіжною грантовою підтримкою. По-третє, технологічна відкритість та загальнодоступність, як засади побудови сучасних інформаційно-комунікаційних систем, які є насамперед інструментом інформаційного обміну сучасної глобальної економіки. З точки зору особи, вона має право на доступ до кращих зразків творів, наукових розробок тощо, як би державі не хотілося отримати контроль над контентом. Зі сторони економічних суб'єктів – обмеження доступу до інформації про характеристики ринку, політичні ризики, споживачів, тощо суперечить ліберальній концепції вільного ринку та ідеології побудови Інтернету, як комерційного інструменту.

Генезис правової думки про інформаційний суверенітет було проаналізовано Д. Дубовим [12]. Так, у Законі України «Про інформацію» (у редакціях 2002–2011 років) поняття «інформаційний суверенітет» пов'язали з інформаційними ресурсами, до яких належить вся належна Україні інформація, незалежно від змісту, форм, часу і місця створення [13]. Змінами 2011 року ці статті були виключені. Захист інформаційного суверенітету визначався «основною метою реалізації положень Доктрини інформаційної безпеки України» 2008 року [14], яка також втратила чинність. Вважаємо, що зазначені норми не були реалізовані через хибне розуміння тенденцій розвитку інформаційних процесів, а тому неправильно визначений об'єкт правового регулювання: в умовах, коли Україна почала

масово користуватися перевагами Інтернету та готовим інформаційним продуктом, у документах акцент робився на «інформаційних ресурсах, що формуються за рахунок коштів державного бюджету» та на «національних системах інформації» (ст. 54).

Тому важливо усвідомити місце України в сучасному інформаційному світі. Технології Інтернет, соціальних мереж, меседжерів, пошуковців та браузерів не є та в найближчому майбутньому не будуть українськими. Говорити про контроль над цими технологіями – це теоретична ілюзія, породжена нашим страхом перед невідомим, яке ми не контролюємо і не завжди розуміємо. В українському прокаті 99 % фільмів зарубіжного походження. Виходить, що інформаційний суверенітет (верховенство і незалежність влади в її класичному розумінні) для України є неможливою на сьогодні декларацією.

За таких обставин виникає питання, на яких частинах інформаційного простору слід концентрувати управлінські, підприємницькі та творчі зусилля, щоб забезпечити інформаційну безпеку та реалізацію національних інтересів України.

Перше – це контентне, змістовне наповнення інформаційного простору, яке є відокремленим від цифрових технологій напрямом. Наявність якісних, змістовних творів, спрямованих на розвиток потенціалу України, – це завдання для усього суспільства. Система забезпечення національної безпеки при цьому повинна реагувати лише на випадки виготовлення і поширення протиправного контенту. Поділяємо точку зору, що на 95 %

Методи, засоби та заходи організаційно-правового захисту інформації з обмеженим доступом

вміст інфопростору визначається не системою заборон і контролюючих органів, а якісними та кількісними характеристиками національного контенту. Разом з цим особливої уваги вимагають саме 5 % контролюючих функцій щодо контенту, оскільки тут маємо справу з діалектикою свободи слова, як основоположного права, та безпекою – як ключовою потребою особи.

Під контролюючими функціями слід розуміти організаційно-правову систему реалізації рішень, які є результатом суспільного консенсусу, тобто законодавчо визначені за допомогою конституційних механізмів законотворчості представницької демократії. Зазначена система включає:

1. Визнання окремих категорій інформації протиправними.

2. Закріплення механізму контролю за дотриманням «правил гри».

Так, до категорії протиправної інформації український законодавець відносить:

1. Брехню, тобто дифамацію про особу чи організацію. Конституція України закріплює право особи на повагу до честі та гідності та обов'язок держави з його захисту. Це право конкретизоване у ст. 297 Цивільного кодексу України. Також у цивільному праві передбачено право на недоторканність ділової репутації юридичної особи: ст. 201 ЦКУ визначає ділову репутацію як одне з немайнових прав, що підлягають захисту законом; ст. 200 ЦКУ встановлює спосіб захисту ділової репутації; статті 23 та 1167 ЦКУ визначають поняття немайнової шкоди та гарантують право на її відшкодування.

2. Інформацію, яка підриває основи національної державності, суспільного ладу чи громадського порядку. Сюди ж слід віднести відносно новий термін «мова ненависті». Йдеться про кримінальну відповідальність за публічні заклики та розповсюдження матеріалів, що посягають на суверенітет, територіальну цілісність та конституційний лад (статті 109–110 ККУ); про заклики до дій, що порушують громадський порядок (ст. 295 ККУ). Заборонена пропаганда війни (ст. 436 ККУ) та фашизму (ст. 436-1 ККУ). Кримінальна відповідальність за ксенофобію («мову ненависті») передбачена у ст. 300 ККУ.

3. Інформацію, від якої ми хочемо уберегти дітей: насильство (ст. 300 ККУ), порнографія (ст. 301 ККУ). Закон України «Про захист суспільної моралі» передбачає заборону інформації, яка «пропагує бузувірство, блюзнірство, неповагу до національних і релігійних святих; принижує особистість, пропагує невігластво, неповагу до батьків». З посиланням на цю норму твори можуть бути заборонені до показу на телебаченні, в кінопрокаті, в Інтернеті тощо.

4. Інформацію з обмеженим доступом. Про особу, про комерційну і державну таємницю тощо. Власне, протиправною є не сама інформація, а факт її несанкціонованого поширення.

Притягнення до адміністративної відповідальності можливе за використання засобів зв'язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність

Methods, means and measures for organizational and legal protection of classified information

громадян (ст. 148-3 КУпАП); за поширення неправдивих чуток (ст. 173-1 КУпАП); за поширення неправдивих відомостей про кандидата в Президенти України або в народні депутати України (ст. 186-2 КУпАП).

Маємо врахувати, що Україна ніяк не може вплинути на комерційні механізми пошукової чи контентної видачі Google чи Facebook. Тобто, якщо росіяни вкладуть (дають) 1 млрд дол. у рекламу інформаційних меседжів про «злочинну владу», «безсилю силовиків», та «не дамо вбивати наших синів», то це, безумовно, матиме (і вже має) значний вплив на стан громадської думки чи результати виборів в Україні. У поєднанні ж з іншими, не цифровими політичними технологіями, які базуються на досконалому вивченні потреб та психотипів населення: зустрічами з виборцями, особистим прийомом, бігбордами, листівками, концертами тощо, – такі інвестиції дають результат у вигляді голосування за потрібного інвестору кандидата.

Друге – це протидія інформаційному впливу Росії. З 2014 року Україна знаходиться у пошуку адекватних заходів захисту інформаційного простору. Протягом 2014–2016 років Національна рада з питань телебачення і радіомовлення заборонила 76 російських каналів [15], як такі, що не відповідають Європейській конвенції про транскордонне телебачення і українському законодавству. Відповідно до ч. 2 ст. 24, «якщо порушення має очевидний, серйозний і тяжкий характер, а також призводить до ви-

никнення складних суспільних проблем і якщо воно триває протягом двох тижнів після повідомлення про нього, приймаюча сторона може тимчасово припинити ретрансляцію програми, яка порушує конвенцію» [16].

Уряд припинив дію угод з РФ про співробітництво у сфері телебачення, радіомовлення та інформації, про які зазначалося вище [17].

Відповідно до Закону України «Про кінематографію» (ч. 3 ст. 15) Державне агентство з питань кіно відмовляє у видачі або припиняє дію вже виданого державного посвідчення на право розповсюдження і демонстрування фільмів, зокрема, якщо одним з учасників фільму є фізична особа, включена до Переліку осіб, які створюють загрозу національній безпеці.

Сам перелік складає Міністерство культури України на підставі звернень РНБО України, СБУ, Національної ради України з питань телебачення і радіомовлення.

До заборонних заходів слід також віднести Закон України «Про заборону пропаганди їхньої символіки».

Україна вжила заходів для заборони розповсюдження в Україні книг з антидержавним змістом та запровадила дозвільний порядок ввезення друкованої продукції з РФ, який передбачений Законом України «Про видавничу справу» (статті 28 та 28-1) [18]. Експертну оцінку змістовної частини текстів здійснює Експертна рада при Держкомтелерадіо України.

Методи, засоби та заходи організаційно-правового захисту інформації з обмеженим доступом

На підставі Закону України «Про санкції» [19] РНБО прийняло рішення «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», яке Президент України ввів у дію своїм указом [20]. Українським провайдером було вказано обмежити доступ до сайтів російських соцмереж «ВКонтакте» та «Однокласники», інтернет-порталу «Яндекс», поштового сервісу Mail.ru. Інструментом виконання цього рішення стала Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації.

Як бачимо, Україна вибудовує всебічний механізм блокування російського контенту. Щоправда, слід визнати обмежену ефективність цих заходів: доступ до заборонених ресурсів відбувається через VPN-з'єднання, а російське телебачення транслюється через супутниковий зв'язок та потужні ретранслятори у прикордонні; книги, заборонені для ввезення до України, все ж таки продаються.

На думку дослідників [21], до негативних наслідків отримання державою (чи корпораціями) контролю над інформаційними ресурсами також варто віднести те, що:

– накопичуючи інформацію держава (корпорація) знає все більше про індивідів, тоді як індивіди знають усе менше про неї;

– використання цифрових технологій реально може знизити, а не збільшити можливості для демократії.

Big Data та Інтернет-таргетування надає все більше можливостей для впливу на особу. Завдяки обробці величезних масивів персональних даних про особу та персоналізації повідомлень в Інтернет компанія Cambridge Analytica змогла реально вплинути на результати голосування під час виборів президента США у 2016 року [22].

Висновки. Державний суверенітет необхідно розглядати не тільки у політичній та економічній площині, але й у інформаційній, оскільки повнота влади та ефективність політичного чи економічного рішення безпосередньо залежить від інформації, на основі якої воно було прийнято, а також від комунікації з суб'єктами цього рішення. Тобто йдеться про інформаційну складову державного суверенітету.

Проте вважаємо, що про інформаційний суверенітет слід говорити лише як про суто теоретичну концепцію ідеального, але недосяжного стану повноти влади над інформаційними ресурсами і незалежності від зовнішніх впливів.

Разом з цим методологічно правильно виокремити із загального поняття державного суверенітету його інформаційну складову. Під *інформаційною складовою державного суверенітету* треба розуміти право та фактичну можливість відповідно до законодавства та з урахуванням балансу інтересів особи, держави та суспільства визначати та реалізовувати внутрішню інформаційну політику,

Methods, means and measures for organizational and legal protection of classified information

гарантувати інформаційну безпеку та виступати рівноправним суб'єктом зовнішнього (міжнародного) інформаційного обміну.

Звідси метою державного управління в інформаційній сфері має бути:

– наповнення внутрішнього та світового інформаційного простору

достовірною і позитивною інформацією про Україну та події, які в ній відбуваються;

– сприяння створенню якісного контенту;

– сприяння розвитку інформаційних технологій;

– забезпечення інформаційної безпеки.

Список використаних джерел

1. Політологічний енциклопедичний словник / уряд. В. П. Горбатенко ; за ред. Ю. В. Шемшученка, В. Д. Бабкіна, В. П. Горбатенка. – 2-е вид. доп. і перероблене. – К. : Генеза, 2004. – С. 643.
2. Большой экономический словарь / под ред. А. Н. Азрилияна. – М. : Институт новой экономики, 1998. – 687 с.
3. Філософія : навч. посіб. / за ред. професора І. Ф. Надольного. – К. : Вікар, 1997. – 485 с.
4. State and Sovereignty in the Global Economy / Edited by David A. Smith, Dorothy J. – London Solinger, Steven C. Topik. – 1999. – P. 34.
5. Алебастрова И. А. Конституционализм как правовое основание социальной солидарности / И. А. Алебастрова. – М. : Проспект, 2015.
6. Горовий В. М. Інформаційний суверенітет: актуальні питання теорії і практики / В. М. Горовий // Інформаційна безпека людини, суспільства, держави. – 2010. – № 1 (3). – С. 19–25.
7. Панарин И. Н. Проблемы информационной безопасности как одна из основ государственного суверенитета [Електронний ресурс] / И. Н. Панарин. – Режим доступу : <http://panarin.com/comment/1053>.
8. Ашманов І. С. Виступ на міжнародній конференції IForum2013 / І. С. Ашманов. – Київ. – 24.04.2013. [Електронний ресурс] / IForum2013. – Режим доступу : <https://habrahabr.ru/post/179579/>.
9. Закон України «Про національну програму інформатизації». [Електронний ресурс] / Офіційний сайт Верховної Ради України. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80>.
10. Угода між Кабінетом Міністрів України та Урядом Російської Федерації про співробітництво в галузі телебачення та радіомовлення від 23.10.2000. [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/643_135.
11. Угода між Кабінетом Міністрів України та Урядом Російської Федерації про співробітництво в галузі інформації від 27.02.1998. [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/643_112.
12. Дубов Д. В. Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні. Аналітична записка [Електронний ресурс] / Д. В. Дубов ; Національний інститут стратегічних досліджень. – Режим доступу : <http://www.niss.gov.ua/articles/1466/>.
13. Закон України «Про інформацію» // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
14. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009. [Електронний ресурс] //

Методи, засоби та заходи організаційно-правового захисту інформації з обмеженим доступом

Офіційний сайт Верховної Ради України. – Режим доступу : <http://zakon4.rada.gov.ua/laws/show/514/2009>.

15. Після «Дождя»: що загрожує медіапростору України? [Електронний ресурс] // Офіційний сайт Національної ради України з питань телебачення і радіомовлення. – Режим доступу : <https://www.nrada.gov.ua/pislya-dozhdya-shho-zagrozhuye-mediaprostoru-ukrayiny/>.

16. Європейська конвенція про транс-кордонне телебачення [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/994_444.

17. 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 року № 1053 [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : <http://zakon5.rada.gov.ua/laws/show/1053-2016-%D0%BF>.

18. Закон України «Про видавничу справу» [Електронний ресурс] // Офіцій-

ний сайт Верховної Ради України. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/318/97-%D0%B2%D1%80>.

19. Закон України «Про санкції» [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/1644-18>.

20. 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 травня 2017 року № 133/2017 [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : <http://www.president.gov.ua/documents/1332017-21850>.

21. Почепцов Г. Г. Інформаційна політика: сучасні підходи [Електронний ресурс] / Г. Г. Почепцов. – Режим доступу : http://osvita.mediasapiens.ua/ethics/manipulation/informatsiyna_politika_suchasni_pidkhodi/.

22. Расследование Das Magazin: как Big Data и пара ученых обеспечили победу Трампу и Brexit [Електронний ресурс]. – Режим доступу : <http://theins.ru/politika/38490>.

Рецензенти:

доктор юридичних наук, професор
Г. Новицький,
кандидат технічних наук, старший науковий співробітник
В. Панченко

Аннотація. В статтю розглядається можливість виділення інформаційної складової державного суверенітету. Інформаційний суверенітет є лише ідеальною концепцією повноти, самостійності та незалежності влади.

Ключові слова: суверенітет, інформаційна безпека, влада, захист інформаційного простору.

Abstract. The possibility of defining the informational component of the state sovereignty was considered in the article. In fact the Informational sovereignty is only the ideal concept of the completeness, self-sufficiency and independence of the power.

Key words: sovereignty, informational security, power, protection of the information area.