11. Про внесення змін і доповнень до деяких законодавчих актів України у зв'язку з прийняттям Закону України "Про обіг в Україні наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів" та Закону України "Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними": Закон України від 15 лют. 1995 р. № 64/95-ВР // Відомості Верховної Ради України. – 1995. – № 10. – Ст. 64.

12. Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, від 8 листоп. 1990 р. // Офіц. вісн. України. –1998. – № 13. – С. 304.

13. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму: Закон України від 28 листоп. 2002 р. № 249-IV // Відомості Верховної Ради України. – 2003. – № 1. – Ст. 2.

14. Про внесення змін до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму": Закон України від 18 трав. 2010 р. № 2258-VI // Відомості Верховної Ради України. – 2010. – № 29. – Ст. 392.

15. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдженню зброї масового знищення: Закон України від 14.10.2014 № 1702-VII // Голос України. – 2014. – № 216.

16. Алиев В.М. Теоретические основы и прикладные проблемы борьбы с легализацией (отмыванием) доходов, полученных незаконным путем: автореф. дисс. на соискание ученой степени д-ра юрид. наук: спец. 12.00.08 "Уголовное право и криминология; уголовно-исполнительное право" / В.М. Алиев. – М., 2001. – 52 с.

Павлютін Ю.М.,
здобувач кафедри адміністративного
права та процесу ОДУВС
Надійшла до редакції: 18.05.2015

УДК 343.26

ОКРЕМІ ПИТАННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Демедюк С. В.

У статті на основі вивчення досвіду провідних країн проводиться дослідження сучасних тенденцій у сфері адміністративно-правового та організаційного забезпечення кібербезпеки. Акцентується увага на тому, що створення дієвого механізму адміністративно-правового регулювання та організації кібербезпеки в Україні є основним пріоритетом розвитку національної безпеки.

***Ключові слова**: кібербезпека, кіберзлочинність, кіберпростір, національна безпека, адміністративно-правове регулювання, протидія кіберзлочинності, нормативно-правовий акт.*

В статье на основе изучения опыта ведущих стран проводится исследование современных тенденций в сфере административно-правового и организационного обеспечения кибербезопасности. Акцентируется внимание на том, что создание действенного механизма административно-правового регулирования и организации кибербезопасности в Украине является основным приоритетом развития национальной безопасности.

***Ключевые слова**: кибербезопасность, киберпреступность, киберпространство, национальная безопасность, административно-правовое регулирование, противодействие киберпреступности, нормативно-правовой акт.*

On the basis of studying the experience of leading countries is to study modern trends in the field of administrative-legal and organizational support of cyber security. The attention that the creation of an effective mechanism of administrative and legal regulation of cyber security and organizations in Ukraine is the main priority of national security.

Keywords: cyber security, cybercrime, cyberspace, national security, administrative and legal regulation, combating cybercrime legal act.

На сьогодні проблема забезпечення кібербезпеки набула великого значення не лише в країні, а й у всьому світі. Швидкий розвиток нових технологій спонукав до не менш швидкої появи нових форм кіберзлочинності, які отримують поширення при використанні нових методів, наприклад, технології Bluetooth, бездротових мереж зв'язку Wi-Fi та WiMAX, пірингових мереж (P2P), спаму тощо [1]. А отже, захист правовідносин, законних прав та інтересів людини й громадянина, підприємств, суспільства та держави у сфері кіберпростору є досить актуальною проблемою для системи національної безпеки кожної країни світу.

За своєю сутністю кіберзлочини є транскордонними, і тому міжнародні організації закликають держави до співпраці з іншими зацікавленими сторонами розробляти дієві механізми адміністративно-правового регулювання у сфері кібербезпеки, що передбачає не лише розроблення та прийняття необхідного законодавства, а й проведення спільних розслідувань зазначених діянь з використанням існуючого міжнародного права й, зокрема, Конвенції Ради Європи з кіберзлочинності.

Міжнародні організації визнають небезпеку кіберзлочинності та її трансграничний характер, обмеженість одностороннього підходу до вирішення цієї проблеми й необхідність міжнародної співпраці як у вжитті необхідних технічних заходів, так і у виробленні міжнародного законодавства. У координації міжнародних зусиль, побудові міжнародної співпраці в боротьбі зі злочинами у сфері високих технологій важливу роль відіграють такі міжнародні організації, як Рада Європи, Європейський союз, ООН і Інтерпол та ін. [2].

Питання адміністративно-правового регулювання забезпечення та кібербезпеки набуває особливої актуальності в умовах інтеграції міжнародних фінансових ринків у площині кіберпростору, зростання швидкості банківських розрахунків і значного поширення швидких інтернет-розрахунків тощо.

Питання дослідження світового досвіду забезпечення кібербезпеки не є новим, воно активно розглядається науковцями, які займаються дослідженням проблеми протидії кіберзлочинності: О.А. Баранов, Ю.М. Батурин,

М.М. Безкоровайний, П.Д. Біленчук, В.М. Бутузов, В. Голубєв, М.В. Грайворонський, Д.В. Дубов, А.М. Жодзишский, О.Є. Користін, М.О. Кравцова, І.Л. Курносов, О.С. Лєнков, С.В. Мельник, О.В. Орлов, Ю.М. Онищенко, В.М. Панченко, Ю.М. Супрунов, А.Л. Татузов, О.О. Тихомиров, І.Г. Чекунов, В.М. Фурашев, В.П. Шеломенцев, І.Б. Яковів та інші. Однак питанням адміністративно-правового регулювання забезпечення та організації кібербезпеки достатньої уваги не приділялося.

Ураховуючи сучасні тенденції у сфері адміністративно-правового та організаційного забезпечення кібербезпеки на міжнародній арені протидії загрозам у кіберпросторі та зміни внутрішньої кібернетичної політики національної безпеки провідних держав світу, а також посилення механізмів і компонентів кібербезпеки, більшість країн світу активно модернізують власні сектори безпеки відповідно до викликів сучасності, особливо зважаючи на потенціал використання кіберпростору в злочинних намірах.

Цей процес відбувається завдяки розробці та затвердженню нормативно-правових документів у вигляді концепцій, норми яких повинні забезпечити цілісність механізмів адміністративно-правового й організаційного забезпечення кібербезпеки та державної політики в цій сфері. Так, на сьогодні Стратегії забезпечення кібернетичної безпеки було розроблено багатьма провідними країнами, зокрема: США, Францією, Німеччиною, Голландією, Великою Британією, Естонією, Фінляндією, Словаччиною, Чехією, Литвою, Люксембургом, Індією, Австралією, Новою Зеландією, Колумбією, Канадою, Японією. У процесі завершення розробки відповідних нормативно-правових актів у сфері забезпечення кібербезпеки знаходяться деякі країни Євросоюзу [3].

З 1985 р. по 1989 р. Спеціальний Комітет експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами, виробив Рекомендацію № 89, затверджену комітетом Міністрів ЄС 13 вересня 1989 р., норми якої містять список правопорушень, рекомендований країнам-учасницям ЄС для розробки єдиної стратегії, пов'язаної з комп'ютерними злочинами [4]. Крім того, у Рекомендації відмічено необхідність досягнення міжнародного консенсусу з питань криміналізації деяких кіберзлочинів, пов'язаних з комп'ютерами. У Рекомендації зроблено першу на міжнародному рівні спробу класифікації кіберзлочинів, які поділено на два списки: мінімальний (включає діяння, які обов'язково мають бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку) та додатковий (значаться ті правопорушення, щодо яких досягнення міжнародної згоди уявляється скрутним) [4].

У 1990 р. VIII Конгрес ООН з попередження злочинності й поводження з правопорушниками ухвалив резолюцію, норми якої закликають держави-члени ООН до збільшення зусиль щодо боротьби з комп'ютерною злочинністю; модернізації національного законодавства; сприяння розвитку в майбутньому міжнародних принципів і стандартів запобігання, судового переслідування і покарання у сфері комп'ютерної злочинності [5]. 14 грудня 1990 р. Генеральною Асамблеєю ООН було ухвалено Резолюцію, що закликає уряди держав-членів керуватися рішеннями, прийнятими на VIII Конгресі ООН.

У 1995 р. в Ліоні (Франція) було проведено міжнародну конференцію Інтерполу з комп'ютерної злочинності, учасниками якої було висловлено тривогу щодо відсутності міжнародного механізму для раціонального й ефективного протистояння кіберзлочинності. За підсумками конференції було зроблено висновок, що в більшості країн світу спостерігається все зростаюче використання інформаційних технологій у кримінальній діяльності, що викликає необхідність постійного вивчення, оскільки розвиток ІКТ призводить до використання цих інновацій при скоєні комп'ютерних злочинів [6].

У 1997 р. на зустрічі у Вашингтоні міністрами внутрішніх справ і міністрами юстиції Великої Вісімки було прийнято «Десять принципів боротьби з високотехнологічними злочинами», норми яких включають також і положення про те, що «для тих, хто зловживає інформаційними технологіями, не повинно бути ніяких зон безпеки». У документі зазначено, що правова система повинна забезпечити захист конфіденційності, цілісності й придатності даних і систем від протиправного ушкодження та гарантувати покарання за серйозні правопорушення [7].

Досвід адміністративно-правового регулювання забезпечення й організації кібербезпеки в країнах ЄС доводить, що безконтрольне використання можливостей кіберпростору надає можливість різним деструктивним силам здійснювати кіберзагрози та небезпеки. При цьому одне з найбільш серйозних обмежень національного законодавства про комп'ютерні злочини полягає в тому, що воно не дозволяє ефективно боротися з глобальним явищем кіберзлочинності. Для вирішення цієї проблеми було розроблено Європейську конвенцію про кіберзлочинність, прийняту Комітетом міністрів Ради Європи 23 листопада 2001 р. Конвенцію підписали 46 країн, зокрема 38 країн-держав Ради ЄС, а також Канада, Японія, Південна Африканська республіка і США; ратифіковано 24 країнами, зокрема й Україною [8]. До країн, що не підписали конвенцію, увійшли Китай, кілька латиноамериканських держав і Росія.

Конвенція про кіберзлочинність – один з найважливіших документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі і доки єдиний документ такого рівня. Прийняття його – це своєрідна віха в історії боротьби з кіберзлочинністю. Нормами зазначеної конвенції охоплено широке коло питань, зокрема різні аспекти кіберзагроз та кіберзлочинності (незаконний доступ до комп'ютерних систем і перехоплення даних, вплив на дані, на роботу системи, протизаконне використання пристроїв, підроблення та шахрайство з використанням комп'ютерних технологій, правопорушення, пов'язані з дитячою порнографією і тероризмом) [9].

На сьогодні Конвенція про кіберзлочинність є одним з базових документів у сфері забезпечення кібербезпеки, однак і цей документ не позбавлений недоліків, на які вказували чисельні міжнародні організації, якими було підписано протест проти прийняття Конвенції Ради Європи про кіберзлочинність, у якому зазначалося, що Конвенція несе в собі загрозу для норм захисту особи, що встановилися, невиправдано розширює поліцейські функції уряду, а також знижує відповідальність держави в правоохоронній діяльності.

Звичайно, єдиним критерієм ефективності Конвенції, так само як і справедливості заперечень критично налагоджених опонентів, є практика застосування положень цього нормативно-правового акта. Однак на сьогодні слід констатувати, що прийнята Конвенція Ради Європи про кіберзлочинність слугує фундаментом для міжнародного законодавства у сфері забезпечення кібербезпеки [9].

Норми Конвенції Ради Європи про кіберзлочинність

деталізовано в нормативно-правових актах національного законодавства у сфері забезпечення кібербезпеки різних держав.

У 2001 р. після трагічних подій 11 вересня урядом США було прийнято Закон «Про об'єднання та зміцнення США», відповідно до норм якого будь-яка дія, що веде до порушення в роботі або незаконного проникнення в комп'ютер, класифікується як тероризм, а провайдер зобов'язаний надати всю відому йому інформацію про користувача на першу вимогу ФБР [10]. У нормах Національної стратегії внутрішньої безпеки США 2007 р. передбачено відповідний розділ «Захист урядового і приватного секторів Інтернету в США», нормами якого наголошується на необхідності захисту від кібератак на теренах кіберпростору. Як зазначають деякі фахівці, прийняття цієї стратегії зміцнило позиції прихильників загального спостереження за електронними комунікаціями. У квітні 2009 р. у Конгрес США було представлено проект нового закону «Акт про кібербезпеку, 2009» (Cybersecurity Act of 2009), розробленого Національною розвідкою США. Нормами законопроекту запропоновано значно розширити повноваження федеральної влади у сфері забезпечення кібербезпеки, а крім того, передбачено обов'язкову ідентифікацію користувачів кіберпростору в інтересах національної безпеки. Проект нового закону може встановити стандарти комп'ютерної безпеки, працювати відповідно до яких будуть зобов'язані як урядові організації, так і приватні компанії, що контролюють функціонування критично важливої інфраструктури [11]. Якщо законопроект буде схвалено, то уряд США зможе на законних підставах перевіряти вміст електронного листа, усі передані файли, а також пошукові запити всіх користувачів кіберпростору [12].

Серед країн заходу Велика Британія одна з перших, яка в 1990 р. прийняла Закон «Про неправомірне використання комп'ютерних технологій» (Computer Misuse Act), норми якого було безпосередньо спрямовано на забезпечення кібербезпеки. Однак можливості застосування зазначеного нормативно-правового акту в кібернетичній сфері було серйозно обмежено. У зв'язку із чим у 2006 р. було прийнято Закон Великої Британії «Про поліцію та юстиції», норми якого направлено на регулювання широкого кола проблем у сфері забезпечення кібербезпеки. Крім того, закон містить поправки до попереднього закону, зокрема, було значно збільшено терміни тюремного ув'язнення за правопорушення у сфері кіберпростору.

Механізм адміністративно-правового регулювання забезпечення та організації кібербезпеки в Німеччині містить значну кількість нормативно-правових актів, які передбачають відповідальність та суворе покарання за різні правопорушення в кіберпросторі. При всій прихильності Німеччини до демократичних цінностей, урядом країни приділяється велика увага питанням контролю над використанням кіберпростору. При цьому багато законодавчих обмежень вводяться при значному опорі з боку громадськості, ЗМІ та компаній, які працюють у сфері комп'ютерних і мережевих технологій.

Досліджуючи організаційні та нормативно-правові засади боротьби із кіберзлочинністю, О.В. Орлов і Ю.М. Онищенко зазначають, що зарубіжний досвід переконливо свідчить, що орієнтація тільки на технічні засоби забезпечення кібербезпеки в умовах інформатизації суспільства, зокрема профілактики боротьби з кіберзлочинами, не досягла значних успіхів [2]. Це значною мірою призвело до підвищення рівня адміністративно-правового регулювання забезпечення та організації кібербезпеки в зарубіжних країнах.

У квітні 2008 р. міністрами ЄС було прийнято рішення про посилення Закону «Про боротьбу з тероризмом». Згідно з новими поправками злочином стало вважатися будь-яке публічне спонукання до терористичної діяльності, у тому числі пропаганда тероризму в мережі Інтернет, а також вербування та тренування терористів за допомогою інтернет-сайтів. З точки зору фахівців ЄС, внесені поправки до Закону «Про боротьбу з тероризмом» стали істотним поліпшенням законодавства ЄС у сфері забезпечення кібербезпеки, оскільки кіберпростір є сучасним потужним інструментом впливу. Крім того, відповідно до норм закону судову систему ЄС наділили правом вимагати закриття екстремістських сайтів [13].

Якщо звернутися до досвіду адміністративно-правового регулювання забезпечення та організації кібербезпеки в країнах Азії, насамперед слід зазначити, що одним із найпотужніших механізмів правового та організаційного забезпечення кібербезпеки є Китайська система контролю Інтернету. На сьогодні саме китайська система адміністративно-правового регулювання забезпечення кібербезпеки є складним, комплексним і дуже ефективним механізмом, загальною метою якого є захист національної безпеки й суспільних інтересів. Ці складні заходи адміністративно-правового регулювання забезпечення кібербезпеки, що проводяться китайською владою, отримали загальну назву «Great Firewall of China», загальною метою яких є очищення від шкідливого порнографічного та антиурядового змісту, пропаганди нелегальних громадських організацій та їх діяльності.

Слід зазначити, що активному створенню механізмів адміністративно-правового та організаційного забезпечення кібербезпеки в зарубіжних країнах сприяє створення та реформування систем управління відповідним сектором безпеки, до яких слід віднести створення спеціалізованих підрозділів та управлінських структур у сфері кібербезпеки, наприклад: U.S. Cyber Command (США), Cyber Security Operations Centre (Велика Британія), Internet Crime Unit (Німеччина), Federal Office for InformatioN Security, The Cyber security operations centre (Австралія) тощо.

З січня 2007 р. у Міністерстві внутрішніх справ Німеччини діє спеціальна група, функціями якої є виявлення випадків радикально-ісламістської пропаганди, а також аналіз роботи сайтів, що представляють потенційну кібернетичну небезпеку; боротьба з кібертероризмом [14].

Активну позицію щодо створення дієвих механізмів правового та організаційного забезпечення кібербезпеки займає і провідна міжнародна організація безпеки – НАТО (Cooperative Cyber Defence Centre of Excellence).

У 2008 р. Спільний Центр передового досвіду з кіберзахисту в Талині (Естонія) було акредитовано як Центр передового досвіду НАТО, функціями якого є проведення досліджень і навчань у сфері кіберзахисту.

Дієвості адміністративно-правового регулювання забезпечення та організації кібербезпеки в зарубіжних країнах сприяє збільшення чисельності відповідних підрозділів у системі кіберзахисту. Так, у Великій Британії створено три регіональних поліцейських кіберпідрозділи The Police Central e-crime Unit, HMRC. У США оголошено про додатковий набір 1000 співробітників у спеціальний департамент кібербезпеки Управління національної безпеки (Department of Homeland Security). У січні 2013 р. у Гаазі було відкрито Європейський центр боротьби з

кіберзлочинністю (ЕС3).

Одним із дієвих заходів адміністративно-правового регулювання забезпечення кібербезпеки є посилення контролю з боку держави у сфері кіберпростору. Так, наприклад, у США в публічних пунктах доступу до Інтернету (бібліотеки, школи, інтернет-кафе тощо) примусово введено фільтри, які обмежують доступ до сайтів, що містять порнографію й екстремістські матеріали [15]. Крім того, провідні держави світу активно беруть участь у навчаннях щодо протидії кібератакам.

Одним із заходів механізму адміністративно-правового регулювання забезпечення та організації кібербезпеки в зарубіжних країнах є проведення активної роз'яснювальної роботи серед населення щодо небезпек кіберзагроз. Наприклад, зовсім недавно Велика Британія вперше провела разом з європейськими, американськими і канадськими партнерами захід під назвою Get Safe Online Week для підвищення розуміння загроз кібербезпеки серед загального населення [16].

Крім того, зарубіжний досвід правового та організаційного забезпечення кібербезпеки свідчить про зростання ролі науки у сфері захисту кіберпростору, про що свідчить створення у Великій Британії нового Інституту віртуальних досліджень (Virtual Research Institute).

Отже, адміністративно-правове регулювання забезпечення та організації кібербезпеки з метою протидії дедалі зростаючого числа злочинів у кіберсфері є загальноприйнятою практикою в багатьох державах світу.

Відзначаючи високий рівень активності й зацікавленості міжнародного співтовариства в стратегічному рішенні проблем розвитку кіберпростору; розглянувши визначення кібербезпеки, яке є комплексним і багатозначним; вивчивши досвід провідних країн у сфері адміністративно-правового та організаційного забезпечення кібербезпеки, який може стати прикладом для України у формуванні її власної Стратегії забезпечення кібернетичної безпеки, можна зробити відповідні висновки, що створення реального міжнародного консенсусу з цього питання між лідерами-державами є об'єктивною необхідністю, оскільки унеможливить подальше стрімке зростання кіберзагроз як на національному, так і міжнародному рівнях.

Україна вже сьогодні відчуває вплив кіберзлочинності, і об'єктивно зацікавлена в тому, щоб брати в цих дискусіях активну участь, оскільки міжнародний досвід у сфері адміністративно-правового та організаційного забезпечення кібербезпеки та у сфері боротьби з кіберзагрозами є необхідним для неї як приклад у формуванні відповідної політики й побудови власної системи правового та організаційного забезпечення кібербезпеки. А створення дієвого механізму адміністративно-правового регулювання забезпечення та організації кібербезпеки в Україні є основним пріоритетом розвитку національної безпеки, яке потребує реорганізації та вдосконалення законодавчої бази, створення єдиної національної системи забезпечення кібербезпеки, організації та вдосконалення взаємодії суб'єктів забезпечення кібербезпеки з провідними міжнародними інституціями.

Література

1. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів [текст]: /// В.М. Бабакін // Форум права. – 2011. – Ms 4. – С. 27-30. - [Електронний ресурс]: http:/Avww. nbuv. gov. ua/e-journals/FP/2011 -4/11 bvmprk.pdf.

2. Орлов О.В., Онищенко Ю.М. Попередження кіберзлочинності – складова частина державної політики в Україні [текст]: // О.В. Орлов, Ю.М. Оніщенко // Теорія та практика державного управління. – Вип. 1 (44). - [Електронний ресурс]: www.irbis-nbuv.gov.ua/.../cgiirbis_64.exe?

3. National Cyber Security Strategies: Setting the course for national efforts to strengtheN security cyberspace, ENISA: [text]: EuropeaN Network and InformatioN Security Agency, May 2012. - [Електронний ресурс]: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.

4. EuropeaN committee oN crime problems (1990) «Computer-related crime. RecommendatioN No. R (89) 9 oN computer-related crime and final report of EuropeaN committee oN crime problems» [text]. - [Електронний ресурс]: Stasbourg 1990. p. 60 (Accessed 30 April 2014).

5. General Assembly UN (1990) «ResolutioN of the General Assembly № 45/113 ofDecember 14, 1990», available at [text]. - [Електронний ресурс]: http://zakon4.rada.gov.ua/laws/show/995_204 (Accessed 30 April 2014).

6. GoodmaN M. D. and SusaN W. B (2002) The Emerging Consensus oN Criminal Conduct iN Cyberspace, UCLA J.L. & Tech. N 3 available at [text]. - [Електронний ресурс]: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php (Accessed 30 April 2014).

7. Kurnosov I.N. (1998)»InformatioN society and global informatioN networks: the public policy» [text]: vol. 6, pp. 29–36http / I.N. Kurnosov. - [Електронний ресурс]:

//emag.iis.ru/arc/infosoc/emag.nsf/BPA/1dac741b1548a987c32569670032fc51 (Accessed 30 April 2014).

8. Про ратифікацію Конвенції про кіберзлочинність [текст]: /офіц. текст: Закон України від 7 вересня 2005 р. № 2824-IV // Відомості Верховної Ради України. – 2006. – №. 5-6. – Ст. 71.

9. Конвенція Ради Європи про кіберзлочинність [текст]: /офіц. текст: Міжнародний документ від 23 листопада 2001 р. // Офіційний вісник України від 10 вересня 2007 р. – 2007. – № 65. – Ст. 2535.

10. The «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism : [text] : USA PATRIOT ACT Act of 2001». - [Електронний ресурс]: Mode of access: http://epic.org/privacy/terrorism/. – Назва титулу з екрану.

11. Киберопасность [текст]. - [Електронний ресурс]: http://www.itsec.ru/keywords.php?keyword=15845&from=40#sthash.qnxYXcOZ. dpuf. – Назва титулу з екрану.

12. S. 773: Cybersecurity Act of 2009: [text]. - [Електронний ресурс]: Mode of access: http://www.opencongress.org/bill/111-s773/show.

13. Берг И.С. Европа против «Аль-Каиди»: в ожидании атак / И.С. Берг / [Электронний ресурс]: http://mnenia.zahav.ru/.

14. Германия будет бороться с терроризмом в Интернете [текст]. // [Электронний ресурс]: // http://search.ligazakon.ua/.

15. Гусев А.В. Зарубежний опит борьби с преступлениями в сфере Интернета [текст]. / [Електронний ресурс]: www.pravo.by/Conf2010/reports/Gusev.doc.

16. Get Safe Online week [text]. / [Електронний ресурс]: http://www.cabinetoffice.gov.uk/news/get-safe-online-week.

Демедюк С.В.,
здобувач кафедри адміністративного права та адміністративного процесу
ОДУВС
Надійшла до редакції: 16.05.2015