УДК 340.134(083.7):004.7–049.65(73)

Олена Бусол,
д-р юрид. наук, ст. наук. співроб.,
Національна бібліотека України імені В. І. Вернадського

ТЕНДЕНЦІЇ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ США

У статті здійснено аналіз стану й сучасних тенденцій забезпечення інформаційної безпеки США.

Ключові слова: інформаційна безпека, законодавство, нормативно-правове забезпечення США, тенденції, ІТ-технології.

Сьогодні в умовах глобалізації, інтелектуалізації злочинності, охоплення інформатизацією усіх суспільних відносин міжнародна спільнота усвідомлює необхідність удосконалення діючих і розроблення уніфікованих нормативно-правових актів щодо регулювання міжнародної інформаційної безпеки.

Проблему інформаційної безпеки, як міжнародної, так і окремих держав, вивчали такі вчені, як А. Баранов, І. Бінько, В. Богуш, В. Головченко, В. Гондюл, В. Горовий, О. Кісілевич-Чорнойван, Б. Кормич, В. Конах, О. Литвиненко, Є. Макаренко, М. Ожеван, О. Олійник, В. Попик, В. Потіха, М. Рижиков, В. Шамрай, О. Юдін та ін.

Дослідження наявних наукових напрацювань і аналіз інформації інтернет-середовища дають підстави стверджувати, що одним з найкращих у забезпеченні інформаційної безпеки є досвід США, чим обумовлений вибір теми пропонованої статті. Так, навіть Японія, яка є однією з найрозвинутіших у технологічному відношенні країн, відстає, за висновком В. Брижка, від США на понад п’ять років у сфері розповсюдження персональних комп’ютерів, кабельного телебачення, цифрової телефонії та в інших аспектах інформаційної політики [1].

Мета статті – встановлення тенденцій нормативно-правового забезпечення США у сфері інформаційної безпеки, що має допомогти Україні прогнозувати розвиток цього напряму та знайти точки дотику для взаємної співпраці між обома державами.

Правову основу забезпечення інформаційної безпеки, завдяки якій можна скласти уявлення про загальну державну політику Сполучених Штатів Америки, становлять закони «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997 р.), «Про комп'ютерне шахрайство та зловживання» (1986 р.), «Про свободу інформації» (1967 р.), «Про висвітлення діяльності уряду», «Про охорону особистих таємниць», «Про таємницю» (1974 р.), «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп'ютерних систем» (1987 р.). Водночас слід зазначити, що підзаконні нормативно-правові акти окремих Штатів США можуть принципово різнитися.

Національна політика США в галузі захисту інформації формується Агентством національної безпеки (далі – АНБ), а найважливіші стратегічні питання інформаційної безпеки розглядаються Радою національної безпеки з виданням директив президента США, серед яких: PD/NSC–24 «Політика в галузі захисту систем зв'язку» (1977 р.), у якій уперше наголошено на необхідності захисту важливої несекретної інформації для забезпечення національної безпеки; SDD–145 «Національна політика США в галузі безпеки систем зв'язку в автоматизованих інформаційних системах» (1984 р.), якою на АНБ покладено функції із захисту інформації та контролю за безпекою не тільки на каналах зв'язку, а й в обчислювальній та інформаційно-телекомунікаційній системах, а також відповідальність за сертифікацію технологій, систем і устаткування в частині захисту інформації в інформаційно-телекомунікаційних системах країни, а також за ліцензування діяльності в галузі захисту інформації.

США, здійснюючи політику в галузі захисту інформації, розуміють, що перехоплення іноземними державами відкритої інформації, яка передається урядовими й комерційними телекомунікаціями, може завдати шкоди державі, оскільки обробка цієї інформації, зіставлення та об'єднання розрізнених відомостей може призвести до розкриття державних секретів. Тож у 80-х роках минулого століття захист ліній зв'язку й автоматизованих систем стає основним завданням компетентних державних органів США. Конгресом США у 1987 р. був прийнятий Закон «Про забезпечення безпеки ЕОМ» Mb HR–145, який визначає, зокрема, пріоритет національних інтересів при розв'язанні проблем інформаційної безпеки приватних організацій. Законом вперше

запроваджено категорію несекретної інформації, що важлива з погляду національної безпеки (несекретна електронна інформація недержавних структур, які на добровільній основі співпрацюють з урядом в інтересах національної безпеки).

Генеральна Асамблея ООН ще у 2001 р. на 56-й сесії акцентувала увагу на понятті «інформаційна та мережева безпека», що означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації та створення надійного джерела постачання обладнання, послуг й інформації. Інформаційна безпека того часу охоплювала захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Уже в ті часи передбачалося, що недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем несе загрозу міжнародній безпеці.

Тенденцію до надання пріоритетної ролі інформаційній безпеці наочно демонструють такі резолюції Генеральної Асамблеї ООН: «Роль науки і техніки в контексті міжнародної безпеки, роззброєння та інших, пов'язаних з цим, сфер» № 53/576 (1998 р.); «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» № 54/49 (1999 р.), № 55/28 (2000 р.), № 60/45 (2005 р.) [2, 3, 4, 5].

Загалом державна політика США у сфері інформаційної безпеки пройшла тривалий еволюційний шлях, який складається з чотирьох етапів: виникнення – 1939–1947 рр.; становлення – 1947–1982 рр.; активний розвиток – 1983–2001 рр.; докорінне вдосконалення – з 2001 р. дотепер. З приходом у 1981 р. до влади президента США Р. Рейгана та його адміністрації в управлінні інформаційними ресурсами відповідно до Закону «Про свободу інформації» напрям інформаційної безпеки був визначений як пріоритетний в урядовій політиці.

Уже в 1992 р. було прийнято програми «Національна інформаційна політика» та «Глобальна інформаційна політика» (GII). Програма GII базувалася на п'яти ключових принципах: залучення приватних інвестицій, сприяння конкуренції, введення гнучких механізмів регулювання, які мають забезпечити пристосовування до швидких технологічних змін і ринкової конкуренції; надання відкритого доступу до існуючих мереж усім провайдерам та користувачам; забезпечення загальнодоступних інформаційних послуг, створення електронного уряду.

Достатньо сказати, що при Бібліотеці Конгресу США створено центральний депозитарій документів з проблем кібер-, медіа- та психотероризму з метою моніторингу теорії і практики інформаційно-психологічних впливів у сучасному світі, створення ефективної регіональної системи інформаційного протиборства та об'єднання зусиль держав-членів Організації американських держав у сфері інформаційної безпеки [6]. Адміністрація США на офіційному рівні розглядає інформацію як певний стратегічний ресурс, який виникає в результаті оброблення даних за допомогою спеціалізованих систем аналізу.

Військово-політичне керівництво США й західних держав на початку 1990-х років приділяє особливу увагу розвитку інформаційної технології, високо оцінюючи її потенційні можливості для досягнення військової переваги. Саме про це свідчить Директива МО США TS від 21 грудня 1992 р. «Інформаційна війна», у якій відзначено необхідність усебічного обліку інформаційних ресурсів при організації планування і функціонування систем управління в інтересах підвищення ефективності своїх військ в умовах протидії супротивнику. Складовими концепту «інформаційна війна» є: оперативна безпека, введення супротивника в оману, психологічні операції, електронна війна і вогневе знищення, які здійснюються в комплексі з глибокою та всебічною розвідкою як для дезорганізації системи управління противника, так і для захисту власної системи управління під час бойових дій. Водночас інформація, що циркулює в системі управління, розглядається як високопріоритетний об'єкт впливу й захисту, зниження або підвищення достовірності. Для Пентагону, який використовує кілька сот різних інформаційних систем і мереж, питання інформаційної безпеки фактично прирівнюється до питань військової безпеки [7].

У присвячених США статтях найчастіше зустрічається таке визначення поняття «інформаційні військові дій»: дії, вжиті для досягнення інформаційної переваги в інтересах національної військової стратегії, дії, що здійснюють шляхом впливу на інформацію та інформаційні системи противника при одночасному захисті власної інформації і своїх інформаційних систем [8].

За 1997–2001 рр. на законодавчому рівні у сфері інформаційної безпеки США було зроблено чимало: пом'якшено експортні обмеження на криптозасоби, сформовано інфраструктуру з відкритими ключами,

розроблено ряд стандартів на кшалт електронного цифрового підпису – FIPS 186–2 (2000 р.). Усе це дало змогу зосередитися на одному з її найважливіших додатків – аутентифікації, розглядаючи її за відпрацьованою на криптографічних засобах методикою. На базі цих законів у США сформовано загальнонаціональну інфраструктуру електронної аутентифікації.

Крім того, у законодавстві США діють як положення обмежувальної спрямованості, так і директиви, що захищають інтереси таких державних відомств, як Міністерство оборони, АНБ, ФБР, ЦРУ.

У березні 2001 р. президент США Д. Буш, виступаючи в штаб-квартирі ЦРУ в Ленглі, вказав на основні загрози національній безпеці США. На другому місці після тероризму в цьому переліку значиться інформаційна війна, уже за нею – розповсюдження зброї масового ураження й засобів її доставки.

Збір розвідувальних даних з комп'ютерних систем противника дає змогу виявляти уразливі місця в його інформаційних системах. Тож США розроблено й реалізуються програми, спрямовані на розширення можливостей розвідки з добування та оброблення інформації щодо загроз національній інформаційній інфраструктурі з боку інших держав. Крім традиційних методів агентурної роботи, ЦРУ приділяє значну увагу аналізу відкритих джерел і проникненню в закриті бази даних програмним шляхом. У США на офіційному рівні визнають, що контроль над секретними комунікаціями противника при одночасному захисті своїх власних надає їм унікальні можливості для збереження лідируючих позицій у світі.

Можна провести деякі паралелі між Указом Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 15 квітня 2017 р. № 133, та ініційованим Конгресом США проектом Акта про кібербезпеку (The Cybersecurity Act of 2009) [9]. У цьому нормативно-правовому документі президенту США, у надзвичайних випадках загроз національній безпеці, надається право обмеження доступу до мережі Інтернет на всій території США. У той же час на розгляд Конгресу США був внесений проект Акта глобальної відповіді на кібервиклики (Fostering a Global Response to Cyber Attacks Act), який містить норми щодо організації взаємодії США з іншими державами світу з проблем протидії кіберзлочинності.

Згідно з Оглядом кібербезпекової політики (Cyberiecurity Review) (2009 р.) Білий дім США визначає структуру системи національної кібербезпеки. Завданням відповідно є: формування кібербезпекової політики; демонстрування суспільству США і міжнародним партнерам важливості для держав цього напряму; удосконалення законодавства у цій сфері, зокрема у частині кримінальної відповідальності; розробка проектів на рівні держави, окремих Штатів та міст у сфері кібернетичної безпеки.

У Зауваженнях щодо забезпечення безпеки національної кіберінфраструктури» (2009 р.) [10] Б. Обама зробив висновок, що «кіберзагрози є одними з найбільш серйозних викликів економічній і національній безпеці, з яким зіткнулася нація». З огляду на це президент оголосив цифрову інфраструктуру США стратегічною національною цінністю, а її захист – національним пріоритетом. Основні заходи в цій сфері спрямовані на розроблення ефективної стратегії забезпечення безпеки інформаційних та комунікаційних мереж; розроблення систем запобігання й реагування на кібератаки; посилення партнерства держави і приватного сектора; збільшення інвестицій в іноваційні технології, а також розгортання масштабної національної кампанії щодо посилення готовності суспільства до протидії кіберзагрозам [11].

Ініціатива з загальної національної кібербезпеки Ради національної безпеки США 2010 р., що є складовою частиною Воєнної доктрини США, містить 12 положень щодо реалізації захисту держави та Білого дому від кібератак. Відповідно до цього документа, у США створено єдину захищену федеральну мережу, доступ до якої чітко контролюється. Крім того, ініціатива передбачає об'єднання всіх наявних у США центрів оперативного реагування на кіберзлочини з метою підвищення ефективності їхньої діяльності та проведення глибокого аналізу щодо хакерських атак.

Також з метою протидії іноземним кібершпигунам документом передбачено створення підрозділів кіберконтррозвідки в державних органах США, зокрема для захисту секретних внутрішніх мереж Міністерства оборони США від терористичних атак.

Важливим кроком уряду є створення системи управління ризиками для прогнозування наслідків зламу систем, викрадення або пошкодження інформації та мінімізації збитків від протиправних втручань у неї, а також захисту мереж недержавної інфраструктури.

З метою захисту мережі вищих державних органів запроваджено роботу програми «Ейнштейн» (Einstein Program, або Einstein) [12], яка розроблена оперативним підрозділом Національного управління кібербезпеки Міністерства внутрішньої безпеки США. Вона дає змогу виявляти та фіксувати несанкціоновані зовнішні втручання.

У Стратегії кібербезпеки США (2011 р.) закріплено право держави вживати заходи у відповідь на хакерські атаки, які у відповідних умовах можуть розглядатися США як оголошення війни.

Закон CISPA (Cyber Intelliggence Sharring and Protection Act) (2012 р.), у свою чергу, дає змогу уряду США та недержавним органам за наявності підозри про вчинення кіберзлочину мати доступ до конфіденційної інформації користувачів приватних фірм.

Основними напрямами забезпечення національної кібербезпеки США є захист критично важливих об'єктів інфраструктури, безпосередньо їхніх інформаційних систем від кібернетичних атак; удосконалення засобів виявлення атак і оперативного реагування на них; визначення завдань безпеки кіберпростору та способи їх вирішення; підготовка відповідних фахівців з безпеки інформації та взаємодія з приватним сектором; співпраця з міжнародними організаціями з метою забезпечення відкритого, безпечного, надійного кіберпростору.

Нормативно-правовими документами США, що регулюють безпеку кіберпростору, стали Національна стратегія безпечного кіберпростору (2003 р.), Огляд політики кібербезпеки (2009 р.), Міжнародна стратегія для кіберпростору (2011 р.), Наказ президента США «Щодо проекту Стратегії покращення кібербезпеки критично важливих об'єктів інфраструктури (2013 р.), проект Стратегії покращення кібербезпеки критично важливих об'єктів інфраструктури (2014 р.), Закон з кібербезпеки та обміну інформацією (2015 р.), Національна стратегія безпеки (2015 р.), Стратегія кібербезпеки департаменту оборони (2015 р.). У зазначених нормативно-правових актах закріплено дії із знешкодження та протистояння атакам у національному інформаційному просторі, визначено види загроз, обов'язки захисту кіберпростору для різних спеціалізованих державних установ. Цими документами визначено умови для обміну даними з протидії кіберзагрозам, прогнозування відповідних ризиків, співробітництва з іншими державами з проблем кібертероризму, а також підвищення кваліфікації фахівців з протидії цим злочинам. Крім

того, окремо акцентується на залученні до протидії тероризму приватних установ і громадських організацій, наприклад CERT, ISACA, CSX, CCSIS, а також залучення освітніх та наукових установ до проведення досліджень щодо забезпечення безпеки національного кіберпростору [13–23].

Аналіз наукових розвідок щодо інформаційної безпеки США показує, що, незважаючи на чималу кількість нормативно-правових актів США у сфері інформаційної безпеки, вони не завжди є ефективними. Законодавство США все ж таки ще не охоплює усіх загроз в інформаційній сфері держави, що існують на сучасному етапі. Прогалинами в політиці інформаційної безпеки США можна вважати випадок з Е. Сноуденом, який викликав шквал суперечливих висловлювань як у США, так і в інших державах про допустимість масового негласного спостереження, межі державної таємниці й баланс між захистом персональних даних і забезпеченням національної безпеки в епоху після 11 вересня 2001 р. (дата наймасштабнішого в історії теракту з численними жертвами, що вчинений шляхом тарану двома пасажирськими літаками, керованими терористами, будівель Всесвітнього торгового центру у м. Нью-Йорк, США). Тож захист інформаційного простору від кібертерористів, а користувачів інформаційних систем від шахрайства, забезпечення конфіденційності інформації в інформаційних системах, захист прав інтелектуальної власності потребують розроблення нормативно-правових актів з інформаційної безпеки США принципово нового, більш високого рівня.

Неможливо в межах цієї статті охопити весь перелік нормативно-правових актів США з інформаційної безпеки повністю, можна лише констатувати їх велику кількість, що є доказом важливості теми для суспільства цієї держави. За останні 35 років у США сформувалася чітка система забезпечення інформаційної безпеки, яка вибудовувалася в декілька етапів. Пороговими серед виявлених тенденцій можуть вважатися такі. У 1981 р. інформаційна безпека стає пріоритетом урядової політики США. У 1987 р. встановлено нову категорію інформації – «несекретна, але важлива з погляду національної безпеки». У 1992 р. інформаційна безпека зводиться в ранг національної інформаційної політики та звертається підкреслена увага на глобальну інформаційну політику. У цьому ж році в обігу уряду США з'являється поняття

«інформаційна війна». У 2001 р. формується поняття «міжнародна інформаційна безпека» і визнається, що незахищеність інформаційних ресурсів становить загрозу всьому світу. Поняття «інформаційна війна» в адміністрації президента за пріоритетністю на другому місці (після тероризму). У 2009 р. цифрова інфраструктура США оголошується стратегічною національною цінністю, а її захист – національним пріоритетом. У 2011 р. хакерські атаки прирівнюються до оголошення війни. З 2015 р. законодавче регулювання кіберпростору виходить на перший план політики США.

Американський досвід державної політики у сфері інформаційної безпеки є важливим для української зовнішньої і внутрішньої політики. Найціннішим є дієвий підхід до регулювання ринку інформаційних технологій в умовах ринкової економіки. Слід усе ж зазначити, що, хоча нині Україна є одним з лідерів у світі з підготовки висококваліфікованих ІТ-фахівців і одним з основних постачальників «мізків» відповідного напряму за кордон, існує залежність України від американського програмного продукту, що можна спостерігати майже в кожній державній установі та в роботі окремих громадян. Отже, для забезпечення національної безпеки України необхідно спрямувати зусилля на створення власних конкурентоспроможних ІТ-технологій і повернення українських фахівців з-за кордону.

США мають величезний досвід застосування інформаційних технологій у всіх сферах життєдіяльності суспільства. Особливо важливим, в умовах проведення Україною урядових заходів у відповідь на зовнішню агресію іноземної держави, є американський досвід використання інформаційних технологій для створення систем зв'язку і військового керування, а також високоточного озброєння.

Інформаційну безпеку можна без перебільшення назвати одним з перспективних напрямів взаємовигідного співробітництва між Україною і США.

Література

1. *Брижко В.* До питання сучасної інформаційної політики / В. Брижко // Вісн. Академії управління МВС. – 2009. – № 2. – С. 32–36.

2. Role of science and technology in the context of international security and disarmament. Report of the First Committee General Assembly. 1998.

№ 53/579. – Mode of access: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/360/57/PDF/N9836057.pdf?OpenElement. – Title from the screen.

3. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly. 1999. № 54/49. – Mode of access: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/13/PDF/N9977713.pdf?OpenElement. – Title from the screen.

4. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly. 2000. № 55/28. – Mode of access: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/07/PDF/N0056107.pdf?OpenElement. – Title from the screen.

5. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly on 8 December 2005. № 60/45. – Mode of access: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/30/PDF/N0549030.pdf?OpenElement. – Title from the screen.

6. National Security Strategy of the United States of America. Washington. 2010, may. 52 p. // White House. – Mode of access: http://www.whitehouse.gov/sites/default/files/r. – Title from the screen.

7. Шамрай В. О. Інформаційна безпека як складова національної безпеки України / В. О. Шамрай. – Режим доступу: http://www.crime-research.ru/library/Shamray.htm. – Назва з екрана.

8. *Баранов А*. Информационный суверенитет или информационная безопасность / А. Баранов // Нац. безпека і оборона. – 2001. – № 1. – С. 70–76.

9. The Cybersecurity Act of 2009. – Mode of access: http: //whiiehouse.gov/ihe_press_ofllce. – Title from the screen.

10. Remarks by (he President on securing our nation’s cyber infrastructure) // White House. – Mode of access: whitehouse.gov/ihe_press_ofIicc/Remarks-by-the-Presidcni-on-Sceuriiy-Nations-Cyber-Infrusimcture. – Title from the screen.

11. Statement by the President on the White House Organization for Homeland Security // White House. – Mode of access: https://obamawhitehouse.archives.gov/the-press-office/statement-president-white-house-organization-homeland-security-and-counterterrorism. – Title from the screen.

12. Privacy Impact Assessment EINSTEIN Program. 2004. September. – Mode of access: https://www.dhs.gov/sites/default/files/publications/privacy_pia_eisntein.pdf. – Title from the screen.

13. National Strategy to Secure Cyberspace. February 2003. – Mode of access: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. – Title from the screen.

14. Updating U. S. Federal Cybersecurity Policy and Guidance. October 2012. – Mode of access: http://csis.org/files/publication/121019_Reeder_A130_Web.pdf. – Title from the screen.

15. Assuring a Trusted and Resilient Information and Communications Infrastructure // White House. – Mode of access: https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. – Title from the screen.

16. The Administration's Priorities on Cybersecurity // White House. – Mode of access: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critical-infrastructure. – Title from the screen.

17. Cyber Security Strategy Documents. – Mode of access: https://ccdcoe.org/strategies-policies.html. – Title from the screen.

18. The Department of Defense Cyber Strategy. – Mode of access: strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. – Title from the screen.

19. International Strategy for Cyberspace // White House. – Mode of access: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. – Title from the screen.

20. *Carter W. A*. The Evolution of Cybersecurity Requirements for the U. S. Financial Industry / W. A. Carter, D. E. Zheng. – 2015. – July. – Mode of access: http://csis.org/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf. – Title from the screen.

21. US Enacts Cybersecurity Information Legislature. – Mode of access: http://www.isaca.org/cyber/Documents/CSX–Special-Report_misc_Eng_0116.pdf. – Title from the screen.

22. US cybersecurity: Progress stalled Key findings from the 2015 US State of Cybercrime Survey. – Mode of access: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf. – Title from the screen.

23. US–CERT: Understanding Hidden Threats: Rootkits and Botnets. – Mode of access: https://www.us-cert.gov/ncas/tips. – Title from the screen.

References

1. Bryzhko, V. (2009). Do pytannia suchasnoi informatsiinoi polityky [To the question of modern information policy]. *Visnyk Akademii upravlinnia MVS – Bulletin of the Academy of the Interior Ministry,* no. 2, pp. 32–36 [in Ukrainian].

2. Role of science and technology in the context of international security and disarmament. Report of the First Committee General Assembly. 1998. № 53/579. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/360/57/PDF/N9836057.pdf?OpenElement [in English].

3. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly. 1999. № 54/49. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/13/PDF/N9977713.pdf?OpenElement [in English].

4. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly. 2000. № 55/28. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/07/PDF/N0056107.pdf?OpenElement [in English].

5. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly on 8 December 2005. № 60/45 Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/30/PDF/N0549030.pdf?OpenElement [in English].

6. National Security Strategy of the United States of America. (2010). *White House*. Retrieved from http://www.whitehouse.gov/sites/default/files/r [in English].

7. Shamrai, V. O. Informatsiina bezpeka yak skladova natsionalnoi bezpeky Ukrainy [Information security as a component of national security of Ukraine]. Retrieved from http://www.crime-research.ru/library/Shamray.htm [in Ukrainian].

8. Baranov, A. (2001). Informacionnyj suverenitet ili informacionnaja bezopasnost [Information sovereignty or information security]. *Natsionalna bezpeka i oborona – National Security and Defense,* no. 1, pp. 70–76 [in Ukrainian].

9. The Cybcrsecurity Aci of 2009. Retrieved from http: //whiiehouse.gov/ihe_press_ofllce [in English].

10. Remarks by (he President on securing our nation's cyber infrastructure).

White House. Retrieved from whitehouse.gov/ihe_press_ofIicc/Remarks-by-the-Presidcni-on-Sceuriiy-Nations-Cyber-Infrusimcture [in English].

11. Statement by the President on the White House Organization for Homeland Security. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/statement-president-white-house-organization-homeland-security-and-counterterrorism [in English].

12. Privacy Impact Assessment EINSTEIN Program. (2004). – Retrieved from https://www.dhs.gov/sites/default/files/publications/privacy_pia_eisntein.pdf [in English].

13. National Strategy to Secure Cyberspace. (2003). Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf [in English].

14. Updating U. S. Federal Cybersecurity Policy and Guidance. (2012). Retrieved from http://csis.org/files/publication/121019_Reeder_A130_Web.pdf [in English].

15. Assuring a Trusted and Resilient Information and Communications Infrastructure. *White House.* Retrieved from https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [in English].

16. The Administration's Priorities on Cybersecurity. *White House.* Retrieved from https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critica l-infrastructure [in English].

17. Cyber Security Strategy Documents. Retrieved from https://ccdcoe.org/strategies-policies.html [in English].

18. The Department of Defense Cyber Strategy. Retrieved from strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [in English].

19. International Strategy for Cyberspace. *White House.* Retrieved from https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [in English].

20. Carter, W. A. Zheng, D. E. (2015). The Evolution of Cybersecurity Requirements for the U. S. Financial Industry. Retrieved from http://csis.org/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf [in English].

21. US Enacts Cybersecurity Information Legislature. Retrieved from http://www.isaca.org/cyber/Documents/CSX–Special-Report_misc_Eng_0116.pdf [in English].

22. US cybersecurity: Progress stalled Key findings from the 2015 US State

of Cybercrime Survey. (2015). Retrieved from https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf [in English].

23. US–CERT: Understanding Hidden Threats: Rootkits and Botnets Retrieved from https://www.us-cert.gov/ncas/tips [in English].

Стаття надійшла до редакції 17.04.2017.

Olena Busol,
Dr. Sci. (Juridical), Senior Research Co-worker,
V. I. Vernadsky National Library of Ukraine

Trends of Regulatory Legal Support of Information Security in the United States

Currently, within the context of globalization, intellectualization of crime, comprehensive cover other social relations by information relations, the international community comes to understanding the need to improve existing, and to develop unified normative-legal acts on international information security regulation.

The article, based on analysis of USA laws, defines the main trends of normative-legal ensuring information security of the state. The USA has wide experience of applying information technologies in all spheres of society activity. In conditions of Ukraine's actions in response to aggression of a foreign state, the American experience of applying information technologies for creation of communication systems and military management, and also high-precision arms is especially important.

Information security without exaggeration could be considered as one of the perspective directions of mutually beneficial cooperation between Ukraine and the USA.

Keywords: copyright, academic plagiarism, intellectual property, legal act, higher education, the subjects of scientific and technical activity.

Елена Бусол,
д-р юрид. наук, ст. науч. сотр.,
Национальная библиотека Украины имени В. И. Вернадского

Тенденции нормативно-правового обеспечения информационной безопасности США

В настоящее время в условиях глобализации, интеллектуализации преступности, всестороннего охвата информатизацией всех общественных отношений международное содружество приходит к пониманию необходимости

усовершенствования действующих и разработки унифицированных нормативно-правовых актов по регулированию международной информационной безопасности.

В статье на основе анализа законодательства США установлены основные тенденции нормативно-правового обеспечения информационной безопасности данного государства.

США имеют большой опыт применения информационных технологий во всех сферах жизнедеятельности общества. Особенно важным, в условиях проведения Украиной мероприятий в ответ на внешнюю агрессию иностранного государства, является американский опыт использования информационных технологий для создания систем связи и военного управления, а также высокоточного вооружения.

Информационную безопасность можно без преувеличения назвать одним из перспективных направлений взаимовыгодного сотрудничества между Украиной и США.

Ключевые слова: информационная безопасность, законодательство, нормативно-правовое обеспечение США, тенденции, IT-технологии.