ність» з метою отримання зауважень та пропозицій до нього.

Проект потребує погодження з Міністерством фінансів України, Міністерством економічного розвитку і торгівлі України, Міністерством внутрішніх справ України, Службою безпеки України, Державною фіскальною службою України, Донецькою, Запорізькою, Миколаївською, Одеською, Херсонською обласними державними адміністраціями та Державною регуляторною службою України.

Вироблення адаптованого механізму втілення Проекту дозволить врегулювати питання щодо вилучення та реалізації вантажів, які знаходяться у морських портах понад установлені терміни.

Отже, питання гармонізації чинного вітчизняного законодавства щодо строків зберігання вантажів у морських портах України дасть змогу уникнути конфлікту інтерсів державних органів і суб'єктів зовнішньоекономічної діяльності.

ЛІТЕРАТУРА

1. Митний кодекс України : Закон України від 13 березня 2012 року № 4495-VI // Голос України. – 2012. – № 73.
2. Кодекс торговельного мореплавства України : Закон України від 23 травня 1995 року № 176/95-ВР // Відомості Верховної Ради України. – 1995. – № 47–52. – Ст. 349.
3. Господарський кодекс України : Закон України від 16 січня 2003 року № 436-IV // Відомості Верховної Ради України. – 2003. – № 18. – Ст. 144.
4. Про затвердження Правил надання послуг у морських портах України : Наказ Міністерства інфраструктури України від 05 червня 2013 року № 348 [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/z1401-13/page
5. Про морські порти України : Закон України від 17 травня 2012 року № 4709-VI// Відомості Верховної Ради України. – 2013. – № 7. – Ст. 65.
6. Статут державного підприємства «Адміністрація морських портів України» : Наказ Міністерства інфраструктури України від 25 березня 2016 року № 119 [Електронний ресурс]. – Режим доступу : http://mtu.gov.ua/files/%D0%A1%D1%82%D0%B0%D1%82%D1%83%D1%82%20%D0%90%D0%9C%D0%9F%D0%A3.pdf
7. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Митного кодексу України : Закон України від 13 березня 2012 року № 4496-VI [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/4496-17
8. Статут залізниць України : Постанова Кабінету Міністрів України від 06 квітня 1998 року № 457 [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/457-98-%D0%BF
9. Про затвердження окремих розділів Правил перевезення вантажів : Наказ Міністерства транспорту України від 21 листопада 2000 року № 644 [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/z0861-00
10. Про реалізацію вантажів, що знаходяться у морських портах понад установлені терміни : Проект постанови Кабінету Міністрів України [Електронний ресурс]. – Режим доступу : http://www.mdoffice.com.ua/pls/MDOffice/aSNewsDic.getNews?dat=15042015&num_c=471381

УДК 35.077.2

ПИТАННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УМОВАХ РОЗБУДОВИ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

QUESTION OF CYBER SECURITY UNDER DEVELOPMENT INFORMATION SOCIETY

Волох О.К.,
к.ю.н., доцент кафедри адміністративного права і процесу
Національна академія внутрішніх справ

У статті розглядаються проблеми нормативно-правового регулювання забезпечення кібернетичної безпеки. Досліджується сутність окремих нормотворчих ініціатив у розглядуваній сфері. Аналізується співвідношення понять «національна безпека», «інформаційна безпека» та «кібернетична безпека». Висвітлюються питання вже наявних повноважень суб'єктів забезпечення кібернетичної безпеки.

Ключові слова: національна безпека, кібернетична безпека, кібернетичний простір, інформаційна безпека, інформаційне суспільство.

В статье рассматриваются проблемы нормативно-правового регулирования обеспечения кибернетической безопасности. Исследуется сущность отдельных нормотворческих инициатив в рассматриваемой сфере. Анализируется соотношение понятий «национальная безопасность», «информационная безопасность» и «кибернетическая безопасность». Освещаются вопросы уже имеющихся полномочий субъектов обеспечения кибернетической безопасности.

Ключевые слова: национальная безопасность, кибернетическая безопасность, кибернетическое пространство, информационная безопасность, информационное общество.

The article is a study of current legislation and current legislative initiatives in the field of cyber security of Ukraine.

Given the rapid development of the global information society, the use of ICT in all spheres of life are particularly important issues of information security. The legislator defines it as a state of protection of vital interests of man, society and the state in which the damage is prevented through: incomplete, untimely and unreliability of information used; negative information influence; the negative effects of information technology; unauthorized distribution, use and violation of the integrity, confidentiality and availability of information.

One element of information security is cybersecurity safety. Today in domestic science and law, no uniform approach to the definition of «cyber security» (the same applies to the term «cyberspace»). Given the existing definition of cybersecurity bills, we propose to define the term as follows: cyber security – a state of protection of vital interests of man and citizen, society and the state in the functioning of information, telecommunication and information and telecommunication systems.

As defined in the UN General Assembly resolution of December, 20, 2002 № 57/239, security should be provided in a way consistent with the values recognized by democratic society, including the freedom to exchange thoughts and ideas, the free flow of information, confidentiality and communication adequate protection of personal information, openness and transparency.

An analysis of the current legislation, the problems that arise in the area of cyber security Ukraine is not so much the result of a lack of sufficient legal framework because of inefficient relevant state bodies authorized to ensure data protection in the use of computer systems and computer networks and telecommunications.

Key words: national security, cyber security, cyberspace, information security, information society.

За умов швидкого розвитку глобального інформаційного суспільства, широкого використання інформаційно-комунікаційних технологій в усіх сферах життя особливого значення набувають проблеми інформаційної безпеки. Законодавець визначає її як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1]. Одним з елементів інформаційної безпеки є кібернетична безпека.

Метою статті є дослідження чинного законодавства, а також наявних законотворчих ініціатив у сфері забезпечення кібернетичної безпеки України.

Як відзначалося у Доктрині інформаційної безпеки 2009 року та у проекті Доктрини інформаційної безпеки 2014 року, інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку [2; 3].

Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки, надання всебічної державної підтримки національним виробникам інформаційного продукту та телекомунікаційного обладнання, створення нормативно-правових, фінансових та інших передумов, необхідних для їх успішної конкуренції на світовому та національному ринках інформаційних та телекомунікаційних послуг.

За оцінками експертів у сфері кібербезпеки переважної більшості провідних країн світу відмічається стійка тенденція до значного зростання кількості та розширення спектра кібератак з метою порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури.

На сьогодні, реальні прояви кібератак мало прогнозовані, а їх результатом є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони [4].

Проблеми кібернетичної безпеки розглядалися у тому числі на міжнародному рівні. Так, за рік до проведення І етапу Всесвітнього саміту з питань інформаційного суспільства (Женева, грудень 2003 року) Генеральною Асамблеєю (далі – ГА) ООН було прийнято Резолюцію, зміст якої пов'язаний з питаннями забезпечення кібернетичної безпеки. Зокрема, у Резолюції визнається, що:

– в ході процесу дедалі більшого залучення країн до інформаційного суспільства зростає необхідність забезпечення кібербезпеки;

– ефективна кібербезпека залежить не лише від дій державних або правоохоронних органів і вона повинна досягатися превентивними заходами і користуватися підтримкою в усьому суспільстві;

– державні органи повинні знати про відповідні фактори, що загрожують кібербезпеці, і про превентивні заходи і мають усвідомлювати свою відповідальність і вживати заходів щодо підвищення безпеки інформаційних технологій.

Крім того, у Резолюції розкривається зміст елементів глобальної культури кібербезпеки. ГА ООН пропонує державам-членам враховувати їх для створення глобальної культури кібербезпеки, зокрема в рамках їхніх зусиль щодо розвитку у своїх суспільствах культури кібербезпеки при застосуванні і використанні інформаційних технологій.

У Резолюції відзначається також важливе значення міжнародного співробітництва в цілях досягнення кібербезпеки шляхом підтримки національних зусиль, спрямованих на укріплення людського потенціалу, розширення можливостей в плані навчання і зайнятості, покращення державних послуг і підвищення якості життя за рахунок використання передових, надійних та безпечних інформаційно-комунікаційних технологій і мереж, а також сприяння забезпеченню загального доступу [5].

Глобальна культура кібербезпеки вимагатиме від усіх учасників врахування дев'яти взаємопов'язаних елементів, основним з яких, на наш погляд, є елемент «е) демократія»: безпека повинна забезпечуватися таким чином, щоб це відповідало цінностям, які визнаються демократичним суспільством, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації і комунікації, належний захист інформації особистого характеру, відкритість і гласність. Підтвердженням тому є документи Всесвітнього саміту з питань інформаційного суспільства (Женева, 2003 рік; Туніс, 2005 рік), у яких декларується те саме.

У Женевській декларації принципів, прийнятій на Всесвітньому саміті з питань інформаційного суспільства у грудні 2003 року, зазначається: «Необхідно формувати, розвивати і впроваджувати глобальну культуру кібербезпеки в співробітництві з усіма заінтересованими сторонами і компетентними міжнародними органами. Ці зусилля повинні спиратися на все ширше міжнародне співробітництво. У рамках цієї глобальної культури кібербезпеки важливо підвищувати безпеку і забезпечувати захист даних і недоторканності приватного життя» (п. 35) [6].

У свою чергу, в Туніській програмі для інформаційного суспільства (п. 39) наголошується таке: «Ми прагнемо підвищувати довіру і безпеку при використанні ІКТ шляхом зміцнення основи для довіри. Ми знову підтверджуємо необхідність далі просувати, розвивати і впроваджувати у співробітництві з усіма заінтересованими сторонами глобальну культуру кібербезпеки, як це викладено в резолюції 57/239 ГА ООН та інших відповідних регіональних основоположних документах. Ця культура потребує національних дій та активізації міжнародного співробітництва для зміцнення безпеки при підвищенні захисту особової інформації, недоторканності приватного життя і даних» [7].

Забезпечення кібернетичної безпеки набуває, без сумніву, важливого значення. У Стратегії кібербезпеки України зокрема відзначається таке: «Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави» [8].

На сьогодні на нормативно-правовому рівні визначення терміну «кібербезпека» міститься лише у вищезазначеній Стратегії, тобто на підзаконному рівні і звучить, як: стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [8].

Слід вказати, що на законодавчому рівні спроби визначити термін «кібербезпека» продовжуються, починаючи з 2012 року. Отже, є сенс здійснити порівняння наявних варіантів визначення цього терміну.

Так, згідно законопроекту від 31 серпня 2012 року № 11125 «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України» кібернетична безпека держави – це стан захищеності об'єктів критичної інформаційної інфраструктури країни (кіберпростір держави), сформований комплексом технологічних, технічних та інформаційних заходів і засобів кіберзахисту від зовнішніх та внутрішніх несанкціонованих посягань, реальних та потенційних кібернетичних загроз [9].

В урядовому законопроекті від 07 травня 2013 року № 2483 кібернетична безпека (кібербезпека) тлумачиться як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [10].

Наступним був проект Закону України від 28 травня 2014 року № 4949 «Про засади інформаційної безпеки України», згідно якого: кібернетична безпека (кібербезпека) – здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та інформаційно-комунікаційних систем і мереж [11].

На думку авторів законопроекту від 14 квітня 2015 року № 2126 «Про основні засади забезпечення кібербезпеки України», кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [12].

У законопроекті від 19 червня 2015 року № 2133а «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю» також пропонується визначити термін «кібербезпека», але зроблено це неординарним способом: і визначення кібернетичної безпеки, і деякі інші «новели» просто скопійовано із законопроекту від 07 березня 2013 року № 2483.

З перелічених визначень ми можемо зробити висновок, що «кібербезпека» – це все ж таки «стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави», а не власне «захищеність…» або «здатність… запобігати, протидіяти…». Але замість розпливчастого «кіберпростору» ми пропонуємо визначити термін «кібербезпека» таким чином: кібербезпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави у сфері функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Станом на сьогодні очікують на розгляд в парламенті законопроекти № 2126а і 2133а. Слід окремо наголосити, що спроби визначити в проекті Закону № 2126а окремі терміни за допомогою їх тлумачення довжиною на півсторінки не додадуть ясності розглядуваній нами сфері кібернетичної безпеки. Це стосується термінів «інцидент кібербезпеки (кіберінцидент)», «кібератака», «національні електронні інформаційні ресурси», «національна телекомунікаційна мережа», «система електронних комунікацій».

Стосовно термінології, яка застосовується у Стратегії кібербезпеки України, необхідно відзначити, що більша частина термінів не розтлумачена. Не зрозуміло, наприклад, що означають поняття: «кіберпростір», «кіберзахист», «інформаційна інфраструктура» (а, відповідно, і – «критична інформаційна інфраструктура»), «електронні комунікації» (і, відповідно, – «інфраструктура електронних комунікацій»), «кіберінцидент», «кібератака», «кібертероризм», «кібершпигунство». У Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року префікс «кібер» повторюється 8 разів. І всі ці рази він виступає як частина слова «кіберзлочинність». Так чи потрібне нам це розмаїття нез'ясованої термінології? До речі, притягнути до кримінальної відповідальності за «кібертероризм» або «кібершпигунство» за такого рівня юридичної визначеності не буде складно. Про заходи щодо цього ми читаємо в останньому розділі Стратегії. Зокрема, «боротьба з кіберзлочинністю передбачатиме здійснення в установленому порядку, серед іншого, таких заходів:

– унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік;

– врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису;

– запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів» (до речі, у Кримінальному процесуальному кодексі України використовується термін «зняття інформації з транспортних телекомунікаційних мереж»).

Також по тексту Стратегії виникають такі питання:

– як співвідносяться між собою терміни «захист у кіберпросторі» і «кіберзахист»?

– що означають складові словосполучення «надання послуг із захисту інформації та кіберзахисту»?

– чи може поняття «захист інформації» бути ширше за обсягом, ніж «кіберзахист», і включати його до себе? А, якщо так, тоді навіщо їх перелічувати, як однопорядкові члени речення?

І ми не можемо відповісти на ці питання, оскільки у законодавстві України немає тлумачення терміну «кіберзахист».

Відсутність правової визначеності означає порушення принципу верховенства права, який закріплено у ст. 8 Конституції України. На необхідності додержання цього принципу у діяльності державних органів неодноразово наголошено у рішеннях Європейського суду з прав людини, у документах Ради Європи, а також Венеціанської комісії.

Нарешті, слід наголосити на зауваженнях, що залишаються актуальними для всіх законопроектів з приводу кібербезпеки (тепер ці зауваження ми відносимо і до Стратегії кібербезпеки України).

Законопроект виглядає вразливим у концептуальному відношенні, оскільки він практично не має нормативно-правового навантаження, перевантажений складними і довгими визначеннями понять, різнорідних цілей та дублюванням загальних правових норм. На наш погляд, такий підхід до нормопроектування є хибним, оскільки він не вносить нічого нового у регулювання відповідних суспільних відносин і ускладнює розуміння та застосування чинних правових норм. Підставою для такого висновку є наступні конкретні зауваження.

Інформаційні відносини, пов'язані із забезпеченням кібернетичної безпеки, вже врегульовані Законами України «Про інформацію», «Про науково-технічну інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації» та ін.

При цьому ключова роль у забезпеченні кібернетичної безпеки покладається на Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Зокрема, в ньому визначаються необхідні для відповідних цілей терміни («блокування інформації», «виток інформації», «захист інформації», «комплексна система захисту інформації», «інформаційна (автоматизована) система», «криптографічний захист інформації», «несанкціоновані дії

щодо інформації в системі», «технічний захист інформації» тощо), об'єкти захисту та суб'єкти відповідних відносин, умови обробки інформації та способи забезпечення захисту інформації в системі, повноваження державних органів у сфері захисту інформації в автоматизованих системах.

Відповідно до ст. 10 вказаного вище Закону, спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (яким є Адміністрація Державної служби спеціального зв'язку та захисту інформації України):

– розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

– визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

– здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням з уповноваженим органом у сфері захисту інформації встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом [13].

Відповідні повноваження Національної поліції визначено у Законі України «Про Національну поліцію».

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Служба безпеки України забезпечує контррозвідувальний захист інтересів держави у сфері інформаційної безпеки.

За відповідні правопорушення у зазначеній сфері чинним законодавством передбачена адміністративна та кримінальна відповідальність. Зокрема, ст. 212-6 Кодексу України про адміністративні правопорушення передбачено відповідальність за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем.

У Кримінальному кодексі України вказаним діянням присвячено окремий Розділ XVI Особливої частини, яким передбачено кримінальну відповідальність за:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2);

4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1).

З огляду на зазначене є достатні підстави вважати, що чинне законодавство України вже містить достатню кількість правових норм, спрямованих на правову охорону кібернетичної безпеки України.

Кібернетична безпека є складовою інформаційної безпеки. У свою чергу, інформаційна безпека є одним з елементів національної безпеки держави. На сьогодні у вітчизняній науці та юриспруденції немає єдиного підходу до визначення терміну «кібернетична безпека» (те саме відноситься і до терміну «кібернетичний простір»). Але проблеми, які виникають у сфері забезпечення кібернетичної безпеки України, є не стільки результатом відсутності достатньої законодавчої бази, скільки результатом недостатньо ефективної діяльності відповідних державних органів, уповноважених забезпечувати захист інформації у процесі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

ЛІТЕРАТУРА

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09 січня 2007 року № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

2. Про Доктрину інформаційної безпеки : Указ Президента України від 08 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua

3. Про затвердження Доктрини інформаційної безпеки : Проект указу Президента України [Електронний ресурс]. – Режим доступу : comin.kmu.gov.ua

4. Пояснювальна записка до проекту Закону України «Про основні засади забезпечення кібербезпеки України» (реєстр. № 2126а від 14 квітня 2016 року) [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua

5. Створення глобальної культури кібербезпеки : Резолюція Генеральної Асамблеї ООН від 20 грудня 2002 року № 57/239 [Електронний ресурс]. – Режим доступу : www.un.org/ru/ga/second/57/second_res.shtml

6. Женевська декларація принципів від 12 грудня 2003 року [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua

7. Туніська програма для інформаційного суспільства [Електронний ресурс]. – Режим доступу : http://uadocs.exdat.com/docs/index-500325.html?page=6

8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»» : Указ Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua

9. Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України : Проект Закону України (реєстр. № 11125 від 31 серпня 2012 року) [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua

10. Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» : Проект Закону України (реєстр. № 2483 від 07 березня 2013 року) [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua

11. Проект Закону України «Про засади інформаційної безпеки України» (реєстр. № 4949 від 28.05.2014 р.) // [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua

12. Проект Закону України «Про основні засади забезпечення кібербезпеки України» (реєстр. № 2126 від 14.04.2015 р.) // [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua

13. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.