СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Земельне право України : підручник / М.В. Шульга та ін. Київ : Юрінком Інтер, 2004. 368 с.;
2. Шелестов В.С. Основные проблемы обеспечения качества продукции в хозяйственных договорах : автореф. дис. … д-ра юрид. наук. Харьков, 1967. с. 70–73.
3. Гук Б.М. Адміністративні послуги органів публічної влади України: поняття, зміст. Право і суспільство. 2011. № 3. С. 117–121.
4. Авер'янов В.Б. Вибрані наукові праці / за заг. ред. Ю.С. Шемшученка, О.Ф. Андрійко. Київ : Ін-т держави і права ім. В.М. Корецького НАН України, 2011. 448 с.
5. Державне управління: європейські стандарти, досвід та адміністративне право / В.Б. Авер'янов, В.А. Дерець, А.М. Школик та ін. ; за заг. ред. В.Б. Авер'янова. Київ : Юстініан, 2007. 288 с.
6. Біла В.Р. Особливості адміністративно-договірних відносин за участю органів Державної податкової служби. Радник: укр. юрид. портал. URL: http://radnuk.info/pidrychnuku/admin-pravo/493-stetsenko/213992012-06-19-22-07-49.html.
7. Концепція розвитку системи надання адміністративних послуг органами виконавчої влади, схвалена розпорядженням Кабінету Міністрів України від 15 лютого 2006 року № 90-р. URL: http://zakon.rada.gov.ua/laws/show/90-2006-%D1%80.
8. Задихайло О.А. Правове регулювання надання адміністративних послуг в Україні. *Форум права*. 2011. № 1. С. 379–384.
9. Світличний О.П. Адміністративні правовідносини у сфері земельних ресурсів України : автореф. дис. ... д-ра юрид. наук : 12.00.07 / Світличний О.П. ; Держ. НДІ М-ва внутр. справ України. Київ, 2012. 35 с.
10. Дрозд О.Ю. Безконтактні адміністративні послуги державної служби України з питань геодезії, картографії та кадастру: питання теорії та практики : монографія / О.Ю. Дрозд, О.В. Левченко ; НДІ публ. права. Київ, 2016. 199 с.;
11. Гладкова Є.О. Адміністративно-правове регулювання земельних відносин в Україні: стан та перспективи розвитку. *Європейські перспективи.* 2014. № 6. С. 74–80.
12. Козаченко Н.М. Система надання публічних послуг у сфері земельних відносин в Україні: становлення та трансформації. *Державне управління та місцеве самоврядування.* 2012. Вип. 4 (15). С. 236–243.
13. Державне управління: Європейські стандарти, досвід та адміністративне право / В.Б. Авер'янов, В.А. Дерець, А.М. Школик та ін. ; за заг. ред. В.Б. Авер'янова. Київ : Юстініан, 2007. 288 с.
14. Державне управління: проблеми адміністративно-правової теорії та практики / за заг. ред. В.Б. Авер'янова. Київ : Факт, 2003. 384 с.
15. Закон України «Про Кабінет Міністрів України» від 7 жовтня 2010 р. № 2591-VI. URL: http://zakon.rada.gov.ua/laws/show/794-18.
16. Кодекс адміністративного судочинства України від 6 липня 2005 року, № 2747-IV. URL: http://zakon.rada.gov.ua/laws/show/2747-15.
17. Закон України «Про адміністративні послуги» від 06.09.2012 р. № 5203-VI. URL: http://zakon.rada.gov.ua/laws/show/5203-17.
18. Земельний кодекс України від 25 жовтня 2001 року, № 2768-III. URL: http://zakon.rada.gov.ua/laws/show/2768-14.
19. Бусуёк Д.В. Методологические подходы к исследованию и усовершенствованию правового регулирования управленческой и сервисной деятельности органов исполнительной власти в сфере использования и охраны земель в Украине. *Право.* 2013. № 1 (21) 2013. С. 119–123.
20. Бусуйок Д.В. Правове регулювання управлінських і сервісних відносин у сфері використання та охорони земель – актуальні напрями удосконалення правового регулювання земельних відносин. *Альманах права. Правовий світогляд: людина і право.* Київ, 2014. Вип 5. С. 389–393.

УДК 340; 316.324.8:004(477)

ЗАРУБІЖНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

FOREIGN EXPERIENCE IN PROVIDING INFORMATION SECURITY OF STATE

Шемчук В.В.,
кандидат юридичних наук, заслужений юрист України,
доцент кафедри конституційного та міжнародного права
Навчально-наукового гуманітарного інституту
Таврійського національного університету імені В.І. Вернадського

Стаття присвячена вивченню зарубіжного досвіду у сфері забезпечення інформаційної безпеки. Вказана проблематика є актуальною і для України, оскільки останнім часом тут інформаційна сфера перетворилась на арену протиборства, держава-агресор використовує нові інформаційні технології впливу на свідомість громадян, розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом, посягання на суверенітет і територіальну цілісність України. З метою протидії таким проявам варто вивчати відповідний позитивний досвід інших країн у цій сфері.

Так, розглянуто базові акти у сфері інформаційної безпеки Франції, зокрема, Білі книги оборони та національної безпеки. Розглянуто основні акти у сфері інформаційної безпеки Франції. Французька система інформаційної безпеки є складовою частиною національної безпеки, і, відповідно, її основні принципи передбачені в Білих книгах Міністерства оборони і національної безпеки. На цей час таких налічується п'ять, останній з яких – Огляд стратегії оборони та національної безпеки – прийнято 2017 р. Тут значна увага приділена загрозам інформації, атакам у кіберпросторі тощо. У зв'язку з цим визначено, що армія повинна повністю планувати і здійснювати операції в цифровому світі, а на тактичному рівні проводити активні операції. Це стосується і виконання військових дій в кіберпросторі, проти держави супротивниці.

Для Франції характерним є так званий «кіберджихадізм», який передбачає використання інтернет-технологій і послуг, особливо соціальних мереж, у сприянні джихаду насильства, залишаючись серйозною загрозою для її інформаційного простору.

Система інформаційної безпеки у Франції складається з таких спеціальних суб'єктів: Національне агентство безпеки інформаційних систем (ANSSI), Служба аудіовізуальних матеріалів, Міжвідомчий директорат з питань інформаційних систем та зв'язку (DISIC), Директорат з розвитку засобів масової інформації (DDM) та деякі інші.

Основний закон в галузі інформаційної безпеки в Німеччині – Закон «Про посилення безпеки систем інформаційних технологій» (Закон про безпеку ІТ) від 25.07.2015 р. Закон відводить Федеральному відомству з безпеки в сфері інформаційних технологій (BSI) центральну роль в захисті критично важливих інфраструктур в Німеччині. Загалом забезпечення інформаційної безпеки Німеччини здійснюється Федеральними збройними силами Німеччини (Бундесвером), зокрема, відділом інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки.

Основними тенденціями забезпечення інформаційної безпеки цих країн є збільшення бюджету, розширення штату, технологічне лідерство та міжнародне співробітництво.

Ключові слова: Біла книга, інформаційна безпека, кіберджихадізм, ANSSI, кіберпростір.

The article is devoted to the experience of France and Germany in providing information security. Basic acts in the field of information security of France are considered. France's information security system is a component of national security, and, accordingly, its basic principles are laid down in the White Papers of Defense and National Security.

There are currently five White Papers in France, the latter being adopted in 2017 under the name of the Strategic Defense Review and National Security 2017. In the Defense Review, considerable attention is paid to information threats and countermeasures. So, it is noted that in cyberspace, some attacks, due to their scale and severity, can be classified as armed aggression. In connection with this, it is noted that the Army must fully plan and conduct operations in digital space up to the tactical level in the chain of planning and conducting kinetic operations. It is also possible to carry out hostilities in cyberspace, which means defensive or offensive struggle throughout the digital environment, against state or non-state opponents.

The national security strategies outlined in the White Papers are the basis of the Laws on Military Planning.

For France, the so-called "cyberjikhadism", which consists in the use of Internet technologies and services, especially social networks, in promoting jihadism of violence, remains a serious threat to its information space.

The information security system in France consists of the following special actors: National Information Security Agency (ANSSI), Audiovisual Service (Service audiovisual), Interdepartmental Directorate for Information Systems and Communications (DISIC), the Directorate for Media Development (DDM) and some others.

The basic law in the field of information security in Germany is the Law "On Enhancement of Security of Information Technology Systems" (IT Security Law) of 25.07.2015. The law gives the federal agency for security information technology (BSI) a central role in protecting critical infrastructure in Germany.

Germany's information security is also provided by the Federal Armed Forces of Germany (Bundeswehr), in particular the Department of Information and Computer Network Operations of the Strategic Intelligence Command.

Key words: White Paper, information security, cyberjikhadism, ANSSI, cyberspace.

Постановка проблеми. За останнє десятиліття комп'ютерні атаки з боку державних і недержавних суб'єктів різко активізувалися, що свідчить про зростаюче поширення і витонченість засобів агресії. Держави вносять безпосередній внесок в ці події шляхом поширення кібернетичної зброї, яка, як відомо, може бути вивчена, перероблена і повторно використана. Вони також роблять непрямий внесок, надаючи свої території для центрів здійснення атак або розвитку засобів цих атак.

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [1].

Отже, в умовах триваючої агресії з боку РФ та стрімкого розвитку інформаційних відносин є нагальна потреба в сучасному і ефективному законодавчому регулюванні інформаційної безпеки особи, українського суспільства та держави. Таке законодавство має засновуватися на позитивному міжнародному досвіді, тому актуальним є ознайомлення з нормативно-правовим регулюванням інформаційної безпеки зарубіжних країн.

Мета статті полягає у вивченні зарубіжного досвіду, зокрема, на прикладі таких держав, як Франція та Німеччина, щодо забезпечення інформаційної безпеки.

Аналіз досліджень та публікацій свідчить про незначну кількість праць, присвячених вивченню зарубіжного досвіду регулювання інформаційної безпеки. Можна виокремити роботи таких вчених, як І. Бережнюк, О. Береза, М. Дмитренко, М. Желіховський, Н. Камінська, Б. Кормич, Я. Малик, В. Ліпкан, В. Марков, Є. Максименко, І. Несторишен, І. Чернухін та інших.

Виклад основного матеріалу. Система інформаційної безпеки Франції є складником національної безпеки, відповідно, основні її принципи закладені у Білих книгах оборони та національної безпеки.

Перша Біла книга з національної оборони була опублікована у 1972 році, у ній викладені принципи оборонної політики Франції та основи стратегії ядерного стримування. Опублікована у 1994 році друга Біла книга була присвячена закінченню «холодної війни» і перенаправленню збройних сил на військові операції за межами національної території, що призвело до професіоналізації збройних сил.

Процес глобалізації та боротьба з тероризмом зумовили розроблення нової концепції стратегії національної безпеки, яка об'єднує, не заважаючи їм, оборонну політику, політику внутрішньої безпеки, зовнішню політику та економічну політику. Ця концепція була закріплена у третій Білій книзі оборони та національної безпеки від 2008 року.

Такий новий підхід до формування стратегії національної безпеки Франції, що характеризується розширенням стратегічного мислення, окрім оборонних причин, був зумовлений глобалізацією, яка глибоко трансформує саму основу міжнародної системи, що стає більш нестабільною і непередбачуваною, ніж під час холодної війни, і породжує нові загрози абсолютно різної природи. З 2009 року ця концепція була включена до Оборонного кодексу Франції.

Особливістю Білої книги оборони та національної безпеки від 2008 року також є те, що у ній названі загрози, пов'язані з використанням інформаційних систем та засобів інформаційного впливу. Так, характеризуючи загрозу масштабних атак на інформаційні системи, зазначається, що останні пронизують основні системоутворювальні ланки економічної та суспільної життєдіяльності. Зокрема, залежність від інформаційних систем інженерних комунікацій, транспортної інфраструктури, продовольчого забезпечення і навіть управління обороною, робить сучасне суспільство та його безпеку вразливими до випадкових пошкоджень та цілеспрямованих атак, які здійснюються через обчислювальні мережі. Загроза шпіонажу та стратегічного впливу обґрунтовується поширенням застосування у міждержавних відносинах засобів «м'якої сили», маніпулюванням свідомістю через ЗМІ та Інтернет, посяганнями на науковий, економічний, оборонний потенціал Франції та її території, небезпекою культурної експансії [2].

Четверта Біла книга опублікована в 2013 році під головуванням Франсуа Олланда. П'ятий документ під трохи іншою назвою («Стратегічний оборонний огляд та національна безпека» (далі – Оборонний огляд)) опубліковано в кінці 2017 року під головуванням Еммануїла Макрона.

В Оборонному огляді значна увага приділяється інформаційним загрозам та заходам протидії ним. Так, зазначається, що у кіберпросторі деякі напади через їх масштаби і серйозність можуть бути віднесені до категорії збройної агресії. Труднощі з розподілом акцій і поєднання прямих дій з методами впливу і пропаганди уможливлюють безліч сценаріїв інструменталізації з метою дестабілізації або підтримки простіших операцій. Облік кіберзагроз та їх еволюції тим складніший, що він не може обмежуватися периметром оборони через заплутування питань і участі державних і приватних суб'єктів. У зв'язку з цим наголошується, що армії повинні повністю планувати і проводити

операції в цифровому просторі аж до тактичного рівня в ланцюжку планування і проведення кінетичних операцій. Операції в цифровому просторі розширюють діапазон традиційних ефектів, доступних політичній владі, і використовують зростаюче оцифрування опонентів Франції, як державних, так і недержавних. Ця здатність вимагає посилених і досить гнучких людських ресурсів, а також постійної розробки конкретних технічних рішень [3].

Крім того, для забезпечення інформаційної безпеки в Оборонному огляді допускається проведення бойових дій в кіберпросторі, що означає оборонну або наступальну боротьбу по всьому цифровому середовищу проти державних або недержавних супротивників.

Стратегії національної безпеки, викладені у Білих книгах, покладаються в основу Законів про військове планування. Сьогодні чинним є Закон Франції «Про військове планування на період з 2019 по 2025 рік та інші положення, що стосуються оборони» № 2018-607 від 13.07.2018.

Для Франції серйозною загрозою її інформаційному простору залишається так званий «кіберджихадизм», який полягає у застосуванні Інтернет-технологій та послуг, особливо соціальних мереж, в просуванні джихадизм насильства. Він здійснюється шляхом злому урядових сайтів, корпоративних сайтів або організацій, пропаганди і вербування. Заходами протидії йому виступають: блокування сайтів та акаунтів, створення контрпропагандистських сайтів тощо.

Система забезпечення інформаційної безпеки Франції складається з таких спеціальних суб'єктів: Національне агентство безпеки інформаційних систем (Agence nationale de la securite des systemes d'information, ANSSI), Служба аудіовізуальних матеріалів (Service audiovisuel), Міжвідомчий директорат з питань інформаційних систем та зв'язку (Direction interministerielle des systemes d'information et de communication, DISIC), Директорат з розвитку засобів масової інформації (Direction du developpement des medias, DDM) та деякі інші.

Національне агенство безпеки інформаційних систем (Agence nationale de la securite des systemes d'information, ANSSI) – французька служба з національною компетенцією, створена декретом в липні 2009 року, підпорядковується Генеральному секретаріату оборони та національної безпеки (Secretariat general de la defense et de la securite nationale, SGDSN), який відповідає за надання Прем'єр-міністру допомоги у виконанні його обов'язків у сфері оборони та національної безпеки, зокрема інформаційної. ANSSI замінило Центральне управління інформаційної безпеки, що було створене декретом в липні 2001 року. Її бюджет становить 80 мільйонів євро, а штат складається з 600 агентів.

ANSSI відповідає за просування технологій, систем і національного досвіду з метою сприяння впровадженню цифрової економіки. Водночас основні зусилля фахівців ANSSI спрямовані на реалізацію заходів, викладених у національній стратегії безпеки та оборони. Основними цілями агентства є: підвищення ефективності управління та координації діяльності органів державної влади, суб'єктів критичної інфраструктури, суспільства в умовах інформатизації; забезпечення промислової безпеки; організація захисту національної інформаційно-телекомунікаційної інфраструктури в умовах військової загрози, в тому числі кібервійни; підтримка технічних засобів, необхідних для виконання покладених на агентство завдань, в актуальному стані. До його повноважень належать:

– формування державної політики у сфері оборони та безпеки інформаційних систем;

– розробка організаційно-правових та технічних заходів захисту державних інформаційних систем та контроль за їх виконанням;

– моніторинг, виявлення, оповіщення і реагування на кібератаки, спрямовані на державні інформаційно-телекомунікаційні системи;

– виявлення і реагування на вірусні атаки, реалізація адаптаційних механізмів захисту від них;

– запобігання загрозам через сприяння розробці програмного забезпечення та засобів обчислювальної техніки, яким можна довіряти;

– консультативна функція і підтримка суб'єктів критичної інфраструктури;

– систематичне інформування громадськості про загрози, зокрема, через урядовий вебпортал з питань ІБ;

– розробка і придбання основних продуктів, призначених для захисту найбільш чутливих ділянок міжвідомчої державної мережі;

– реалізація засобів контролю управління і зв'язку з питань оборони і національної безпеки;

– сертифікація комплексних систем захисту інформації [2; 4].

Прикметно, що ANSSI є спадкоємцем цілого ряду організацій, спочатку створених з військової точки зору, які відповідали за забезпечення безпеки конфіденційної інформації держави, а саме: Технічний відділ шифрування (створений в Алжирі, 1943 р.); Центральна технічна служба шифрування (в Парижі, 1951 р.); Центральна служба безпеки телекомунікацій (1977 р.); Національна служба безпеки інформаційних систем (1986 р.); Центральне управління комп'ютерної безпеки (2001 р.).

У реалізації інформаційної політики Франції бере участь і Служба аудіовізуальних матеріалів (Service audiovisuel), яка діє при канцелярії Президента. Служба проектує аудіовізуальні технічні платформи Президента Республіки, організовує його виступи та забезпечує їх трансляцію по всій території країни і за кордоном.

Крім того, вказана Служба веде фотографічний блок щодо діяльності Президента та життя Єлисейського палацу, керує банком фотографій та взаємодіє зі ЗМІ та громадськістю. Важливою функцією цієї Служби є аудіовізуальний моніторинг ЗМІ та формування відповідного архіву матеріалів. Загалом її діяльність спрямована на формування іміджу Президента.

З огляду на активну інформатизацію діяльності органів державної влади у складі Генерального секретаріату уряду (le Secretariat general du gouvemement, SGG), що підпорядковується Прем'єр-міністру, на початку 2011 року (Декрет № 2022-193 від 21.02.2011) було створено Міжвідомчий директорат з питань інформаційних систем та зв'язку (Direction interministerielle des systemes d'information et de communication, DISIC). Він відповідає за функціонування інформаційно-телекомунікаційних систем, призначених для обміну інформацією між різними відомствами та з громадянами. Основними завданнями підрозділу є: проектування інформаційно-телекомунікаційної інфраструктури уряду з урахуванням потреб діяльності та оптимізації ресурсів, організація закупівлі обладнання, програмного забезпечення та інформаційних послуг, розподіл електронно-обчислювальної техніки між міністерствами, впровадження нових інформаційних систем, забезпечення стратегічного планування розвитку інформаційної інфраструктури.

Метою створення DISIC є моніторинг тенденцій у галузі інформаційних технологій, оптимальне використання інформаційних ресурсів завдяки спільним банкам даних, запобігання ризикам безпеки інформації, пов'язаним із впровадженням масштабних проектів, підвищення обслуговування користувачів інформаційних систем [2].

Базовим законом у сфері інформаційної безпеки Німеччини є Закон «Про посилення безпеки систем

інформаційних технологій» (Закон про безпеку IT) від 25.07.2015. Закон відводить Федеральному відомству з безпеки в сфері інформаційних технологій (BSI) центральну роль в захисті критично важливих інфраструктур у Німеччині. При цьому під критичними інфраструктурами розуміються об'єкти, установки або їх частини, які належать до секторів енергетики, інформаційних технологій і телекомунікацій, транспорту і дорожнього руху, охорони здоров'я, водопостачання, харчування, фінансів і страхування. Такі об'єкти мають велике значення для функціонування спільноти, тому що їх зупинка або погіршення роботи призведе до значного дефіциту поставок або створить загрози громадській безпеці.

27 березня 2019 Федеральне міністерство внутрішніх справ також опублікувало проект закону про безпеку інформаційних технологій, в якому міститься цілісний підхід до безпеки вказаної сфери. Крім іншого, передбачається запровадження зручного для споживача ярлика IT-безпеки для комерційних продуктів, а також посилення компетенції BSI і розширення переліку правопорушень у сфері кібербезпеки і пов'язаних з ними слідчих дій. Законопроект також збільшує кількість адресатів звітності та зобов'язань. Загалом закон, як очікується, створить певні економічні складнощі для компаній і органів державної влади [5].

Забезпечення інформаційної безпеки Німеччини здійснюється Федеральними збройними силами Німеччини (Бундесвером), зокрема, відділом інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки.

Командування стратегічної розвідки також здійснює управління супутниковою розвідувальною системою SAR-Lupe, яка була запущена в грудні 2008 р. За допомогою п'яти супутників система SAR-Lupe, яка вважається однією з найдосконаліших систем у своєму роді, може передавати зображення з роздільною здатністю менше одного метра не залежно від денного світла і погоди. Таким чином, можна пояснити майже будь-яку точку на землі. Система збирає й оцінює інформацію про військово-політичну ситуацію в окремих країнах і альянсах потенційного або фактичного противника і його збройних сил.

Суттєве значення для забезпечення інформаційної безпеки має і супутникова система зв'язку Бундесверу SATCOMBw, яка розпочала свою роботу з жовтня 2009 р. Вона включає роботу супутників, які покривають східну і західну півкулі планети, організують нові та безпечні канали зв'язку.

Висновки. Система забезпечення інформаційної безпеки Франції та Німеччини ґрунтується на усвідомленні ризиків і загроз, які зумовлюються швидким розвитком інформаційних та комунікаційних технологій. Тому політика цих країни у вказаній сфері є послідовною, засновується на компетентних оцінках та стратегіях, спрямована на професійну підготовку кадрів та розвиток технологій. Так, одним з головних суб'єктів системи забезпечення інформаційної безпеки Франції є Національне агентство безпеки інформаційних систем (ANSSI), у Німеччині – відділ інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки Бундесверу. Основними тенденціями у їх роботі є збільшення бюджету, розширення штату, технологічне лідерство та міжнародне співробітництво.

Вважаємо, що позитивний досвід проаналізованих нами держав може бути корисним для України, практики забезпечення інформаційної безпеки в сучасних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Доктрина інформаційної безпеки України: Затверджена указом Президента України від 25 лютого 2017 року № 47/2017. Київ : *Офіційний вісник України*, 2017. № 20.

2. Забезпечення інформаційної безпеки держави : підручник / за заг. ред. О.А. Семченка та В.М. Петрика. Київ : ДНУ «Книжкова палата України», 2015. 672 с.

3. Revue stratégique: une analyse lucide et volontariste pour préparer la prochaine loi de programmation militaire. 2017. URL: https://www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.

4. Décret № 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information». URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte= JORFTEXT000020828212&dateTexte= &categorieLien=id.

5. IT-Sicherheitsgesetz (IT-SiG) 2.0 – die wichtigsten Änderungen des Referentenentwurfs im Schnellüberblick. Beck-community. Abgerufen am 3. April 2019. URL: https://community.beck.de/2019/04/03/it-sicherheitsgesetz-it-sig-20-die-wichtigsten-aenderungen-des-referentenentwurfs-im-schnellueberblick.

6. Камінська Н.В. Міжнародна інформаційна безпека в умовах глобалізації та інтеграції. *Міжнародне право: виклики сьогодення* : матер. міжнар. науково-практ. інтернет-конфер. (Київ, 20 грудня 2016 р.) Київ : КНТЕУ, 2016. С. 22–27.