УДК 004.056.5:343.326 (045)

С.О. Гнатюк, к.т.н., доцент
академічний радник Інженерної академії України

БАЗОВІ ДЕФІНІЦІЇ У ГАЛУЗІ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Національний авіаційний університет, E-mail: s.gnatyuk@nau.edu.ua

Анотація. *Проблема кібертероризму носить глобальний характер і досить гостро постає у сучасному інформаційному суспільстві. Кібератаки за досить короткий проміжок часу перетворилися з поодиноких випадків на один з головних бізнес-ризиків для організацій у всьому світі. У глобальному контексті провідні держави світу все більшої уваги приділяють захисту критичних інформаційних ресурсів та можливості впливу на інформаційні ресурси інших держав. Проте існує низка проблем різного характеру, які необхідно вирішити державам як у національних сегментах, так і в усьому кіберпросторі. З огляду на це, у роботі наведено різні тлумачення таких понять як кіберпростір, кібератака та кібертероризм, а також запропоновано власне бачення кожного з понять.*

Ключові слова: *кіберпростір, кібербезпека, кібертероризм, кібератака, кіберзлочин, стратегія кібербезпеки, критична інформаційна інфраструктура держави.*

Аналіз сучасних досліджень та постановка проблеми. У наш час з'являються *нові форми тероризму,* такі як ядерний, біологічний, хімічний, екологічний, психологічний та кібернетичний тероризм (КбТ) [1]. Останній, з огляду на масову інформатизацію суспільства, несе одну з найбільших і найсерйозніших загроз людству. Протягом тривалого періоду часу благоустрій суспільства та економічна стабільність ґрунтувались на надійній роботі мереж передачі інформації та обчислювальних сервісів. Проте на функціонування ключових інформаційних та комунікаційних систем (ІКС) впливає багато негативних чинників і саме це робить однією з базових задач держави саме забезпечення кібернетичної безпеки як на державному, так і на міжнародному рівні. Дослідженню особливостей кібернетичного простору (КбП) та несанкціонованих дій у ньому, а також розробці методів протидії, присвятили свої роботи такі вітчизняні й закордонні науковці як В. Бесчастний, В. Бурячок, В. Бутузов, С. Гавриш, В. Голубєв, Д. Деннінг, О. Довгань, Д. Дубов, А. Коларік, О. Корченко, М. Литвинов, В. Мохор, Д. Номоконов, В. Панченко, Е. Рижков, Є. Скулиш, Т. Тропина, В. Шеломенцев, Д. Шиндер, В. Шурухнов та ін. Проте, з огляду на безперервну еволюцію потенційного інструментарію неавторизованих користувачів (порушників), аналіз останніх тенденцій у галузі кібернетичної безпеки держави є безперечно актуальним завданням. Проведений пошук вказав на відсутність ґрунтовних наукових досліджень, пов'язаних із багатокритеріальним аналізом понятійного апарату у галузі кібербезпеки. Зважаючи на це, першочерговим завданням, а одночасно й ***основною метою*** цього дослідження, є аналіз різних варіацій ключових дефініцій («кіберпростір», «кібератака» та «кібертероризм») у галузі кібернетичної безпеки держави, а також формування власного бачення кожного з понять.

Основна частина дослідження. Сучасні загрози кібернетичній безпеці характеризуються асиметричністю та гнучкістю, а кібератаки (КбА) уже давно перестали бути самоціллю – вони стали ефективним засобом для досягнення широкого спектру цілей, різноманітність яких обмежена лише уявою та фантазією порушників. Усі КбА можна диференціювати на три категорії – це КбА, що відповідно впливають на конфіденційність, цілісність чи доступність інформації, а всі інші види є похідними від них. Відповідно до міжнародного стандарту [2], ***КбП*** – це середовище існування, отримане у результаті взаємодії людей, програмного забезпечення і послуг в Інтернет за допомогою технологічних пристроїв і мереж, підключених до них, яке не існує у будь-якій фізичній формі. Серед інших, відповідно до наукових публікацій [3-6] та стратегій кібербезпеки провідних держав світу [7], варто відзначити такі визначення поняттю КбП:

— сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язану з ними фізичну інфраструктуру.

— віртуальний простір, в якому циркулюють електронні дані світових ПК.

— усі форми мережевої, цифрової активності, що включають у себе контент та дії, що здійснюються через цифрові мережі.

— уся інформаційна інфраструктура, що доступна через Інтернет поза будь-якими територіальними кордонами.

— поліморфний віртуальний простір, що генерує інформаційні системи як у формі складних світів, так і у простих реалізаціях (типу електронної пошти, глобальної навігації тощо);

— комунікаційне середовище, утворене системою зв'язків між об'єктами кіберінфраструктури – електронними обчислювальними машинами, комп'ютерними мережами, програмним забезпеченням та інформаційними ресурсами, що використовується для забезпечення певних інформаційних потреб;

— штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене у результаті функціонування кібернетичних комп'ютерних систем управління і обробки інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо);

— простір, сформований інформаційно-комунікаційними системами, у якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних;

— об'єкти інформаційної інфраструктури що керуються інформаційними (автоматизованими) системами управління та інформація, що в них циркулює;

— середовище, утворене організованою сукупністю інформаційних процесів на основі взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Проаналізуємо наведені визначення поняття КбП за такими базовими критеріями (табл. 1): 1) Віртуальність *(Virt);* 2) Врахування людського чинника *(HF);* 3) Врахування програмного забезпечення *(Soft);* 4) Наявність фізичної інфраструктури *(PhI);* 5) Мережева складова *(Net);* 6) Врахування Інтернет *(INet);* 7) Надання інформаційних послуг *(IServ);* 8) Врахування інформаційних ресурсів *(IRes);* 9) Наявність системи управління *(MSys);* 10) Врахування інформаційних процесів *(IPr)*.

Таблиця 1

Аналіз дефініцій поняття КбП за базовими критеріями

№	Дефініція	Базовий критерій									
		Virt	*HF*	*Soft*	*PhI*	*Net*	*INet*	*IServ*	*IRes*	*MSys*	*IPr*
1.	Стандарт ISO/IEC 27032	+	+	+	+	+	+	+	-	-	-
2.	Нормативна база США	-	-	-	+	+	-	-	+	-	+
3.	Офіційні документи ЄС	+	-	-	-	-	-	-	+	-	-
4.	Концепція кібербезпеки Великобританії	-	-	-	-	+	-	-	+	-	+
5.	Законодавство Німеччини	-	-	-	+	-	+	-	-	-	-
6.	В. Харченко, О. Корченко та ін.	+	-	-	-	-	-	-	-	-	+
7.	В. Бурячок	-	-	+	+	+	-	-	+	-	-
8.	М. Погорецький та В. Шеломенцев	-	-	-	+	+	-	+	+	+	+
9.	С. Мельник та О. Тихомиров	-	-	-	-	+	-	-	+	-	+
10.	Д. Дубов та М. Ожеван	-	-	-	-	-	-	-	+	+	-
11.	В. Шеломенцев	-	-	-	-	+	-	-	-	-	+

Провівши багатокритеріальний аналіз визначень поняття КбП (див. табл. 1), можна зробити висновок, що жодна з дефініцій не враховує повної множини параметрів. З огляду на це, доцільно було б запропонувати таке узагальнене визначення: *віртуальний простір, отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у т.ч. Інтернет) для підтримки та управління процесами перетворення інформації з метою забезпечення інформаційних потреб суспільства.*

З огляду на відмінність у трактуванні поняття КбП, яке є основоположним, відповідно і виникають складнощі у визначенні інших похідних термінів у цій галузі.

Термін **«КбТ»** є синтезом понять «КбП» та «тероризм» і до сьогодні у наукових колах ведуться активні дискусії щодо того чи є КбТ просто реалізацією актів тероризму у новому просторі (КбП), чи це принципово нове явище, яке має нові методи, засоби та інструментарій. У роботах [3-7] містяться такі визначення поняттю КбТ:

1) застосування методів тероризму (створення в соціальній сфері обстановки страху, неспокою, пригніченості з метою прямого або непрямого впливу на прийняття будь-яких рішень) у КбП (В. Харченко, О. Корченко та ін.);

2) принципово новий вид тероризму, який передбачає використання ресурсів інформаційних систем не лише як предмет злочинних посягань, а й середовище чи засіб скоєння злочину (О. Корченко та ін.);

3) навмисна, політично мотивована атака на інформацію, яка обробляється комп'ютерами, комп'ютерну систему і мережі, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту;

4) один із видів несанкціонованого доступу до ресурсів інформаційних систем з метою порушення їх базових характеристик інформаційної безпеки (обидва 3-4 В. Голубєв);

5) сплановані, політично мотивовані атаки на інформацію, комп’ютерні системи, комп’ютерні програми і дані, які призводять до насильства і здійснюються субнаціональними групами або таємними агентами (М. Політ, ФБР);

6) суспільно небезпечна діяльність, що здійснюється в КбП (або з використанням його технічних можливостей) із терористичною метою і полягає у свідомому, цілеспрямованому залякуванні населення та органів влади або вчиненні інших посягань на життя і здоров’я людей (О. Довгань та В. Хлань);

7) навмисна руйнівна діяльність, чи загроза такої, проти комп’ютерів та/чи комп’ютерних мереж, спрямована на заподіяння шкоди чи досягнення соціальних, релігійних, політичних чи інших подібних цілей, а також залякування будь-якої особи для досягнення цих цілей (К. Колмен);

8) злочинні дії, вчинені з використанням комп’ютерів та телекомунікаційних можливостей, які мають наслідком насильство, руйнування та/або припинення функціонування, спрямовані на залякування, шляхом створення невпевненості серед населення, з метою впливу на уряд або населення для досягнення певних політичних, соціальних або ідеологічних цілей (Національний центр захисту інфраструктури США);

9) незаконна атака чи загроза атаки проти комп’ютерів, мереж та інформації, що у них накопичується, вчинені щоб залякати або примусити уряд чи населення до певних політичних або соціальних дій, а також така атака неодмінно має призвести до насильства проти людей або власності, чи принаймні завдати шкоди, що призведе до побоювання (Д. Деннінг);

10) використання інструментів комп’ютерної мережі для припинення роботи критичних національних інфраструктур (наприклад, енергозабезпечення, транспорт, державне управління) або примусити чи залякати уряд та цивільне населення (Дж. Левіс, Центр стратегічних та міжнародних досліджень, США);

11) нова форма тероризму, яка для досягнення своїх терористичних цілей використовує комп’ютери й електронні мережі, сучасні інформаційні технології (Ю. Травніков);

12) використання інформаційних технологій терористичними групами чи особами для досягнення своїх цілей (Національна конференція державної законотворчості, США);

13) форма терористичного прояву, в якій електронно-обчислювальні машини (комп’ютери), системи та комп’ютерні мережі використовуються як засіб вчинення злочину (О. Климчик та Р. Кравченко);

14) різновид тероризму (поряд з ядерним, хімічним, космічним, сейсмічним, бактеріологічним, технологічним та ін.), який виник у процесі інформатизації суспільства і полягає у нанесенні збитків інформаційним системам за допомогою комп’ютерних атак (Д. Малишенко);

15) завдання шкоди інформаційним системам за умови використання, як засобу вчинення злочину, інформаційних систем чи інших електронних засобів (К. Керр);

16) різновид тероризму, в основу якого покладено спосіб здійснення терористичних дій, що виник у процесі розвитку інформаційно-телекомунікаційних технологій та впровадження їх у всі сфери сучасного суспільства (Є. Старостіна);

17) свідоме, цілеспрямоване застосування комп’ютерної інформації, комп’ютерів, комп’ютерних систем та мереж для захоплення комп’ютерних систем управління потенційно небезпечними об’єктами з метою: а) виведення цих об’єктів з ладу або їх руйнування, що прямо чи опосередковано створює або загрожує виникненням загрози надзвичайної ситуації внаслідок цих дій та становить небезпеку для персоналу, населення та довкілля; б) створення умов для аварій і катастроф техногенного характеру; в) залякування населення та органів влади погрозами вчинення вищезазначених протиправних дій; г) вчинення провокацій воєнного конфлікту та міжнародного

ускладнення; д) здійснення впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами; забезпечення організаційного чи іншого сприяння створенню або діяльності терористичної групи чи терористичної організації (С. Гавриш);

18) вчинення терористичними угрупованнями або окремими особами комп'ютерних атак на певні елементи інформаційної інфраструктури, спрямовані на проникнення у комп'ютерні системи, перехоплення управління комп'ютерною системою, порушення функціонування засобів комп'ютерного обміну в мережі, справляти інший деструктивний вплив, що може привести до тяжких наслідків і здійснення впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади шляхом залякування населення та органів державної влади погрозами вчинення вищезазначених протиправних дій (В. Бутузов);

19) суспільно-небезпечна діяльність, що полягає у свідомому, цілеспрямованому залякуванні населення та органів влади з метою досягнення злочинних цілей, і здійснюється з використанням інформаційно-телекомунікаційних систем (С. Мельник, О. Тихомиров);

20) дії щодо дезорганізації інформаційних систем, що створюють небезпеку загибелі людей, значної матеріальної шкоди чи інших суспільно небезпечних наслідків, за умови їх здійснення із спеціальною метою – порушити суспільну безпеку, залякати населення або здійснити вплив на прийняття рішень органами влади, а також з метою загрози (погрози) здійснення вказаних дій у тих же цілях (О. Федоров та ін.);

21) навмисна, політично вмотивована атака на об'єкти інформаційного простору (інформацію, що обробляється, комп'ютерну систему, мережу, а також на людину), що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної або суспільної безпеки, залякування населення, провокації військового конфлікту, чи загрозу вчинення таких дій (В. Пилипчук та О. Дзьобань);

22) свідоме зловживання цифровими інформаційними системами, мережами чи компонентами цих систем або мереж з цілями, що сприяють здійсненню терористичних операцій чи актів (М. Девост, Б. Хьютон та Н. Поллард);

23) здійснення протиправного впливу на інформаційні системи, вчинене з метою створення небезпеки заподіяння шкоди життю, здоров'ю або майну невизначеного кола осіб шляхом створення умов для аварій і катастроф техногенного характеру або реальної загрози такої небезпеки (Ю. Гаврилов та Л. Смирнов);

24) використання комп'ютерів як зброї або об'єкта атаки політично мотивованими міжнародними чи міжнаціональними групами, або таємними агентами, які загрожують насильством чи заподіюють його, насаджують страх для того, щоб впливати чи примусити уряд змінити політику (К. Вілсон);

25) безпосереднє вчинення терористичних дій за допомогою комп'ютерів і комп'ютерних мереж або використання КбП терористичними групами в організаційно-комунікаційних цілях і з метою шантажу, але не для безпосереднього здійснення терактів (Є. Роговський).

Для проведення аналізу зазначених визначень поняття КбТ пропонується обрати такі критерії (табл. 2): 1) розуміння під КбТ реалізацію терористичних актів у КбП, тобто компоненти КбП є фактично інструментом для здійснення терористичних дій *(Instrument);* 2) використання компонентів КбП як предмет злочинних посягань *(Subject);* 3) використання КбП у суміжних цілях *(AdjTarget).*

Провівши аналіз дефініцій поняття КбТ, можна провести певне диференціювання усієї множини визначень на три категорії, відповідно до кожного із зазначених критеріїв:

1) Віднесення до КбТ терористичних дій (обов'язкова присутність усіх ознак традиційного тероризму), реалізованих за допомогою сучасних інформаційних та комунікаційних технологій – це класичний випадок КбТ = «тероризм» + «КбП». З огляду на табл. 2, переважна кількість науковців, а саме В. Харченко, О. Корченко, О. Довгань, В. Хлань, Ю. Травніков, О. Климчик, Р. Кравченко, Є. Старостіна, М. Девост, Б. Хьютон та Н. Поллард вважають, що під КбТ необхідно вважати виключно використання компонентів КбП у якості засобів (середовища) для реалізації терористичних дій.

2) Кваліфікування як КбТ дій, пов'язаних із використанням елементів КбП як предмету злочинних посягань (реалізація різного роду КбА, спрямованих на нанесення шкоди конкретним об'єктам критичної інформаційної інфраструктури з певних характерних тероризму мотивів). Цієї думки притримуються такі вчені як В. Голубєв, М. Політ, Д. Деннінг, В. Пилипчук, О. Дзьобань, Ю. Гаврилов та Л. Смирнов.

3) Включення до КбТ використання КбП у цілях терористичних угруповань (у суміжних цілях)

але не у якості безпосереднього інструментарію здійснення терактів (використання ІКС для зв'язку із суспільством, інформаційно-психологічний вплив, створення пропагандистських сайтів, збирання необхідної для реалізації терактів інформації засобами Інтернет тощо). Така гіпотеза чітко прослідковується у роботах К. Колмена, С. Мельника, О. Тихомирова, О. Федорова та Є. Роговського.

Таблиця 2

Багатокритеріальний аналіз визначень поняття КбТ

№	Дефініція	Базовий критерій		
		Instrument	***Subject***	***AdjTarget***
1.	В. Харченко, О. Корченко та ін.	+	-	-
2.	О. Корченко та ін.	+	+	-
3-4.	В. Голубєв	-	+	-
5.	М. Політ	-	+	-
6.	О. Довгань та В. Хлань	+	-	-
7.	К. Колмен	-	+	+
8.	Націон. центр захисту інфраструктури США	+	-	-
9.	Д. Деннінг	-	+	-
10.	Дж. Левіс	+	+	-
11.	Ю. Травніков	+	-	-
12.	Націон. конф. держ. законотворчості, США	+	-	-
13.	О. Климчик та Р. Кравченко	+	-	-
14.	Д. Малишенко	+	+	-
15.	К. Керр	+	+	-
16.	Є. Старостіна	+	-	-
17.	С. Гавриш	+	+	-
18.	В. Бутузов	+	+	-
19.	С. Мельник та О. Тихомиров	-	-	+
20.	О. Федоров та ін.	-	+	+
21.	В. Пилипчук та О. Дзьобань	-	+	-
22.	М. Девост, Б. Хьютон та Н. Поллард	+	-	-
23.	Ю. Гаврилов та Л. Смирнов	-	+	-
24.	К. Вілсон	+	+	-
25.	Є. Роговський	+	-	+

Проте, ціла низка авторів під КбТ розуміють синтез дій, визначених зокрема у пп. 1-2 – це О. Корченко, Дж. Левіс, Д. Малишенко, К. Керр, С. Гавриш та К. Вілсон. Варто відмітити, що жодне із визначень не задовольняє одночасно усі вказані у табл. 2 критерії. З огляду на це, на базі проведеного аналізу, варто сформулювати таке ґрунтовне визначення поняття КбТ: *різновид*

тероризму, що полягає у свідомому та цілеспрямованому застосуванні ресурсів інформаційних систем для реалізації терористичних дій у КбП, а також для досягнення інших суміжних цілей в інтересах терористичних угруповань.

Крім того, очевидно, що КбТ нерозривно пов'язаний з іншим важливим у цій сфері поняттям – **КбА** (так як КбТ за своєю природою є сукупністю (комплексом) пов'язаних між собою КбА, навмисних, попередньо спланованих і реалізованих у КбП для досягнення певних цілей). З огляду на це, необхідно також формалізувати поняття КбА, яке не має стандартизованого визначення (поняття КбП, для порівняння, визначено в єдиному на сьогодні стандарті [2] у цій галузі). Серед найбільш вдалих дефініцій терміну КбА необхідно, перш за все, відзначити такі:

— *В. Харченко із співавторами* визначає КбА як заходи, що здійснюються для підриву безпеки систем чи реалізації загрози характеристикам безпеки ресурсам інформаційних систем шляхом використання їх уразливостей;

— *автори Д. Дубов та М. Ожеван* як КбА кваліфікують цілеспрямовані дії, що реалізуються в КбП (або за допомогою його технічних можливостей), та призводять (можуть призвести) до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, авторства, доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість та психічний стан громадян);

— *В. Шеломенцев* під КбА розуміє процес реалізації програмно-математичних заходів з метою пошуку та використання кібернетичних уразливостей інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем;

— *відповідно до роботи С. Мельника, О. Тихомирова та О. Лєнкова* КбА – це використання технічних недоліків механізмів безпеки сучасного КбП з метою дезорганізації роботи його елементів;

— *В. Бурячок у своїй монографії [4]* наводить таку дефініцію поняття КбА: сукупність узгоджених за метою, змістом і часом дій або заходів – так званих кібератакцій, спрямованих на певний об'єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережності та/або авторства циркулюючої в ньому інформації, а також порушення роботи його ІТ систем та мереж.

Узагальнюючи опрацьований матеріал, можна сформулювати таке визначення поняттю КбА: *реалізація у КбП загроз безпеці його компонентів (а саме загроз порушення конфіденційності, цілісності та доступності) з урахуванням їх уразливостей.*

Висновки

Таким чином, у цій роботі проведено багатокритеріальний аналіз ключових дефініцій у галузі кібербезпеки, а саме КбП, КбТ та КбА, що містяться у міжнародних стандартах, нормативних документах провідних держав світу, а також у вітчизняних та закордонних наукових публікаціях. У результаті проведеного аналізу за різними параметрами було сформульовано узагальнені визначення зазначених понять. У подальших дослідженнях необхідно провести аналіз інших важливих понять у цій галузі (наприклад, кібербезпека, кіберзахист, кіберзброя, кібервійна тощо), а також дослідити критичну інформаційну інфраструктуру держави з точки зору можливих загроз та уразливостей.

Список літературних джерел:

1. *Корченко О.Г.* Кібернетична безпека держави: характерні ознаки та проблемні аспекти // *О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк* / Безпека інформації. — Том 19, №1. — 2013. — С. 40-45.

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

3. *Гнатюк С.О.* Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи // *С.О. Гнатюк* / Безпека інформації. — Том 19, №2. — 2013. — С. 118-129.

4. *Бурячок В.Л.* Основи формування державної системи кібернетичної безпеки: Монографія. — К. : НАУ. — 2013. — 432 с.

5. *Дубов Д.В.* Кібербезпека: світові тенденції та виклики для України / *Д.В. Дубов, М.А. Ожеван.* — К. : НІСД, 2011. — 30 с.

6. *Словник* термінів з кібербезпеки / За загальною редакцією *Копана О.В., Скулиша Є.Д.* — К. : ВБ «Аванпост-Прим». — 2012. — 214 с.

7. *Государственные* стратегии кибербезопасности [Електронний ресурс]. — Режим доступу: http://ibst.pnzgu.ru/index.php/news/novosti-v-mire-it-i-ib/129-gosudarstvennye-strategii-kiberbezopasnosti