УДК 340.13+007.51+165.12

БАРАНОВ О.А., *кандидат технічних наук, старший науковий співробітник*

ПРО ТЛУМАЧЕННЯ ТА ВИЗНАЧЕННЯ ПОНЯТТЯ “КІБЕРБЕЗПЕКА”

Анотація. *Дослідження дефініції терміна “кібербезпека”.*
Ключові слова: *інформація, інформаційна безпека, кібербезпека.*

Аннотация. *Исследование дефиниции термина “кибербезопасность”.*
Ключевые слова: *информация, информационная безопасность, кибербезопасность.*

Summary. *Research of the “cybersecurity” term definition.*
Keywords: *information, information security, cybersecurity.*

Постановка проблеми. Все більш широке використання в останні 30-40 років у найрізноманітніших сферах життєдіяльності соціуму комп’ютерних і телекомунікаційних технологій, у тому числі Інтернет-технологій, разом з великою кількістю переваг привнесло також і чималу кількість загроз. Реалізація цих загроз може завдати значної шкоди як на мікро, так і на макрорівні в рамках суверенних держав, а також і в світовому масштабі. Це привело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації цієї нової сукупності загроз. Одночасно з цим виникає термін “кібербезпека”. Вважають, що вперше він виник у середині 1990-х років, коли уряд США став досліджувати цю тему [1].

З того часу відбулося досить багато міжнародних і національних форумів, конференцій, семінарів на різних рівнях, опубліковано багато наукових робіт, присвячених найрізноманітнішим аспектам кібербезпеки. Велика кількість країн прийняли або розробляють стратегії кібербезпеки (США, Німеччина, Франція, Канада та багато інших) [2 – 5]. Частина з них активно створюють інституційні системи кібербезпеки. Однак, як правильно зауважує В.П. Шеломенцев, в законодавстві відсутнє визначення не тільки поняття “кібернетична безпека (кібербезпека)”, а й таких понять, як “кібернетичний простір (кіберпростір)”, “кібернетична загроза (кіберзагроза)”, “кібернетична атака (кібератака)”, “кібернетичний захист (кіберзахист)”, “кіберзлочинність” тощо [6].

У цих умовах актуальною є проблема визначення змісту терміна “кібернетична безпека”. І цьому є кілька причин.

По-перше, класична причина – дефініція терміна дозволяє вичерпно окреслити предмет досліджень і дискусій, коло проблем, які можуть бути при цьому зачеплені.

По-друге, проблема кібербезпеки в силу своєї специфіки є глобальною і тому найбільш ефективно може бути вирішена лише за умови об’єднання зусиль найширших кіл міжнародних гравців як на державному рівні, так і на рівні приватних корпорацій і асоціацій. Тому для забезпечення ефективності взаємодії на міжнародному рівні необхідно узгоджене розуміння терміна кібербезпека.

Безсумнівно, ці та ряд інших факторів і визначають необхідність якомога якнайшвидшої “стандартизації” терміна “кібернетична безпека”.

Метою статті є проведення подальших досліджень у сфері “кібернетичної безпеки”, визначення дефініції цього терміна та розкриття його зв’язку із терміном “інформаційна безпека”.

Виклад основних положень Деякі експерти, також як і Д. Франсело, вважають, що останнім часом термін cybersecurity все частіше і частіше використовується, але при цьому багато керівників служб безпеки і просто експерти з інформаційної безпеки досі плутаються в тому, коли і як використовувати цей термін [7].

Проведемо аналіз дефініцій терміна “кібернетична безпека”, які наведені в деяких національних стратегічних документах. У стратегії Франції, присвяченій питанням кібербезпеки, дано таке визначення: кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов’язаних з ними послуг, які ці системи пропонують або роблять доступними [3].

Насамперед, треба розуміти, що відповідно до цього визначення кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об’єктів, на які можуть діяти якісь загрози з кіберпростору, послуг інформаційних систем це визначення терміна дозволяє мати на увазі наявність якихось загроз функціональності систем більш високого порядку, до яких в якості складових елементів входять інформаційні системи. Це положення має важливий методологічний зміст у розумінні місця і ролі проблеми кібербезпеки в контексті інших видів безпеки.

У німецькій стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків [5]. При цьому в стратегії стверджується, що кібербезпека повинна базуватися на комплексному підході. Це досить прагматична точка зору, яка дозволяє розробляти практичні кроки щодо забезпечення кібербезпеки, проте вона не надає достатніх методологічних підстав для проектування та оцінки систем, що забезпечують цю безпеку. Про це побічно свідчить зміст десяти стратегічних напрямів у стратегії забезпечення кібербезпеки, оголошених федеральним урядом Німеччини [5].

У Канаді стверджують, що з метою забезпечення найсучаснішого використання кіберпростору, який є стратегічним активом, необхідно передбачати і протистояти кіберзагрозам, що виникають [2]. У канадській стратегії кібербезпеки не міститься чіткого визначення того, що являє собою кібербезпека. Відповідно до цього документа під кібербезпекою можна розуміти захист киберсистем від шкідливого неправильного використання та від інших деструктивних атак. З іншого боку, надано досить докладне визначення кібератаки, а кібербезпека – це засіб захисту від цих загроз.

Кібератаки включають ненавмисні або несанкціонований доступ, використання, маніпуляції, переривання або знищення (через електронні засоби) електронної інформації та/або електронної та фізичної інфраструктури, що використовується для обробки, зв’язку, та/або баз даних [2]. При цьому рівень кібербезпеки визначається рівнем шкоди, що може бути завданий від кібератаки.

В цілому, канадська стратегія таки розглядає основний збиток від реалізації кіберзагроз як збиток, який можуть мати системи життєзабезпечення та підтримки діяльності всієї країни, бізнесу та окремого громадянина.

Одна із найостанніших за часом національних стратегій кібербезпеки (Турецька Республіка) містить таке визначення: кібербезпека – захист інформаційних систем, що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам [8]. При цьому під кіберпростором розуміється середовище, що

складається з інформаційних систем, розподілених по всьому світу, в тому числі мереж, що з’єднують ці системи. Національний кіберпростір визначається як простір, який складається з інформаційних систем суб’єктів, що перебувають під юрисдикцією Турецької Республіки.

У Нідерландах також приділяють велику увагу наявності загроз інформаційній інфраструктурі в умовах широкого застосування цифрових (комп’ютерних) технологій. Національним координатором з безпеки та боротьби з тероризмом в 2013 році була опублікована Національна стратегія кібербезпеки. На думку авторів стратегії, кібербезпека – це сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз [9]. До збоїв стратегія відносить зниження надійності ІКТ, обмеження доступності та порушення конфіденційності та/або цілісності інформації, що зберігається в системах ІКТ. Таке тлумачення робить вельми складним вирішення проблеми визначення критеріїв забезпечення кібербезпеки.

Однак у цій стратегії було зроблено вельми важливий в методологічному аспекті висновок – кібербезпека може бути досягнута тільки в системній кореляції з вирішенням проблем захисту та забезпечення основних прав, цінностей і соціально-економічних вигод членів соціуму.

Метою політики кібербезпеки австралійського уряду є підтримка безпечної, стійкої і надійної роботи електронного операційного середовища, яке підтримує національну безпеку Австралії та максимізує переваги цифрової економіки [10]. В опублікованій у 2009 році Стратегії під кібербезпекою розуміється забезпечення доступності, цілісності та конфіденційності ІКТ Австралії, а також захист людей, особливо дітей, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і від використання ІКТ для цілей сексуальної експлуатації [10].

В українському законопроекті запропоновано свій варіант визначення кібербезпеки, під якою розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави в кіберпросторі [11]. При цьому в законопроекті кіберпростір – середа, яка виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Дане визначення має дуже низький методологічний потенціал і не дозволяє конкретизувати особливості кібербезпеки. Більше того, абсолютно необґрунтовано до кібербезпеки віднесені проблеми функціонування інформаційних систем в загальному сенсі, внаслідок чого до проблематики кібербезпеки можуть бути віднесені телебачення і радіо, а також навіть бібліотеки та архіви.

З урахуванням того, що проблема кібербезпеки носить глобальний характер, вельми цікавою видається позиція міжнародних організацій. Так, Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у своїй Рекомендації дає таке визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача [12]. При цьому ресурси організації та користувача включають під’єднані комп'ютерні пристрої, персонал, інфраструктуру, додатки, послуги, системи телекомунікацій і всю сукупність переданої та/або збереженої інформації в кіберсередовищі, а мета кібербезпеки полягає в спробі досягнення і збереження властивостей безпеки ресурсів організації або користувача, спрямованих проти

відповідних загроз безпеки в кіберсередовищі. Загальні завдання забезпечення безпеки включають таке: доступність; цілісність, яка може включати автентичність і безвідмовність; конфіденційність [12].

У Європейському Союзі у зв’язку з розумінням важливості проблеми кібербезпеки в 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки [13]. У 2012 році це Агентство опублікувало огляд “Національні стратегії кібербезпеки. Практичний посібник з розвитку та виконання” [14]. Щодо визначення терміна “кібербезпека” в цьому огляді сказано таке: в національних стратегіях не існує ні загальноприйнятого, ні однозначного визначення кібербезпеки.

Таким чином, можна констатувати, що на рівні національних та міжнародних стратегічних документів визначення кібербезпеки значно різняться. А значить, розрізняються і підходи не тільки до змісту відповідних стратегій, а й до змісту планів дій із забезпечення кібербезпеки. Однак транскордонний характер цієї проблеми настійливо диктує необхідність координації зусиль як на національному, так і на міжнародному рівні. Передусім, мова йде про осмислення суті кіберзагроз, змісту робіт щодо забезпечення кібербезпеки, чітке визначення цілей стратегії і власне визначення змісту самого терміна “кібербезпека”.

З урахуванням того, що термін “кібербезпека” отримав значного поширення не тільки в середовищі фахівців, а й у різних міжнародних і національних документах, пропонується не розгортати дискусію власне про назву самого терміна, незважаючи на те, що вона викликає обґрунтовані нарікання у багатьох фахівців.

Деякі західні фахівці запевняють, що слово “cyber” пов’язане з використанням інформаційних технологій і комп’ютерів [1]. Цю ж позицію займає і Д.В. Грибанов, який обґрунтовуючи необхідність застосування в правовій науці терміна “кібернетичний простір”, розуміє під ним сукупність суспільних відносин, що виникають в процесі використання функціонуючої електронної комп’ютерної мережі, що складається з приводу інформації, яка обробляється за допомогою ЕОМ, і послуг інформаційного характеру, що надаються за допомогою ЕОМ та засобів зв’язку комп’ютерної мережі [15].

В цілому слід зазначити, що практично всі національні стратегії щодо забезпечення кібербезпеки і переважна більшість експертів пов’язують проблематику кібербезпеки саме з використанням у процесі людської діяльності комп’ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет).

Дійсно, саме з початку використання комп’ютерних технологій, особливо у сукупності із телекомунікаційними мережами, виникає особливий клас загроз інформаційній безпеці. Ситуація набуває ще більшого загострення разом з поширенням використання мережі Інтернет. Але широких масштабів проблема кібербезпеки набула тоді, коли можлива шкода від реалізації загроз у сферах, де використовувались комп’ютерні системи та телекомунікаційні мережі, стала досягати великих обсягів. Це пояснюється значним коефіцієнтом “корисної” дії цих загроз, тому що обсяг ресурсів, що витрачаються на реалізацію загроз, є набагато меншим, ніж результати, що отримуються.

Існує й інша точка зору, яку М.С. Соколов висловив таким чином: використання термінів, похідних від терміна “кібернетика”, наприклад, таких як “кібернетична атака”, “кібернетична безпека”, “кіберпростір”, “кіберсфера”, “кіберзлочинність”, “кібервійна”, “кібероборона”, є виправданим у разі опису явищ або фактів, безпосередньо пов’язаних із системами і процесами управління [16].

Дійсно, процеси управління нерозривно пов'язані з інформаційними процесами як у процесі підготовки управлінських рішень, так і безпосередньо у процесі управління. Сучасні системи управління, особливо великими територіально-розподіленими

соціотехнічними системами (системи управління енергетичною інфраструктурою, повітряним і залізничним рухом, банківськими та фінансовими системами, великими промислово-виробничими комплексами тощо), неможливо уявити без використання комп’ютерних систем і телекомунікаційних мереж. Тому розуміння кібербезпеки як проблеми, пов’язаної із системами управління, не суперечить тим поглядам, які висловлюють більшість експертів за умови того, що ця проблема буде розумітися як часткова проблема у всій проблематиці кібербезпеки.

Таким чином, можна зробити перший висновок про те, що основною кваліфікуючою ознакою віднесення до проблематики кібербезпеки є обов’язкова умова використання комп'ютерних систем і телекомунікаційних мереж.

Українські дослідники пропонують своє бачення терміна кібербезпеки. Так деякі з них вважають, що в контексті нормативно-правового розуміння національної та інформаційної безпеки кібербезпека може визначатися як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем [17]. Цим визначенням автори визначають в якості об’єкта загроз – національні інтереси у сфері функціонування інформаційно-телекомунікаційних систем, що значно звужує поле можливих життєво важливих інтересів людини і громадянина, суспільства і держави. Крім того, пропозиція використовувати в якості критерію захищеності життєво важливих інтересів людини і громадянина, суспільства і держави критерій “стабільний розвиток суспільства” не дозволяє сформувати методологічну основу для оцінки рівня такої захищеності, оскільки важко дати кількісні оцінки “стабільного розвитку”.

В.Н. Фурашев визначає кібербезпеку як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації [18].

Методологічно важливим для визначення обсягу юрисдикції поняття кібербезпеки є знання об’єкта можливих загроз, а також видів і типів можливого збитку. Ці знання і розуміння мають високу практичну цінність, оскільки саме від них залежить зміст стратегій кібербезпеки, охоплення об’єктів, які підпадають під заходи щодо забезпечення кібербезпеки, рівень і перелік інституцій та органів, склад і обсяги ресурсів, які повинні бути при цьому задіяні.

Виходячи з цільового призначення систем, що містять в якості складових комп’ютерні системи та телекомунікаційні мережі, можна зробити висновок про те, що кіберзагрози насамперед спрямовані на порушення обігу інформації. При цьому мова може йти як про фундаментальні системні загрози, пов’язані з порушенням власне обігу інформації на будь-якому з його етапів – створенні, поширенні, використанні, зберіганні і знищенні інформації, так і про загрози, пов’язані з недостовірністю, несвоєчасністю і неповнотою інформації. Крім того, до цього класу загроз слід віднести загрози, пов’язані з несанкціонованим використанням та поширенням інформації, порушенням її цілісності та конфіденційності.

Отже, другий висновок полягає в тому, що проблематика кібербезпеки має відношення до обороту інформації, зокрема, до забезпечення суб’єктів інформаційних відносин достовірною, своєчасною та повною інформацією, а також до недопущення несанкціонованого використання і поширення інформації, порушення її цілісності та конфіденційності.

Широке використання в останні роки комп’ютерних систем і телекомунікаційних мереж для створення та розповсюдження інформації істотно підвищило ефективність цих процесів, а отже, і ефективність інформаційного впливу. Однак поряд з позитивом комп'ютерні системи та телекомунікаційні мережі також дозволили істотно підвищити ефективність негативного інформаційного впливу. Не проводячи детальний аналіз видів і типів таких впливів, скажемо тільки, що левова частка з них пов’язана з використанням інтернет-технологій. Тому протидія негативному інформаційному впливу іноді здійснюється не на контентному рівні, а на технологічному. Тобто у цьому випадку протидія може бути віднесена до заходів із кібербезпеки.

Ось для цієї ситуації зробимо третій висновок, який полягає в тому, що з проблемою кібербезпеки пов’язана проблема нейтралізації негативних інформаційних впливів на технологічному рівні.

Непоодинокі випадки, коли функціонування соціальних і соціотехнічних систем повністю базується на використанні якихось технічних комплексів комп’ютерних систем і телекомунікаційних мереж. Тому досягнення цілей функціонування цих соціальних і соціотехнічних систем залежить від якості, надійності та стабільності роботи цих комплексів. Або іншими словами, порушення функціонування комп’ютерних систем і телекомунікаційних мереж може призвести до погіршення або навіть припинення роботи соціальних і соціотехнічних систем, елементами яких вони є.

А це означає, що такі комплекси (комп'ютерні системи та телекомунікаційні мережі) зобов’язані належним чином проектуватися, будуватися, здаватися в експлуатацію, експлуатуватися, супроводжуватися проектантами і виробниками тощо. Недоліки в нормативно-правовому та нормативно-технічному забезпеченні цих процесів, прорахунки в їх організації та реалізації, які можуть призвести до порушення функціонування комп’ютерних систем і телекомунікаційних мереж у процесі їх експлуатації, становлять окрему групу кіберзагроз.

Крім того, при створенні соціальних та соціотехнічних систем, елементи яких знаходяться на різних територіях і на значній відстані, досить важливим фактором є забезпечення оптимального проектування топології територіальнорозподілених комп'ютерних систем та телекомунікаційних мереж з метою забезпечення їх інфраструктурної стійкості та достатності. Недотримання або невиконання вимог інфраструктурної стійкості та достатності територіальнорозподілених комп’ютерних систем та телекомунікаційних мереж може призвести до погіршення або навіть припинення роботи соціальних і соціотехнічних систем, елементами яких вони є.

Приходимо до четвертого висновку – серед проблем кібербезпеки є проблема забезпечення інфраструктурної безпеки соціальних та соціотехнічних систем, що використовують комп’ютерні системи та телекомунікаційні мережі, або іншими словами, проблема, пов’язана з завданням можливого збитку через негативні наслідки використання інформаційних комп’ютерних технологій [19].

Деякі експерти при дослідженні об’єктів кібербезпеки не уникають спокуси перерахувати конкретні види або навіть типи технічних систем, що містять комп'ютерні та телекомунікаційні технології [6]. Але тоді в якості збитку доведеться розглядати тільки лише збої у функціонуванні цих технічних систем. Насправді технічні системи є лише складовими елементами систем більш високого порядку – соціальних та соціотехнічних систем і призначені для забезпечення їх функціонування чи діяльності. Прикладом можуть служити банківські автоматизовані системи “банк-банк” або “банк-клієнт”, які являють собою сукупність комп’ютерних і телекомунікаційних технологій. Збої у функціонуванні цих автоматизованих систем призводять, насамперед, до

порушення інформаційного обміну між банками та їх клієнтами. А вже системним збитком для банків є зрив фінансового обороту, для якого інформаційний обмін є необхідною умовою.

Наведений приклад, а також маса інших, свідчать про те, що, врешті-решт, всі можливі види і типи збитку, які можуть мати місце в результаті порушення кібербезпеки, зводяться до збитку, який безпосередньо несуть соціальні та соціотехнічні системи. Або для загального випадку можна стверджувати, що порушення кібербезпеки призводить до зниження рівня захищеності життєво важливих інтересів людини, суспільства і держави. Ця обставина знайшла відображення в багатьох національних стратегіях кібербезпеки або в частині, де надається обґрунтування, або в частині, в якій описуються напрями проведення заходів для забезпечення кібербезпеки.

Таким чином, приходимо до п’ятого висновку: базова мета забезпечення кібербезпеки – це забезпечення стану захищеності життєво важливих інтересів людини, суспільства і держави.

Кібербезпека не є річчю в собі, замкнутої тільки на комп’ютерних системах та/або телекомунікаційних мережах. Із системних позицій заходи щодо забезпечення кібербезпеки насамперед спрямовані на збереження якості функціонування соціальних і соціотехнічних систем, до складу яких входять відповідні комп’ютерні системи та телекомунікаційні мережі. Тому основними критеріями ефективності заходів щодо забезпечення кібербезпеки повинні бути критерії, що базуються на оцінці якості функціонування соціальних і соціотехнічних систем. Наприклад, якщо реалізація кіберзагроз навіть і призводить до порушення роботи комп’ютерних систем, але це майже не позначається на якості функціонування відповідної соціальної або соціотехнічної системи, гострота проблеми забезпечення кібербезпеки різко падає.

Отже, зміст шостого висновку – проблема оцінки стану кібербезпеки повинна передусім розглядатися в нерозривному зв’язку з оцінкою можливих чи завданих збитків соціальним або соціотехнічним системам як системам більш високого порядку.

Похідним від цього останнього висновку є методологія визначення об’єктів критичної інфраструктури в контексті кібербезпеки. До об’єктів критичної інфраструктури в загальному випадку слід відносити ті інфраструктурні об’єкти, порушення функціонування яких призводить або може призвести до збитку для життєво важливих інтересів суспільства і держави. А для випадку кібербезпеки: об’єкти критичної інфраструктури – це інфраструктурні об’єкти, що мають у своєму складі комп’ютерні системи та/або телекомунікаційні мережі, порушення функціонування яких призводить або може призвести до збитку для життєво важливих інтересів суспільства і держави.

Автором у своїй роботі [19] було обґрунтовано дефініцію терміна “інформаційна безпека”, яка знайшла в подальшому законодавче закріплення у Законі України “Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”. Інформаційна безпека – стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого запобігається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [20].

На основі зіставлення результатів аналізу проблем визначення терміна “кібербезпека”, що були отримані вище, та законодавчого визначення терміна “інформаційна безпека” можемо зробити висновок про те, що кібербезпека – це окремий

випадок інформаційної безпеки, поява якого обумовлена використанням комп’ютерних систем та/або телекомунікаційних мереж.

В такому випадку можемо дати таке визначення: **кібербезпека** *–інформаційна безпека в умовах використання комп’ютерних систем та/або телекомунікаційних мереж.*

Або дамо розгорнуте визначення: **кібербезпека** – *це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.*

Висновки.

1. Надане в роботі визначення кібербезпеки засноване на діалектичному зв’язку категорій загального і одиничного у сфері інформаційної безпеки. Кібербезпека розглянута як одиничне стосовно інформаційної безпеки, яка виступає в якості загального.

2. Запропонований підхід дозволяє розглядати проблеми кібербезпеки з позицій відносно напрацьованої теоретичної та практичної бази інформаційної безпеки та створювати несуперечливі моделі правового регулювання в цих сферах.

Використана література

1. Stubley D. What is Cyber Security? – Режим доступу : //www.7elements.co.uk/resources/blog/what-is-cyber-security

2. Canada’s Cyber Security Strategy: For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada, 2010. – 14 с. – Режим доступу : //www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

3. Information systems defence and security: France’s strategy. – French Network and Information Security Agency. – 2011. – С. 23. – Режим доступу : //www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf

4. The national strategy to secure cyberspace. – Washington, 2003. – 60 с. – Режим доступу : //www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

5. Cyber Security Strategy for Germany. –Berlin : Federal Ministry of the Interior. – 2011. – 15 с. – Режим доступу : //www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

6. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 1. – С. 312-320.

7. Franscella J. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term / J. Franscella. – Режим доступу : //www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html

8. National Cyber Security Strategy and 2013-2014 Action Plan. – Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, 2013. – С. 47. – Режим доступу : //www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf

9. Национальная стратегия кибербезопасности (NCSS). От понимания к возможности. – Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. – Режим доступу : //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie

10. Cyber security strategy. – Commonwealth of Australia: Australian Government, 2009. – Режим доступу : //www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf

11. Про внесення змін до Закону України “Про основи національної безпеки України” : проект Закону України щодо кібернетичної безпеки України від 07.03.13 р. № 2483. – Режим доступу : //www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998

12. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. – Женева : МСЭ, 2009. – С. 55. – Режим доступу : //www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru

13. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) // Official Journal L 077, 13/03/2004 P. 0001-0011. – Режим доступу : //www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

14. National Cyber Security Strategies. Practical Guide on Development and Execution. –ENISA, 2012. – Режим доступу : //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

15. Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений : автореф. дис. на соискание ученой степени канд. юрид. наук : спец. 12.00.01 / Д.В. Грибанов. – Екатеринбург, 2003. – 23 с. – Режим доступу : http://law.edu.ru/book/book.asp?bookID=126348

16. Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности // Военное право. – 2012. – № 1. – Режим доступу : http://db.inforeg.ru/eni/artList.asp?j=4&id=0220913464&idfull=0421200099

17. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки : зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 22 березня 2011 р.). – К. : Вид-во НА СБ України, 2011. – Ч. 2. – С. 43-48.

18. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.

19. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К. : Видавничий дім “СофтПрес”, 2005. – 316 с.

20. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~