Електронне наукове фахове видання "Державне управління: удосконалення та розвиток" включено до переліку наукових фахових видань України з питань державного управління (Наказ Міністерства освіти і науки України від 06.11.2014 № 1279)

ДЕРЖАВНЕ УПРАВЛІННЯ
удосконалення та розвиток

Академія муніципального управління

№ 5, 2014 Назад Головна

УДК 343.98

О. В. Орлов,
д. держ. упр., доцент, зав. кафедри інформаційних технологій і систем управління
ХарРІ НАДУ при Президентові України
Ю. М. Онищенко,
викладач кафедри інформаційної безпеки
Харківського національного університету внутрішніх справ, м. Харків

ОРГАНІЗАЦІЙНІ ТА НОРМАТИВНО-ПРАВОВІ ЗАСАДИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

O. V. Orlov,
Doctor of Sciences in Public Administration, Associate Professor, Head of Information Technology & Management Systems Department, KRI NAPA, Kharkiv
Y. N. Onishchenko,
Teaching assistant of the department information security, Kharkiv National University of Internal Affairs, Kharkiv

ORGANIZATIONAL AND LEGAL PRINCIPLES STRUGGLE AGAINST CYBERCRIME

Розглянуто та досліджено проблеми існуючої сучасної нормативної бази по боротьбі з кіберзлочинності як складової частини державної політики в галузі боротьби зі злочинами в сфері інформаційних, телекомунікаційних технологій і засобів державного регулювання та контролю над нею.
Запропоновано шляхи щодо покращення ситуації з регулюванням та попередженням кіберзлочинності в країні, а саме – які реорганізація та удосконалення законодавчої і нормативно-правової бази; створення єдиного інформаційного простору в загальній та організація і удосконалення динамічної взаємодії із зарубіжними законодавчими та державними органами; запровадження сучасних новітніх інформаційних технологій в органи державної влади, створення нової системи технічної підготовки, перепідготовки та підвищення кваліфікації фахівців по боротьбі з кіберзлочинністю.

Considered and investigated problems of the existing modern legal framework to combat cybercrime as part of the state policy in the fight against crimes in the field of information , communication technologies and means of government regulation and control over it.
Ways to improve the situation of control and prevention of cybercrime in the country - namely, that the reorganization and improvement of the legal and regulatory framework ; creation of a common information space in general and the organization and improvement of dynamic interaction with foreign laws and institutions; introduction of modern advanced information technologies in public authorities, a new system of technical training , retraining and advanced training of specialists in the fight against cybercrime.

Ключові слова: *нормативна база, конвенція, кіберзлочин, кібербезпека, злочин, телекомунікаційні технології, державна стратегія.*

Keywords: *normative base, convention, cybercrime, cyber security, crime, telecommunication technology, the government strategy.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими і практичними завданнями. Міжнародні організації визнають небезпеку кіберзлочинності і її трансграничний характер, обмеженість одностороннього підходу до вирішення цієї проблеми і необхідність міжнародної співпраці як у вжитті необхідних технічних заходів, так і у виробленні міжнародного законодавства. Рада Європи, Європейський союз, ООН і Інтерпол - усі ці організації відіграють важливу роль в координації міжнародних зусиль, побудові міжнародної співпраці у боротьбі із злочинами у сфері високих технологій.

Аналіз останніх досліджень и публікацій, в яких започатковано Вирішення даної проблеми. Аналіз змісту вітчизняних публікацій по державному управлінню кримінології, криміналістики, праву свідчить, що вказаній проблематиці не приділяється належної уваги. Це, у свою чергу, обумовлено тим, що в нашій країні питання боротьби з кіберзлочинністю практично не розглядалися. Грунтовному дослідження проблем боротьби з кіберзлочинністю в нашій країні також перешкоджала відсутність статистичних показників даного виду злочинів.

Деякі аспекти нормативної бази по боротьбі з кіберзлочинності вивчали та обговорювали в своїх публікаціях К. Бєляков, В. Бутузов, А. Волеводз, Д. Гавловський, В. Голубєв, В. Гуславський *Д.* С. Кльоцкін, М. Литвинов, Е. Рижков, В. Розовський Т. Тропина, В. Цимбалюк, О. Юхно та інші.

Аналіз наукової літератури засвідчив, що при всій значущості теми розвитку нормативно-правової бази в галузі боротьби з кіберзлочинністю в Україні вивчена ще не у повному обсязі. На сьогодні вітчизняними та зарубіжними вченими опубліковано та обговорено недостатня кількість наукових праць, що досліджують цю актуальну проблематику. Зокрема, не дістала належного висвітлення організаційних та нормативно-правові засади боротьби з кіберзлочинністю.

Мета статті – дослідити та проаналізувати проблеми, сучасної нормативної бази по боротьбі з кіберзлочинності як складової частини державної політики в галузі боротьби зі злочинами в сфері інформаційних, телекомунікаційних технологій і засобів держаного регулювання та контролю над нею. Надати пропозиції щодо покращення ситуації з регулюванням та попередженням кіберзлочинності в країні.

Виклад основного матеріалу та їх обгрунтування. Представляється необхідним коротко охарактеризувати найбільш важливі документи міжнародних організацій в області боротьби з кіберзлочинністю.

З 1985 по 1989 р. Спеціальний Комітет експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами, виробив Рекомендацію № 89, затверджену комітетом Міністрів ЄС 13.09.1989 року. Вона містить список правопорушень, рекомендований країнам - учасницям ЄС для розробки єдиної карної стратегії, пов'язаної з комп'ютерними злочинами. Також в документі відмічена необхідність досягнення міжнародного консенсусу з питань криміналізації деяких злочинів, пов'язаних з комп'ютерами. Рекомендація містить два списки злочинів - «мінімальний» і «факультативний (додатковий)». «Мінімальний» список включає діяння, які обов'язково мають бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку. «Додатковий» список містить ті правопорушення,

по яких досягнення міжнародної згоди представляється скрутним [12].

Значення Рекомендації № 89 важко переоцінити. На відміну від прийнятої більш ніж через 10 років після неї Конвенції Ради Європи про кіберзлочинність, яка досі не ратифікована рядом країн, що підписали її, цей документ зробив великий вплив на розвиток і зміну законодавства країн Європи.

У 1990 році VIII Конгрес ООН з попередження злочинності і поводження з правопорушниками ухвалив резолюцію, що закликає держави - члени ООН збільшити зусилля із боротьби з комп'ютерною злочинністю, модернізуючи національне карне законодавство, сприяти розвитку в майбутньому структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області комп'ютерної злочинності [9]. 14 грудня 1990 року Генеральна Асамблеєю ООН ухвалила резолюцію, що закликає уряди держав - членів керуватися рішеннями, прийнятими на VIII Конгресі ООН.

У 1995 році в Ліоні (Франція) була проведена міжнародна конференція Інтерполу з комп'ютерної злочинності. Учасники конференції підкреслили, що викликає тривогу відсутність міжнародного механізму для раціонального і ефективного протистояння цьому виду злочинності. За підсумками конференції був зроблений висновок, що у більшості країн світу спостерігається усе зростаюче використання інформаційних технології в кримінальній діяльності. Це викликає необхідність постійного вивчення цього кримінального прояву, оскільки розвиток комп'ютерних технології призводить до використання цих інновацій при скоєні комп'ютерних злочинів [13].

Підхід Інтерполу до боротьби з кіберзлочинністю полягає в тому, щоб використовувати досвід його членів у боротьбі із злочинами у сфері інформаційних технологій шляхом функціонування робочих груп або експертних груп. Робочі групи створюються для вивчення регіонального досвіду і існують в Європі, Азії, Африці і Північній і Південній Америці.

У 1997 році міністри внутрішніх справ і міністри юстиції Великої Вісімки на зустрічі у Вашингтоні прийняли «Десять принципів боротьби з високотехнологічними злочинами», що включають, у тому числі, положення про те, що «для тих, хто зловживає інформаційними технологіями, не повинно бути ніяких» зон безпеки. Правова система повинна забезпечити захист конфіденційності, цілісності і придатності даних і систем від протиправного ушкодження і гарантувати покарання за серйозні правопорушення [6].

Продуктом багаторічних зусиль Ради Європи стала прийнята 23 листопада 2001 року у Будапешті Конвенція Ради Європи про кіберзлочинність. Це 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 [3]. Наша країна ратифікувала цю конвенцію 7 вересня 2005 року [7].

Підготовка Конвенції була тривалим процесом - за чотири роки було складено 27 проектів. Завершальна версія, що містить преамбулу і чотири глави, датована 25 травня 2001 року, була представлена Європейській комісії з боротьби з кіберзлочинністю на 50-м пленарному засіданні 18-22 червня 2001 року.

Про Конвенцію Ради Європи в цій роботі вже було сказано немало, зокрема, про види злочинів, передбачених нею. Ще раз відмітимо, що Конвенція підрозділяє злочини в кіберпросторі на 4 групи. У першу групу злочинів, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних даних і систем входять: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не лише комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених в статтях 2-5 Конвенцій, але і комп'ютерні паролі, коди доступу і їх аналоги, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому або будь-якій її частині (з урахуванням злочинного наміру). Норми ст. 6 Конвенцій застосовні тільки у тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на здійснення протиправних діянь.

До другої групи входять злочини, пов'язані з використанням комп'ютерних засобів : підлог і шахрайство з використанням комп'ютерних технологій (статті 7, 8 Конвенцій).

Третю групу складають злочини, пов'язані з контентом (змістом) даних. До четвертої групи увійшли порушення авторського права і суміжних прав.

Крім того, на початку 2002 р. до Конвенції ухвалив протокол, що додає в перелік злочинів поширення інформації расистського і іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що грунтуються на расовій, національній, релігійній або етнічній приналежності.

Таким чином, перший розділ Конвенції присвячений видам діянь, що підлягають криміналізації. Її другий розділ освітлює процесуальні аспекти боротьби з кіберзлочинністю.

У Конвенції піднімається одна із основних проблем правового регулювання Інтернету - визначення юрисдикції (ст. 22). Конвенція пропонує традиційне рішення проблеми юрисдикції : карна юрисдикція визначається відповідно до територіальної ознаки (територія держави; борт судна або літака держави). Проте у разі, якщо злочин скоєний поза територіальною юрисдикцією держави, то застосовується карне законодавство тієї держави, громадянином (підданим) якої є злочинець. Тут виникає неясність: незрозумілий статус кіберпростору - чи поширюється на нього національне законодавство або ні? Відповіді на поставлені питання, судячи з усього, з'являться найближчими роками - у міру появи практики рішення конкретних правових суперечок в всесвітній мережі. Таким чином, проблема визначення підвідомчості і осудності злочинів в кіберпросторі як і раніше залишається відкритою. Щоб уникнути можливих подальших суперечок в Конвенції передбачається, що внутрішні закони держав можуть містити інші норми про юрисдикцію.

Зважаючи на відсутність кордонів в глобальних мережах, Конвенція уточнює ситуацію колізії юрисдикції декількох держав: у такому разі, згідно п. 5 ст. 22, держави повинні проводити консультації для визначення відповідної юрисдикції для судового переслідування.

Глава III Конвенції – «Міжнародна співпраця» - присвячена питанням екстрадиції, спільній діяльності держав-учасників у сфері боротьби з комп'ютерними злочинами і досягнення узгодженості для збору доказів в електронній формі.

Конвенція про кіберзлочинність на сьогодні є одним з базових міжнародно-правових актів у сфері права телекомунікацій, але і цей документ не позбавлений недоліків. Ще до підписання Конвенції деякі групи по захисту громадянських прав і провайдери інтернет-послуг приводили серйозні аргументи проти укладення цього договору, який на їх погляд має неясні формулювання і пред'являє провайдерам непосильні вимоги.

У число організацій, що підписали протест проти прийняття Конвенції, увійшли «Фонд Електронних Меж» (Electronic Frontier Foundation, США), міжнародна організація «Суспільство Інтернет» (Internet Society), «Організація кіберправа і кіберсвободи» (Cyber - Rights & CyberLiberties, Великобританія), «Кріптополіс» (Kriptopolis, Іспанія) і інші. У протесті відзначається, 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, являється практика її застосування положень. Окремі положення Конвенції (наприклад, що стосуються процесуальних питань, визначення юрисдикції і класифікації кіберзлочинів) надалі будуть переглянуті. Але сьогодні можна констатувати, що прийняття Конвенції послужить фундаментом для міжнародного законодавства, що формується. Навіть ті країни, які з яких-небудь причин не підписали Конвенцію можуть використовувати досвід, що накопичується, по правовому регулюванню нової предметної області – кіберпростір.

Зусилля, що робляться на міжнародному рівні, пов'язані з діями з реформування карного законодавства на національному рівні. Національні і міжнародні зусилля доповнюють один одного, забезпечуючи глобальну увагу до проблем кіберзлочинності і обумовлюючи координацію кроків по боротьбі з кіберзлочинністю і уніфікацію національних законодавств.. Міжнародні і наднаціональні організації, безумовно, внесли величезний вклад в реформування національних законодавств і координацію процесуальних, технічних і інших дій з виявлення кіберзлочинів, їх розслідування і судового переслідування.

Але навіть якщо враховувати прогрес в реформуванні національних законодавств і координації міжнародних зусиль експертами постійно підкреслюється необхідність розвитку усебічних, послідовних національних стратегій, які наслідуватимуть глобальну стратегію боротьби з кіберзлочинністю. Зусилля, що робляться на міжнародному рівні, обов'язково повинні підкріплюватися діями на рівні окремо взятої держави.

10 березня 2004 року європейським парламентом створено європейське агентства по мережевій і інформаційній безпеці (ENISA). Це агентство Євросоюзу, створені з метою підвищення ефективності функціонування внутрішнього ринку. Агентство виступає в ролі консультанта і центру передових технологій у сфері мережевої і інформаційної безпеки для країн-членів і інститутів Євросоюзу. Крім того, агентство сприяє розвитку зв'язків між країнами-членами Євросоюзу, інститутами Євросоюзу, господарюючими суб'єктами і приватним бізнесом [1].

У січні 2013 року в Гаазі відкрився Європейський центр боротьби з кіберзлочинністю (ЕС3). Завдання ЕС3 - присікати дії організованих злочинних мереж. На даний момент об'єкти уваги ЕС3 обмежені трьома онлайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи [4].

У 2007 році в Україні створено CERT-UA (Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події України) – спеціалізований структурний підрозділ Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку). CERT-UA з 2009 року була акредитована у FIRST (Forum for Incident Response and Security Teams – Форум команд реагування на інциденти інформаційної безпеки) та вже протягом 5 років є його повноправним членом. Слід зазначити, що членство у FIRST, в рамках протидії кібернетичним загрозам на міжнародному рівні, надає можливість оперативно взаємодіяти з 284 командами реагування на комп'ютерні інциденти (CERT) з 61 країни світу [11].

В нашій державі нормативно-правову базу правового регулювання в даній сфері складають Конституція України, Кримінальний кодекс України, Конвенція Ради Європи «Про кіберзлочинність», Закони України «Про основи національної безпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо, Укази Президента України від 08 липня 2009 року № 514/2009, від 08 червня 2012 року № 389/2012, № 390/2012, інші нормативно-правові акти.

У ряді міждержавних нормативно-правових актів визнано, що кіберзлочинність сьогодні представляє загрозу не лише національної безпеки окремих держав, а погрожує людству і міжнародному порядку.

З початку 90-х років XX століття вказаній проблемі приділяється значна увага у багатьох країнах світу. Позначені питання знаходяться і у полі зору урядових структур нашої держави. Стимулом для цього також виступають узяті Україною зобов'язання по інтеграції у міжнародну та світову спільноту, у тому числі відповідно до Програми інтеграції України в Європейський Союз (розділ 13 - "Інформаційне суспільство") [8].

Дуже високий рівень латентності кіберзлочинності обумовлено рядом причин таких як: низький рівень спеціального технічного оснащення правоохоронних структур сучасними засобами комп'ютерної техніки і комп'ютерними технологіями; відсутність знань і навичок виявлення, розкриття і розслідування кіберзлочинів із-за обмеження доступу до сучасних методик, тактики і техніки; низький рівень інформаційної культури, підготовленості широкого круга кадрів правоохоронних органів і суддів про залучення винних до карної відповідальності; недовіра потерпілих в правоохоронні органи (пов'язано з вищезгаданими чинниками) і т.д.

Порівняльний аналіз досліджень передового зарубіжного досвіду боротьби з кіберзлочинністю свідчить, що вона має тенденцію до росту. Однією з умов її росту є ускладнення сучасних телекомунікаційних та технічних систем глобального зв'язку і спрощення доступу до використання комп'ютерних технологій широкого круга користувачів через персональні комп'ютери.

У ведучих, економічно розвинених країнах рівень втрат від кіберзлочинності вимірюється кількісно тисячами, а економічні збитки складають мільярди доларів США. За оцінками Інтерполу тільки в Європі збиток від дій кіберзлочинців щорічно складає 750 мільярдів євро [2]. Втрати США від кіберзлочинності складають від 20 до $ 140 млрд. доларів, або близько 1% від ВВП країни, а в Латинській Америці фінансові втрати від діяльності кіберзлочинців в 2013 склали 1,1 млрд. доларів. Такі дані опублікувала неурядова організація LACNIC, що займається аналізом Інтернет - активності в регіоні [10].

Дослідження питань боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні засоби забезпечення інформаційної безпеки в умовах інформатизації суспільства, у тому числі профілактики боротьби з кіберзлочинами, не досягла значних успіхів. Це в значній мірі зобов'язано з підвищенням рівня знань користувачів комп'ютерної та телекомунікаційної техніки.

Парадокс полягає в тому, що чим складніше стає програмне забезпечення (software), тим більш вразливими виявляються традиційні організаційні заходи і засоби інженерного та технічного захисту інформації в комп'ютерних та інформаційних системах, зокрема стосовно несанкціонованого доступу до комп'ютерів та мереж.

Ще однією проблемою порядку є і те, що з розвитком електронних засобів інформації розвиваються технічні засоби перехоплення і несанкціонованого доступу до інформації, яка передається по електронним системах зв'язку.

Найбільшу небезпеку для держави та суспільства складає міжнародна організована кіберзлочинність особливо у сфері економічних відносин в фінансових та банківських системах.

Правовою основою по протидії комп'ютерної злочинності на національному рівні є Кримінальний кодекс України (КК). В цьому КК окремі види комп'ютерних злочинів (кіберзлочинів) виділено в розділ VI Особливої частини - Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361, 363). Окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочини, розміщені в інших розділах Особливої частини : В Розділу V Особливої частини зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину (ст. 163, 176, 177) та Злочини у сфері господарської діяльності (ст. 200) в Розділу VII - [5].

Серед інших організаційних заходів в Україні потрібно зазначити, що на урядовому рівні створено декілька робочих груп, які розробляють проекти законодавчих актів у сфері громадських стосунків стосовно використання інформаційних технологій, які відображають питання боротьби з кіберзлочинністю і взаємодію з різними міжнародними державними та правоохоронними структурами.

Аналіз різних ініціатив по створенню проектів нормативно-правових актів свідчить, що між державними структурами не має взаємодії, координації їхньої діяльності. На законодавчому рівні ініціюються суперечливі ідеї, що не є потрібним правотворчій діяльності. На сьогоднішній день у сфері інформаційного законодавства створені умови, які дозволяють злочинцям уникати відповідальності за скоєння злочинів використовуючи недосконалу правову базу в різних країнах Вказаний чинник можна розглядати як ознаку латентності кіберзлочинності.

Висновки. Для ефективної протидії кіберзлочинності відомчих ініціатив вже недостатньо. Потрібна чітка централізована координація зусиль для забезпечення злагодженої взаємодії усіх зацікавлених суб'єктів.

Ми можемо визначити основні пріоритети розвитку державних структур по боротьбі з кіберзлочинністю такі як: реорганізація та удосконалення законодавчої і нормативно-правової бази; створення єдиного інформаційного простору в загальній та організація і удосконалення динамічної взаємодії із зарубіжними законодавчими та державними органами; запровадження сучасних новітніх інформаційних технологій в органи державної влади, технічна підготовка, перепідготовка та підвищення кваліфікації фахівців по боротьбі з кіберзлочинністю.

Література.

1. Государственные стратегии кибербезопасности [Електронний ресурс] – Режим доступу: http://www.bezpeka.com/ru/lib/sec/gen/government-cybersecurity-strategy.html

2. Европа объявила войну киберпреступности / [Електронний ресурс] – Режим доступу: http://www.dw.de/европа-объявила-войну-киберпреступности /a-15988857-1

3. Европейская Конвенция по киберпреступлениям от 23 ноября 2001 г. / [Електронний ресурс] – Режим доступу: http://www.eos.ru/eos_delopr/eos_law /detail.php?ID=32003&SECTION_ID=671

4. Европейский центр борьбы с киберпреступностью отчитался за первый год работы / [Електронний ресурс] – Режим доступу: http://www.interfax.ru/world /357250

5. Кримінальний кодекс України / [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2341-14

6. Курносов И.Н. Информационное общество и глобальные информационные сети: вопросы государственной политики / И.Н. Курносов // Информационное общество, 1998, вып. 6, с. 29 – 36. [Електронний ресурс] – Режим доступу: http://emag.iis.ru/arc/infosoc/emag.nsf /BPA/1dac741b1548a987c32569670032fc51

7. Про ратифікацію Конвенції про кіберзлочинність: закон України від 7 верес. 2005 р. № 2824-IV // Відомості Верховної Ради України. - 2006. - № 5-6. - Ст. 71

8. Програма інтеграції України до Європейського Союзу / [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/n0001100-00

9. Резолюція 45/113 Генеральної Асамблеї ООН від 14 грудня 1990 року / [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_204

10. Финансовые потери от киберпреступности в Латинской Америке превысили $1 млрд. / [Електронний ресурс] – Режим доступу: http://itar-tass.com /mezhdunarodnaya-panorama/1001716

11. Computer Emergency Response Team of Ukraine / [Електронний ресурс] – Режим доступу: http://cert.gov.ua

12. Computer-related crime. Recommendation No. R (89) 9 on computer-related crime and final report of European committee on crime problems. Stasbourg 1990. p. 60

13. Goodman M. D., Brenner S. W. The Emerging Consensus on Criminal Conduct in Cyberspace / Marc D. Goodman and Susan W. Brenner // UCLA J.L. & Tech. 2002. N 3 [Електронний ресурс] – Режим доступу: http://www.lawtechjournal.com/articles/ 2002/03_020625_goodmanbrenner.php

References

1. Information Security Center (2012) “State cybersecurity strategy”, available at:http://www.bezpeka.com/ru/lib/sec/gen/government-cybersecurity-strategy.html (Accessed 30 April 2014).

2. Deutsche Welle (2014) “Europe declared war on cyber crime”, available at: http://www.dw.de/evropa-ob'yavila-voynu-kiberprestupnosti/a-15988857-1 (Accessed 30 April 2014).

3. Electronic Office Systems (2014) “European Convention on cyber crimes from November 23, 2001”, available at: http://www.eos.ru/eos_delopr/eos_law /detail.php?ID=32003&SECTION_ID=671 (Accessed 30 April 2014).

4. Interfax (2014) “The European Centre for the fight against cyber crime reported for the first year of operation”, available at: http://www.interfax.ru/world/357250

(Accessed 30 April 2014).

5. The Verkhovna Rada of Ukraine (2014), The Law of Ukraine “The Criminal Code of Ukraine”, available at: http://zakon4.rada.gov.ua/laws/show/2341-14 (Accessed 30 April 2014).

6. Kurnosov I.N. (1998)“Information society and global information networks: the public policy”, [Online], vol . 6, pp. 29–36, available at: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/1dac741b1548a987c32569670032fc51 (Accessed 30 April 2014).

7. The Verkhovna Rada of Ukraine (2005) “On Ratification of the Convention on Cyber crime: the law of Ukraine on Sept. 7. 2005 y. № 2824-IV” // Vidomosti Verhovnoyi Radi Ukrayini. - 2006. - no 5-6. – p. 71

8. The Verkhovna Rada of Ukraine (2000) “Program integrating Ukraine into the European Union”, available at: http://zakon4.rada.gov.ua/laws/show/n0001100-00 (Accessed 30 April 2014).

9. General Assembly UN (1990) “Resolution of the General Assembly № 45/113 ofDecember 14, 1990”, available at: http://zakon4.rada.gov.ua/laws/show/995_204 (Accessed 30 April 2014).

10. ITAR-TASS News Agensy (2014)“Financial losses from cyber crime in Latin America exceeded $ 1 billion”, available at: http://itar-tass.com/mezhdunarodnaya-panorama/1001716 (Accessed 30 April 2014).

11. CERT-UA (2014) “Computer Emergency Response Team of Ukraine”, available at: http://cert.gov.ua (Accessed 30 April 2014).

12. 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”. Stasbourg 1990. p. 60 (Accessed 30 April 2014).

13. Goodman M. D. and Susan W. B (2002) The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA J.L. & Tech. N 3 available at http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php (Accessed 30 April 2014).

Стаття надійшла до редакції 20.05.2014 р.