УДК 004.056.5:343.326 (045)

М. М. Присяжнюк, Є. І. Цифра
Навчально-науковий інститут інформаційної безпеки
Національної академії СБ України
вул. Михайла Максимовича, 22, 03022 Київ, Україна

Особливості забезпечення кібербезпеки

Проведено аналіз історичних передумов виникнення поняття «кіберпростір», розкрито особливості кіберзагроз, здійснено порівняльний аналіз стратегій кібербезпеки провідних країн світу, наведено комплекс проблем вітчизняної кібербезпекової сфери, обґрунтовано необхідність створення загальнодержавної системи забезпечення кібербезпеки та показано першочергові пріоритети та завдання щодо протидії загрозам у кіберпросторі України.

Ключові слова: *кіберпростір, кіберзагрози, кібербезпека.*

Постановка проблеми

Стрімкий розвиток інформаційних технологій, інформатизація та комп'ютеризація, створення глобального інформаційного простору сформували принципово нові субстанції — інформаційне суспільство, інформаційний і кібернетичний простори, які мають невичерпний потенціал і відіграють головну роль в економічному та соціальному розвитку країн світу. Однак, створення інформаційного суспільства може призвести до виникнення багатьох інформаційних загроз, а одним із головних завдань сучасної інформаційної епохи є забезпечення інформаційної та кібернетичної безпеки, тому тему «Кібербезпека держави» можна вважати актуальною.

Аналіз основних публікацій

Аналіз наукових публікацій В. Гібсона, М. Камчатного, О. Манжая, Л. Бурячка, Б. Толубка, В. Хорошка, С. Гнатюка та ін. щодо розкриття суті та значення поняття «кіберпростір», показав, що всі вони тлумачать це по-різному. Законодавство окремих країн показує також різні підходи до кібербезпеки, яка теж трактується ними по-різному.

Вітчизняні реалії свідчать про низку важливих проблем, що заважають ефективно протидіяти загрозам у кіберпросторі.

Метою статті є дослідження особливостей організації кібербезпеки провідними країнами світу та України. Для досягнення мети у статті вирішуються такі *завдання*: аналіз історичних передумов виникнення поняття «кіберпростір», розкриття особливостей кіберзагроз у кіберпросторі, порівняльний аналіз стратегій кібербезпеки провідних країн світу.

Виклад основного матеріалу

Науково-технічна революція початку XXI ст. спричинила в усьому світі глибокі системні перетворення. Поєднання досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) та стрімкого розвитку інформаційно-телекомунікаційних систем (ІТКС) викликало появу так званого віртуального простору, який ще отримав назву «кіберпростір». Він не має загальноприйнятих кордонів чи меж, проте повністю може вважатися міжнародним простором [1].

Уперше термін «кіберпростір» використав письменник В. Гібсон у 1982 р. у новелі «Палаючий Хром» («Burning Chrome»). На його думку, кіберпростір (cyberspace) — це створена галюцинація, під дією якої щодня перебувають мільярди звичайних операторів у всьому світі. Це логічне представлення відомостей, що збережені в пам'яті та на магнітних носіях комп'ютерів усього людства, потоки даних у просторі розуму; скупчення та сузір'я інформації [2].

Якщо розглядати кіберпростір як словосполучення «кібернетичний простір», то кіберпростір – це простір (територія), який створений та працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки інформації) [3].

Відповідно до міжнародного стандарту, кіберпростір — це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, якого не існує в будь-якій фізичній формі [4].

У нормативній базі США зазначено, що кіберпростір — це сфера, яка характеризується можливістю використання електронних і електромагнітних засобів для запам'ятовування, модифікування та обміну даними в мережевих системах і пов'язану з ними фізичну інфраструктуру.

За офіційними документами Євросоюзу, кіберпрострір — це віртуальний простір, у якому циркулюють електронні дані світових персональних комп'ютерів.

Для Великобританії кіберпростір — це всі форми мережевої цифрової активності, що включають у себе контент і дії, здійснювані через цифрові мережі.

У Німеччині вважають, що кіберпростір — це вся інформаційна інфраструктура, яка доступна через Інтернет поза будь-якими територіальними кордонами.

В Україні взагалі відсутнє стандартизоване поняття кіберпростору. Варто навести найбільш повні визначення вітчизняних фахівців щодо цього поняття.

Так С. Гнатюк, провівши багатокритеріальний аналіз, запропонував таке узагальнене визначення: кіберпростір — це віртуальний простір, що отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у т.ч. Інтернет) для підтримки та управління процесами перетворення інформації (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства [5].

В. Бурячок, В. Толубко, В. Хорошко та інші автори підручника «Інформаційна та кібербезпека: соціотехнічний аспект» наводять ще одне визначення кіберпростору як віртуального комунікаційного середовища, що утворений системою зв'язків між користувачами та об'єктами інформаційної інфраструктури, такими як електронний інформаційний ресурс, системи та мережі всіх форм власності, керовані автоматизованими системами управління, що використовуються не лише для перетворення та передачі інформації, яка в них циркулює, з метою забезпечення інформаційних потреб суспільства, а й для впливу на аналогічні об'єкти протиборчої сторони [6].

Відкритий кіберпростір розширює свободу та можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну й ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність і прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного кіберпростору обумовили виникнення нових загроз національній і міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Аналіз існуючих тенденцій свідчить, що терористичні організації для реалізації власної протиправної мети починають дедалі частіше вдаватися до кібератак. Сьогодні комп'ютерні атаки, що здійснюються терористами або хакерськими групами, афілійованими до терористичних організацій, як правило, направлені на:

— виведення з ладу ІТКС і систем зв'язку за допомогою вірусів, спаму;

— тимчасове блокування публічних веб-сайтів шляхом масованих DDOS-атак;

— атаки на офіційні веб-сайти або сторінки у соціальних медіаорганів державної влади та комерційних організацій з метою розміщення повідомлень терористичного спрямування;

— несанкціонований доступ у систему з метою викрадення даних або її використання в організації кібератак на інші системи (створення бот-мереж);

— незаконне оприлюднення персональних даних у мережі Інтернет стосовно політиків, правоохоронців чи військовослужбовців у поєднанні із прямими погрозами [7].

Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства та держави.

Кіберпростір поступово перетворюється на окрему, поряд із традиційними «Земля», «Повітря», «Море», «Космос», сферу ведення бойових дій, в якій активно діють відповідні підрозділи збройних сил провідних держав світу [8].

На сьогодні є основний напрямок бойових дій у кіберсфері: блокування серверів і інтернет-ресурсів за допомогою DDoS-атак.

Так в Україні хакерам вдалося атакувати десятки об'єктів критичної інфраструктури. Все почалося з того, що у травні 2014 року вони ледь не зірвали процес підведення підсумків президентських виборів. Вночі були атаковані сервери ЦВК з метою видалення даних про хід виборчого процесу. Чудом утрати даних вдалось уникнути. Цей епізод не став для України повчальним уроком. Наприкінці 2015 та 2016 років зловмисники провели декілька операцій, у ході яких у де-

яких регіонах країни тисячі споживачів залишилися без електроенергії, виходили з ладу електронні системи Укрзалізниці, на грані знищення опинилися дані Держказначейства якраз перед плануванням соціальних виплат і пенсій тощо [9].

Виникає необхідність нейтралізації подібних загроз.

З'являється термін «кібербезпека». Проте, загальноприйнятого визначення кібербезпеки у законодавстві допоки не існує.

Так у стратегії Франції, яка присвячена 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, та пов'язаних з ними послуг, які ці системи пропонують або роблять доступними [10].

У німецькій стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, у результаті реалізації яких досягається мінімізація ризиків [11].

У канадській стратегії кібербезпеки не міститься чіткого визначення того, що вона собою являє. Відповідно до цього документа під кібербезпекою можна розуміти захист кіберсистем від шкідливого неправильного використання та від інших деструктивних атак [12]. З іншого боку, надано досить докладне визначення кібератаки, а кібербезпека — це засіб захисту від цих загроз.

Одна із найостанніших за часом національних стратегій кібербезпеки (Турецької Республіки) містить таке визначення: кібербезпека — захист інформаційних систем, що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється у цьому просторі, виявлення та протидія атакам і кіберінцидентам [13].

За Національною стратегією кібербезпеки Нідерландів 2013 р. кібербезпека — це сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їхнього використання, а також з відновлення ІКТ після реалізації цих загроз [14].

Метою політики кібербезпеки австралійського уряду є підтримка безпечної, стійкої і надійної роботи електронного операційного середовища, яке підтримує національну безпеку та максимізує переваги цифрової економіки. В опублікованій у 2009 р. 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 [15].

Стратегія кібербезпеки України визначає це поняття як стан захищеності життєво важливих інтересів людини та громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних та інформаційних заходів [8].

В ЄС у зв'язку з розумінням важливості проблеми кібербезпеки в 2004 р. створено Європейське агентство з мережевої та інформаційної безпеки. У 2012 р. це Агентство опублікувало огляд «Національні стратегії кібербезпеки. Практичний посібник з розвитку та виконання», в якому сказано, що в національних стратегіях не існує ні загальноприйнятого, ні однозначного визначення кібербезпеки [16].

Отже, на рівні національних і міжнародних стратегічних документів визначення кібербезпеки значно різняться. А значить, різняться і підходи не лише до змісту відповідних стратегій, а й до планів дій із забезпечення кібербезпеки. Однак транскордонний характер цієї проблеми настійливо диктує необхідність координації зусиль як на національному, так і на міжнародному рівнях. Передусім, мова йде про осмислення суті кіберзагроз, змісту робіт щодо забезпечення кібербезпеки, чітке визначення цілей стратегії і власне визначення змісту самого терміну «кібербезпека».

На сьогоднішній день кіберпростір, через певну новизну, все ще не повністю нормативно врегульований на міжнародному рівні, тому спецоперації, що здійснюються в ньому військовими чи розвідувальними підрозділами, не підпадають під визначення «акту війни» і можуть бути віднесені до операцій «відмінних від війни». Фактично, йдеться про можливість забезпечити ефект військового втручання без подальших офіційних санкцій як з боку держави, що зазнала нападу, так і світового співтовариства. З огляду на рівень проникнення ІКТ у всі критично важливі сфери життєдіяльності людини та держави, таку можливість надає протистояння у кіберпросторі та ведення кібервійн. Крім того, це призводить до трансформації державної політики більшості провідних держав у питанні контролю за власним інформаційним (кібер) простором і посилення яскраво виражених обмежувальних тенденцій.

Україна також потребує створення адекватної системи безпеки у світі, де виклики національній безпеці все частіше набувають рис, що відмінні від традиційних загроз. Активність з боку провідних держав світу в кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах в кіберпросторі, обумовлюють необхідність вироблення рекомендацій щодо короткота довгострокових пріоритетів трансформації вітчизняного безпекового сектора.

Різке зростання кількості кібератак зловмисників на системи управління та об’єкти критичної інфраструктури країн світу стало глобальною ключовою проблемою сучасності. У зв’язку з цим провідними науковцями та фахівцями світу за темою кібербезпеки проводяться наукові та науково-практичні форуми з метою дослідження причин виникнення та технологій здійснення кіберзлочинів і вироблення пропозицій до стратегії ефективної міжнародної співпраці в області попередження та ліквідації наслідків кібератак і забезпечення кібербезпеки.

Вітчизняні реалії кібербезпекової сфери також свідчать про низку важливих проблем, що заважають створенню ефективної системи протидії загрозам у кіберпросторі. До таких проблем у першу чергу відносяться:

— термінологічна невизначеність;

— відсутність належної координації діяльності відповідних відомств;

— залежність України від програмних і технічних продуктів іноземного виробництва;

— складнощі з кадровим наповненням відповідних структурних підрозділів.

Можна відзначити, що питання підготовки кадрів певною мірою зрушило з місця. Так, після запровадження Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266, спеціальності галузі

знань «Інформаційна безпека» стали складовою підготовки фахівців за спеціальністю «125 Кібербезпека» галузі знань 12 «Інформаційні технології». З цією метою у навчальний процес Національної академії СБ України, Національного авіаційного університету, Національного технічного університету України «КПІ імені І. Сікорського» тощо впроваджуються навчальні програми за цим напрямом [17].

Проте кадрове наповнення відповідних підрозділів фахівцями по боротьбі з кіберзлочинністю почнеться лише через декілька років після їхнього випуску з українських ВНЗ.

В Україні також відсутні системні нормативні документи, що описували би саме загрози Україні у кіберпросторі, давали їхні визначення та формували цілісну державну політику із кібербезпеки. «Стратегія кібербезпеки України» (від 15 березня 2016 року) зазначає тільки чинники, через які можуть виникнути загрози, а опис самих загроз відсутній.

Україна все ще залишається вразливою (особливо її телекомунікаційна складова), не в останню чергу через надмірно широке впровадження західних програмних продуктів і використання матеріально-технічної бази іноземного виробництва. Актуальною залишається проблема створення національної операційної системи (принаймні для використання у системі органів державної влади, хоча для такого переходу до програмного забезпечення з відкритим кодом є і суттєві зауваження з боку ключових вітчизняних безпекових організацій), відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу.

Розглянувши комплекс проблем у сфері забезпечення кібербезпеки та констатуючи її кризовий стан, що загрожує національній безпеці, РНБО України розробила рішення «Про загрози кібербезпеці держави та невідкладні заходи з їхньої нейтралізації», яке Президент України своїм указом від 13.02.2017 р. № 32/2017 увів у дію [18].

За цим рішенням Президент України має визначити Генерального державного замовника Національної програми інформатизації з урахуванням актуальних загроз кібербезпеці держави.

Рішення визначає першочергові завдання та терміни їхнього виконання Кабінету Міністрів України, Службі безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Національній поліції України щодо підготовки законодавчих пропозицій і вжиття невідкладних заходів з метою: забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури; посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах; забезпечення повного та об'єктивного розслідування кібератак на інформаційно-телекомунікаційні системи фінансового сектора держави; виявлення та припинення фактів використання органами державної влади програмних продуктів, що розроблені суб'єктами господарювання держави-агресора, використання яких заборонено відповідно до рішень РНБО України щодо застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій), уведених у дію указами Президента України.

Рішення також рекомендує Національному банку України опрацювати питання щодо розроблення правового механізму блокування (припинення) на території України функціонування електронних платіжних систем суб'єктів господарювання держави-агресора та підготувати пропозиції щодо удосконалення з урахуванням актуальних кіберзагроз вимог до захисту інформації в інформаційно-телекомунікаційних системах банків та інших фінансових установ, системах дистанційного банківського обслуговування.

Висновки

Враховуючи виклики вітчизняного безпекового середовища та триваючу антитерористичну операцію на Сході України, яка певною мірою знаходить своє відображення і в кіберпросторі, виникає потреба у ґрунтовному дослідженні явища кібертероризму з метою розбудови комплексного механізму протидії, який перш за все має виконувати превентивну функцію.

Необхідно оптимізувати та систематизувати основні напрями діяльності правоохоронних органів із протидії використанню кіберпростору з терористичною метою, а також розширити застосування новітніх інформаційних технологій (у тому числі апаратно-програмних засобів моніторингу та аналізу ресурсів мережі Інтернет) в інтересах антитерористичної діяльності.

Крім того, потребує підвищення рівень кіберзахисту критичної інфраструктури держави, який на сьогодні залишається недостатнім, що продемонстрували вдалі кібератаки на об'єкти енергетичного комплексу України наприкінці 2015–2016 років [19].

Зазначене насамперед вимагає налагодження механізму державно-приватного партнерства у сфері кібербезпеки з власниками та операторами приватних об'єктів критичної інфраструктури України.

З метою організації протидії загрозам у кіберпросторі України варто розробити та впровадити дієву нормативно-правову базу, в якій були би чітко визначені поняття «кіберпростір», «кіберзагрози», «кібербезпека» та дана класифікація кіберзагроз. Створити загальнодержавну систему забезпечення кібербезпеки та законодавчо закріпити права і обов'язки її суб'єктів.

Одним із пріоритетів розбудови національної системи кібербезпеки є створення ефективного механізму координації та взаємодії між її суб'єктами.

Для вирішення цієї задачі доцільно створити при РНБО України Національний координаційний центр кібербезпеки [20].

1. Камчатний М.В. Нормативно-правове закріплення питань кібербезпеки у міжнародному праві. URL: http://dspace.nlu.edu.ua/bitstream/123456789/9826/1/Kamchatnuy.pdf

2. Гібсон Вільям. Нейромант (1984). URL: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%BB%D1%8C%D1%8F%D0%BC_%D0%93%D1%96%D0%B1%D1%81%D0%BE%D0%BD.

3. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і Безпека*. 2009. № 4. С. 215–219.

4. ISO/IEC 27032. Information technology — Security techniques — Guidelines for cybersecurity. 2012. 50 p.

5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118–129. URL: http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8.

6. Бурячок В.Л., Толубко Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник; за заг. ред. д-ра техн. наук, професора Б. Толубка. Київ: ДУТ, 2015. 288 с.

7. Schellong A.Breaking down the threat of cyber terrorism. URL: http://blogs.csc.com/2016/02/04/breaking-down-the-threat-of-cyber-terrorism

8. Указ Президента України від 15 березня 2016 року № 96/2016 «Про затвердження Стратегії кібербезпеки України». URL: http://zakon3.rada.gov.ua/laws/show/96/2016/conv#n11

9. Юрасов С. Полигон Украина Цифровая война на пороге. URL http://www.liga.net/projects/cyberattacs/

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

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

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

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

14. Национальная стратегия кибербезопасности (NCSS). От понимания к возможности. Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. URL: //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2 Engelseversie

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

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

17. Панченко В.М. Перспективи підготовки фахівців для сфери інформаційної безпеки у національній академії СБ України. Матеріали Міжнародної науково-практичної конференції «Інформаційний вимір гібридної війни: досвід України». НУО ім. Івана Черняховського. 2017. С. 60–62.

18. Указ Президента України від 13 лютого 2017 року № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». URL: http://www.rnbo.gov.ua/documents/437.html

19. *Корреспондент.net.* 5 січня 2016. Хакери атакували низку українських обленерго: URL: http://ua.korrespondent.net/ ukraine/3611402-khakery-atakuvaly-nyzku-ukrainskykh-oblenerho-zmi.

20. Ткачук Н.А. Кібербезпека у контексті актуальних змін до стратегічних документів у сфері національної безпеки і оборони. *Вісник Прокуратури*. 2016. № 3. С. 56–64.

Надійшла до редакції 15.05.2017