КІБЕРТЕРОРИЗМ: ІСТОРІЯ РОЗВИТКУ, СУЧАСНІ ТЕНДЕНЦІЇ ТА КОНТРЗАХОДИ

Сергій Гнатюк

Національний авіаційний університет, Україна

ГНАТЮК Сергій Олександрович, к.т.н.

Рік та місце народження: 1985 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, квантова криптографія, кібербезпека цивільної авіації, реагування на інциденти інформаційної безпеки.
Публікації: більш ніж 120 наукових публікацій, серед яких монографії, наукові статті у міжнародних та вітчизняних фахових журналах, патенти та авторські свідоцтва на програмні продукти.
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, наведено різні тлумачення таких понять як кіберпростір, кібератака та кібертероризм, запропоновано власне бачення кожного з понять. Висвітлено узагальнену хронологію розвитку кібертероризму та еволюції кібератак з моменту зародження обчислювальної техніки до сьогоднішнього часу. Також, наведено заходи світової спільноти у відповідь на акти кібертероризму та з метою попередження інших нелегітимних дій у кіберпросторі. Проведено аналіз прийнятих провідними державами світу стратегій кібербезпеки і наведено їх коротку характеристику. Крім того, ґрунтуючись на світовому досвіді і національних особливостях, сформульовано рекомендації щодо забезпечення кібербезпеки України.*

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

Вступ. Історія сучасного тероризму сягає своїм корінням далеко в глибину століть, проте питання, пов'язані з чітким поняттям тероризму та його різновидами донині викликають дискусії в наукових колах і поки не знайшли остаточної відповіді. Можна переконливо говорити лише про те, що безглуздо боротися з тероризмом, не маючи навіть найменшого уявлення про нього, умови і причини його виникнення, види і сучасні прояви. Сучасний міжнародний тероризм характеризується: широким розмахом і відсутністю чітких державних кордонів; зв'язками і взаємодією з міжнародними терористичними центрами та організаціями; чіткою організаційною структурою (інтегруючою керівну і оперативну діяльність, розвідку і контррозвідку, матеріально-технічне забезпечення, бойові групи, прикриття і т.д.); жорсткою конспірацією і ретельним відбором кадрів; агентурною мережею, яка, як правило, охоплює правоохоронні та державні органи; відмінним технічним оснащенням; наявністю розгалуженої мережі конспіративних укриттів, навчальних баз і полігонів [1].

Постановка задачі. У наш час з'являються *нові форми тероризму*, такі як ядерний, біологічний, хімічний, екологічний, психологічний та комп'ютерний (кібернетичний) тероризм (КбТ) [2]. 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 [1-3] 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 (кіберпростору, КбП) та КбТ, 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 неавторизованої сторони, аналіз останніх тенденцій

розвитку КбТ з метою визначення ефективних контрзаходів є безперечно актуальним завданням. **Метою** цієї роботи є дослідження хронології кібертероризму, сучасних тенденцій цього явища, а також формулювання відповідних контрзаходів (орієнтованих на нашу державу). Мета дослідження визначає перелік **завдань,** які необхідно виконати: 1) дослідити різні варіації ключових у цій галузі дефініцій, таких як КбП, КбТ та КбА, а також запропонувати власне бачення кожного поняття; 2) провести аналіз розвитку КбТ та еволюцію КбА з моменту зародження обчислювальної техніки до сьогодні; 3) дослідити превентивні та контрзаходи європейських і світових держав на масові КбА та акти КбТ (прийняття концепцій кібербезпеки, створення загонів кібервійськ тощо); 4) на основі проведених досліджень розробити систему контрзаходів для мінімізації впливу КбТ зокрема на державні інформаційні ресурси України.

Основні результати дослідження. Сучасні загрози інформаційній безпеці (кібербезпеці [3]) характеризуються асиметричністю та гнучкістю, а КбА уже давно перестали бути самоціллю – вони стали ефективним засобом для досягнення широкого спектру цілей, різноманітність яких обмежене лише уявою та фантазією неавторизованої сторони. 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.

Аналіз поняття КбП. Відповідно до міжнародного стандарту [3], ***кіберпростір*** – 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. Нормативна база США ґрунтується дещо на іншому визначенні [4] – це 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. Офіційні документи Євросоюзу [5] використовують таке визначення поняттю КбП – це віртуальний простір, в якому циркулюють електронні дані світових ПК. Кібербезпека Великобританії базується на такому визначенні цього поняття – це всі форми мережевої, цифрової активності, що включають у себе контент та дії, що здійснюються через цифрові мережі [6]. Німеччина під КбП розуміє всю інформаційну інфраструктуру, що доступна через Інтернет поза будь-якими територіальними кордонами [7]. Серед інших варто відзначити такі визначення поняття КбП:

– поліморфний віртуальний простір, що генерує інформаційні системи як у формі складних світів, так і у простих реалізаціях (типу електронної пошти, глобальної навігації тощо) [1];

– 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 [8];

– 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) [9];

– простір, сформований інформаційно-комунікаційними системами, у якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних [10];

– об'єкти інформаційної інфраструктури що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює [11];

– середовище, утворене організованою сукупністю інформаційних процесів на основі взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [12].

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 [3]	+	+	+	+	+	+	+	-	-	-
2.	Нормативна база США [4]	-	-	-	+	+	-	-	+	-	+
3.	Офіційні документи ЄС [5]	+	-	-	-	-	-	-	+	-	-
4.	Концепція кібербезпеки Великобританії [6]	-	-	-	-	+	-	-	+	-	+
5.	Законодавство Німеччини [7]	-	-	-	+	-	+	-	-	-	-
6.	В. Харченко, О. Корченко та ін. [1]	+	-	-	-	-	-	-	-	-	+
7.	В. Бурячок [8]	-	-	+	+	+	-	-	+	-	-
8.	М. Погорецький та В. Шеломенцев [9]	-	-	-	+	+	-	+	+	+	+
9.	С. Мельник та О. Тихомиров [10]	-	-	-	-	+	-	-	+	-	+
10.	Д. Дубов та М. Ожеван [11]	-	-	-	-	-	-	-	+	+	-
11.	В. Шеломенцев [12]	-	-	-	-	+	-	-	-	-	+

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 *(Phl);* 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).*

Провівши багатокритеріальний аналіз визначень поняття КбП (див. табл. 1), можна зробити висновок, що найбільш ґрунтовними та всеохоплюючими є визначення, зазначені у джерелах [3, 9], проте вони не враховують 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 (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства.*

З огляду на відмінність у трактуванні поняття КбП, яке є основоположним (центральним), відповідно і виникають складнощі у визначенні похідних термінів, таких як «КбА», «КбТ», «кіберзагроза», «кібербезпека», «кіберзахист», «кіберінфраструктура», «кіберзброя», «кіберзлочин», «кібервійна» тощо.

Кібертероризм. 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 джерелах [1, 2, 13-31] 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)** спланованої, 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);

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. державної 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	+	-	+

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 (див. табл. 2), 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, М. Девост, Р. Кравченко, Є. Старостіна, 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 [10, 19, 26, 31].

Проте, ціла низка авторів у своїх роботах [2, 14, 19, 22, 29] 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.*

Кібератаки. 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 атак (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 [3] у цій галузі). Серед найбільш вдалих дефініцій терміну КбА необхідно, перш за все, відзначити такі: В. Харченко із співавторами у роботі [1] 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) [11]; В. Шеломенцев під КбА розуміє процес реалізації програмно-математичних заходів з метою пошуку та використання кібернетичних уразливостей інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [12]; відповідно до роботи С. Мельника, О. Тихомирова та О. Лєнкова [32] КбА – це використання технічних недоліків механізмів безпеки сучасного КбП з метою дезорганізації роботи його елементів; В. Бурячок у своїй монографії [8] наводить таку дефініцію поняття КбА: сукупність узгоджених за метою, змістом і часом дій або заходів – так званих кібератакій, 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.*

Історія розвитку КбТ в контексті еволюції обчислювальної техніки [8, 26, 32-37]:

– 1960 рр. – поява перших транзисторних обчислювальних систем та, як наслідок, виникнення перших примітивних кіберзлочинів, що полягали здебільшого у фізичному пошкодженні комп'ютерних систем і даних, що на них зберігались;

– 1970 – початок 1980-х рр. – перехід від фізичних пошкоджень обчислювальних систем до протиправного використання комп'ютерних систем та маніпулювання з електронними даними;

– 1976 р. – заснування компанії Apple Computer Inc., початок ери персональних комп'ютерів;

− 1981 р. – компанія Microsoft Corp. Випустила першу операційну систему;

− 1982 р. – співробітниками компанії Xerox Дж. Шоком та І. Хуппом вперше введено термін «черв'як»;

− 1983 р. – перший арешт «віртуальних злочинців» – групу хакерів під назвою «банда 414» (Мілуокі, США), яка зламала 60 комп'ютерів (деякі з них належали Лос-Аламоській національній лабораторії);

− 1984 р. – Європейська організація ядерних досліджень починає використовувати Інтернет-протокол для об'єднання своїх внутрішніх комп'ютерів;

− 1986 р. – перше вдале розслідування КбА, що була здійснена співробітниками КДБ на інформаційні ресурси Стратегічної оборонної ініціативи США;

− 1987 р. – зареєстровано перше сімейство комп'ютерних вірусів «Єрусалим»;

− 1988 р. – створено перший мульти-платформний черв'як, здатний переміщатися мережею Інтернет; епідемія внаслідок дії «черв'яка Морріса», пошкоджено 4 тис. Інтернет серверів, загальна шкода – більш ніж $ 98 млн.;

− 1989 р. – Інтернет налічує 100 тис. користувачів по усьому світу; хакерська група «The Legion of Doom» отримала контроль над телефонною мережею BellSouth, включаючи можливість прослуховування телефонних розмов, маршрутизацію викликів та маскування під технічний персонал станції; поява першого антивірусного програмного забезпечення (McAfee);

− 1990 р. – перший в історії суд над автором комп'ютерного вірусу – суд приговорив студента Корнельського університету Р. Морріса до 3 років позбавлення волі умовно та штрафу в $ 10 тис.;

− 1991 р. – офіційна поява «всесвітньої павутини» (WWW);

− 1992 р. – створено перше поліморфне сімейство вірусів (Mutation Engine);

− 1993 р. – у Лондоні низка брокерських контор, банків і крупних фірм отримали вимогу щодо виплати £ 10-12 млн. відступних зловмисникам;

− 1994 р. – організація «Фронт звільнення Інтернет», об'явивши кібервійну компаніям National Broadcasting Corporation та General Electric, за допомогою КбА вивів з ладу їх внутрішні мережі;

− 1995 р. – група хакерів «Strano Network» реалізує потужну КбА на комп'ютери уряду Франції – це перша атака типу «відмова в обслуговуванні» (DoS-атака);

− 1996 р. – представники терористичної організації «Тигри звільнення Таміл-Ілама» провели мережеву КбА проти дипломатичних представництв Шрі-Ланки; компанія NOKIA випустила перший мобільний телефон з можливістю підключення до Інтернет;

− 1997 р. – у результаті дій невстановленого хакера було перервано передачу медичних даних між наземною станцією НАСА і космічним кораблем «Атлантіс»; підліток вивів із ладу основний комп'ютер телефонної компанії, що обслуговувала аеропорт у м. Ворсестер, внаслідок чого диспетчерська вишка не змогла виконувати свої функції протягом 6 годин; ФБР США провело розслідування 200 випадків кіберзлочинів;

− 1998 р. – 12-річний хакер проникнув у комп'ютерну систему, що контролює паводкові шлюзи греблі Т. Рузвельта в Арізоні – під загрозою затоплення два міста з населенням 1 млн. чоловік; створено перший Java вірус Strange Brew; корпорація Google об'явила про створення першої пошукової системи; потужна КбА на індійський Центр ядерних досліджень ім. Баба – пряма загроза виведення з ладу системи управління реактором;

− 1999 р. – поява в Інтернет вірусу під назвою «Хеппі-99»; широкомасштабна компанія КбА Китаю та Тайваню один проти одного (постраждали портали державних установ, фінансових компаній, університетів тощо); на урядові електронні адреси більш ніж 20 держав світу надійшли листи від імені російських офіцерів-ракетників із погрозою самовільного запуску ракет на столиці і промислові центри західних держав; хакери захопили керування військовим телекомунікаційним супутником серії Skynet і змінили його орбіту; за рік ФБР розслідувало 800 кіберзлочинів;

− 2000 р. – із пригороду Маніли в Інтернет запущено вірус «I love you» (інша назва «Love Bug»), що дуже швидко поширився по усьому світу і заразив більше 45 млн. комп'ютерних мереж (у т.ч. мережі Білого дому, ЦРУ, Міністерства оборони і Конгресу США, Британського Парламенту тощо); масштабна DoS-атака, що зробила недоступними протягом 2-3 годин сервери великих компаній Yahoo, eBay, CNN та ZDNet; КбА від імені чеченських націоналістів на сервер «Росбізнесконсалтинг» з метою «антипутінської» пропаганди; група пакистанських хакерів «Мусульманський он-лайн синдикат» атакувала більш ніж 500 індійських Інтернет-сайтів у знак протесту проти військових дій у Кашмірі;

− 2001 р. – шотландський хакер Г. Маккінон зламав десятки комп'ютерів оборонних відомств, що стало «найбільшою КбА на військові комп'ютери в історії»; 15-річний канадський хакер Mafia Boy успішно реалізував DoS-атаку на декілька великих мережевих компаній – нанесена шкода оцінюється більш ніж у $ 1 млрд.;

− 2002 р. – у першу добу року зареєстровано 79 потужних КбА; поява вірусу, здатного заражати Macromedia Flash-файли (Actn/LFM.A);

− 2003 р. – поява черв'яка Blaster, що використовує вразливості Windows; реєстрація першого коду, що використовує вразливості Microsoft SQL-Server (Win32/SQLSlammer);

− 2004 р. – масована КбА на електронні ресурси уряду Південної Кореї; зафіксовано 75 тисяч спроб злому серверів Пентагону; реєстрація першого черв'яка для мобільних засобів (SymbOS/Cabir); виявлено перший web-черв'як, що використовує Google; поява першого ICQ-червяка Bizex (Exploit), метою якого була крадіжка банківської інформації, атрибутів доступу тощо;

− 2005-2006 рр. – зафіксовано більш ніж 2 млн.

КбА на інформаційні ресурси органів державної влади по всьому світу; реєстрація Троянського коня, що маскується під відеокодек (Win32/Trojan Downloader); поява черв'яка Lion, що вражає сервери Linux;

− 2007 р. – Інтернет налічує 1 млрд. користувачів; масована КбА на весь Рунет; потужна КбА на сайти державних структур Естонії; виявлена botnet Storm, залучена до розсилання спаму (Win32/Nuwar);

− 2008 р. – потужна КбА на ІКС Грузії, що призвела до ізоляції грузинського уряду і народу від зовнішнього світу; мільйони робочих станцій на базі Windows по усьому світу стали жертвами черв'яка Win32/Conficker;

− 2009 р. – китайська шпіонська кібероперація «Ghostnet» з проникненням у комп'ютерні мережі більш ніж 100 країн світу; зареєстрований botnet Zeus із числом машин у мережі більш ніж 1 900 000 і центром керування в Україні;

− 2010 р. – КбА перед самітом «Великої двадцятки» у Парижі (Франція); перша міжконтинентальна КбА Stuxnet в Ірані, внаслідок якої була уражена автоматизовані системи управління атомною інфраструктурою країни; потужна DoS-атака на інформаційну інфраструктуру М'янми напередодні виборів; на сторінках сайту Wikileaks опубліковано величезну кількість грифованих документів щодо воєн США в Афганістані та Іраку, а також понад 250 тис. документів переписки американських дипломатів; у результаті КбА виведено з ладу сайти найбільших міжнародних платіжних систем Visa, MasterCard та PayPal; група хакерів реалізувала DDoS-атаку на «Аерофлот», у результаті чого на протязі тижня була заблокована послуга купівлі електронних квитків;

− 2011 р. – безпрецедентний витік даних у результаті КбА на сервери Пентагону; КбА на сервери Sony та «Банку Америки» з подальшою публікацією конфіденційної інформації в Інтернет; широкомасштабна КбА перед самітом Євросоюзу в Брюсселі (Бельгія);

− 2012 р. – хакерська група Anonymous реалізувала КбА на сайти державних установ Ізраїлю – у результаті постраждали сайти «Моссаду», армії та спецслужб; у Швеції реалізовано потужну КбА на Міністерство оборони, «Сведбанк» та Управління залізничних доріг; американські кіберексперти провели успішну КбА на пропагандистський сайт «Аль-Каїди» у Ємені; проведено потужні вірусні КбА на електроенергетичні компанії США; зареєстровано Троянські програми Win32.Duqu та Win32.Flame, що поширюються в Інтернет через знімні носії інформації і слугують для систематичного збору та модифікації конфіденційної інформації; КбА на сайти державних установ України (варто відзначити такі несанкціоновані дії: хакери відкрили доступ до сервера МВС України через ftp, у результаті чого інформація з обмеженим доступом стала загальнодоступною в мережі Інтернет; «противники закриття» популярного вітчизняного файлобмінника Ex.ua реалізували системні «розподілені DoS-атаки» (DDoS) на сайти Президента, Кабінету міністрів України, Партії регіонів (1 лютого 2012 року) – це вплинуло на їх нормальне безперервне функціонування; реалізація DDoS-атак на сайти політичних партій, зокрема «Батьківщина» та «Партія регіонів», а також на персональні сайти деяких політичних лідерів у день Парламентських виборів);

− 2013 р. – невідомі хакери отримали доступ і опублікували персональні дані 40 тис. солдатів армії США та більше 2 млн. партійних функціонерів керуючої партії Республіки Корея; активісти хакерського угруповання WikiCrew за допомогою DDoS-атаки вивели з ладу офіційний сайт Агентства національної безпеки США; хакерська група Syrian Electronic Army провела КбА на інформаційну інфраструктуру системи водопостачання ізраїльського м. Хайфа; одна з найбільш масштабних КбА на сервери Інтернет у результаті конфлікту інтересів активістів груп Spamhaus (спеціалізується на боротьбі зі спамом) та Cyberbunker (допомагає користувачам розміщати контент у мережі).

Еволюція КбТ показує, що КбА сьогодення мають яскраво виражене політичне забарвлення і все більше проявляються у кібернетичному впливі на міждержавному рівні. Досліджуючи паралельно розвиток ІКС та технологій, можна відмітити, що основними причинами виникнення КбТ є, перш за все, різке *збільшення продуктивності* та одночасне *здешевлення* сучасних обчислювальних засобів, що робить їх загальнодоступними і значно розширює множину потенційних кіберзагроз, а також *відсутність чітких кордонів* у КбП, що нівелює відмінність між зовнішніми та внутрішніми джерелами загроз кібербезпеці держави. Крім того, КбП дає можливість зловмисникам маніпулювати інформацією і її сприйняттям суспільством на власний розсуд, а також дозволяє реалізувати терористичні дії з безпрецедентною оперативністю і зробити завдання ідентифікації зловмисників дуже складним. Аналізуючи сучасні тенденції розвитку КбТ, варто також відзначити, що за даними «Лабораторії Касперського» [38] на початок 2013 року *найнебезпечнішими кіберзагрозами* у світі (топ-5) є *спеціально створена кіберзброя* (програмні та апаратні засоби, що все частіше націлені на об'єкти критичної інфраструктури, які часто використовують схожі системи захисту), *маніпуляції у соціальних мережах* (наприклад, за допомогою соціальних мереж можуть організовуватись різного роду протести, мітинги та демонстрації – тобто організатори таких заходів можуть, знаходячись у іншому місці, ефективно маніпулювати масами), *онлайн-покоління* (нове покоління, яке фактично живе у віртуальному світі і, як наслідок, дуже вразливе до кіберзагроз), *втрата приватності* (сучасні інформаційні системи, форуми, портали і т.д. заставили людство відмовитись від приватного життя і підсвідомо зробити його публічно доступним, а крім того ще є маса камер відео нагляду, безпілотні літаючі апарати, Google Street View тощо) та *зламування мобільних пристроїв* (більшість людей щодня користуються різними засобами комунікації: мобільними телефонами, смартфонами, нетбуками

тощо, які є популярними об'єктами посягань з боку кіберзлочинців та кібертерористів [16]).

Заходи, спрямовані на протидію КбТ. Головною зброєю у боротьбі з КбТ залишається законодавство, яке потребує подальшого вдосконалення. Якщо говорити про міжнародні нормативні та правові акти у цій галузі, то першим і головним документом, у якому мова йде про боротьбу з кіберзлочинністю, є *Міжнародна конвенція про кіберзлочинність* (прийнято Радою Європи 23 листопада 2001 р., ратифіковано Верховною Радою України 7 вересня 2005 р.). Цей документ є своєрідною реакцією на терористичні акти 11 вересня у США, його націлено на здійснення загальної політики з питань кримінального права, метою якої є захист суспільства від КбТ шляхом прийняття потрібних законодавчих актів, а також шляхом розширення міжнародного співробітництва. У цій Конвенції згадуються такі типи комп'ютерних злочинів: незаконний доступ; незаконне перехоплення; втручання в дані; втручання в систему, а засобами КбТ є комп'ютерна система, комп'ютерні дані, послуги інформаційно-комунікаційних технологій та дані трафіку.

Також, серед *превентивних та контрзаходів світової спільноти,* варто виділити:

− 2003 р. – опублікування у США *Національної стратегії безпеки у кіберпросторі* (є частиною більш загальної Стратегії забезпечення національної безпеки, створеної як реагування на події 11 вересня 2001 р.) [39];

− 2005 р. – Німеччина приймає *Державний план захисту інформаційної інфраструктури* [40];

− 2006 р. – Швеція розробила *Стратегію підсилення безпеки Інтернет;* США проводить перші глобальні навчання з питань кібербезпеки *Cyber Storm I,* що вказали на велику вразливість держави до сторонніх кібернетичних впливів;

− 2008 р. – Естонія опублікувала *розширену державну стратегію кібербезпеки* (реакція на потужні КбА 2007 р., одна з перших у Європі розширених стратегій, центральним об'єктом є безпека інформаційних систем, а контрзаходи базуються на правовому регулюванні, навчанні та співпраці) [41]; прийняття стратегій кібербезпеки у Фінляндії (інтерпретація кібербезпеки як проблеми економічного характеру, тісно пов'язаної з розвитком інформаційного суспільства) [42] та Словаччині (забезпечення кібербезпеки розглядається у якості необхідної умови нормального функціонування та розвитку суспільства, а сама стратегія спрямована на попередження кіберзагроз та забезпечення готовності засобів протидії); США проводить навчання *Cyber Storm II,* результати яких виявились не набагато кращими за попередні навчання (Cyber Storm I) [8];

− 2009 р. – введення в США посади *Національного радника з питань кібербезпеки;*

− 2010 р. – опубліковано стратегії кібербезпеки Канади (стратегія базується на «трьох китах» - це захист урядових систем, забезпечення безпеки канадських громадян в онлайн-середовищі, співпраця з метою захисту ключових кібернетичних систем) [43] та Японії (створення спеціального органу, що займається попередженням та протидією КбА, введення гнучких політик, направлених на боротьбу з можливими масовими КбА) [44]; проведено першу навчальну симуляцію кібервійни під назвою «Шокова кіберхвиля», що показала уразливості КбП США [8]; США проводить триденні навчання *Cyber Storm III,* що були присвячені випробуванням нової системи протидії КбА із залученням провідних фахівців з Австрії, Великобританії, Японії, Німеччини, Нідерландів, Швеції, Франції та інших держав [8]; проведено перші кібернавчання державами Європейського союзу під назвою *Cyber Europe-2010* – перший крок у розробці стратегії комплексної безпеки на території об'єднаної Європи [8];

− 2011 р. – прийняття стратегій кібербезпеки у Великобританії (основною метою є забезпечення лідируючих позицій у галузі інформаційно-телекомунікаційних технологій, виключення ризиків у КбП, який має стати повністю безпечним для громадян та економіки держави) [6], Чехії (забезпечення вільного доступу до інформаційних сервісів, цілісності та конфіденційності даних у КбП) [45], Франції (орієнтація на протидію загрозам конфіденційності, цілісності та доступності інформаційних ресурсів у КбП, боротьбу з кіберзлочинністю та забезпечення кіберзахисту, основний інструмент – технічні засоби захисту інформації) [46], Німеччині (основним об'єктом захисту є критичні інформаційні системи, велика увага приділяється попередженню КбА та впливу на інформаційні системи випадкових чинників) [47], Литві (особлива увага приділяється захисту від КбА персональних даних, телекомунікаційних мереж, інформаційних систем та критично важливих інфраструктур, формалізовано відповідні контрзаходи) [48], Люксембурзі (стратегія містить п'ять базових напрямів – це захист критичної інформаційної інфраструктури та своєчасне реагування на інциденти безпеки, удосконалення нормативно-правової бази, внутрішньодержавна та міжнародна співпраця, навчання та інформування, просування стандартів) [49] та Нідерландах (з одного боку декларується відкритість КбП, а з іншого – необхідність забезпечення кібербезпеки ІКС, під якою розуміється захист від збоїв та невірної експлуатації ІКС) [50]; опублікування в США *Міжнародної стратегії для кіберпростору* (базується на моделі співпраці між урядом, міжнародними партнерами та приватним сектором, основні задачі: захист національних мереж, модернізація законодавства, підготовка військової галузі до нових загроз, забезпечення приватності й недоторканості особистого життя в Інтернет) [51]; заснування у Великобританії *Міжнародного альянсу забезпечення кібербезпеки;* початок програми американського кіберкомандування «Кібервиклик для США», метою якої є залучення до співпраці ІТ-фахівців для забезпечення безпеки критично важливих об'єктів військової, державної та комерційної інфраструктури держави; створення в Україні

Управління по боротьбі з кіберзлочинністю МВС України – окремого оперативного підрозділу, що спеціалізується виключно на протидії кіберзлочинності;

− 2012 р. – під егідою Єврокомісії проведено чергові кібернавчання типу «стрес-тест» під назвою *Cyber Europe-2012*, де використовувались віртуальні стендові системи, що відтворюють реальні характеристики критичних інформаційних інфраструктур Євросоюзу [8]; створення в Україні та апробація першого навчального курсу під егідою ІКАО, присвяченого захисту цивільної авіації від кіберзагроз [52]; прийняття першого стандарту [3] по кібербезпеці (стандарт спрямований на ліквідацію недоліків, які виникають внаслідок відсутності взаємодії між поставщиками та користувачами Інтернет-послуг, а також на боротьбу із загрозами сучасних Інтернет і мереж та забезпечення безпеки ІКС);

− 2009-2012 рр. – створення загонів кібервійськ у КНР, США, Росії, Індії, Великобританії, Німеччині, Австралії (початок створення аналогічних вітчизняних загонів) [11], організація агентств кібернетичної оборони у Австрії (APCIP), Великобританії (CPNI), Німеччині (NCAZ), Швейцарії (MELANI) та Нідерландах (NICC) а також включення вимог щодо забезпечення захисту від кіберзагроз у ключові нормативні документи критично важливих галузей народного господарства, таких як, наприклад, галузь енергетики, транспорту (зокрема цивільної авіації [53, 54]) та ін.;

− 2013 р. – відкрито Європейський центр по боротьбі з кіберзлочинністю (EC3), який став координаційним центром ЄС у боротьбі із кіберзлочинністю; Президент США Б. Обама підписав указ щодо підвищення кібербезпеки США (велика увага приділяється розмежуванню функцій органів, що відповідають за кібербезпеку держави, обміну інформацією щодо кіберінцидентів, а також структуруванню та аналізу отриманої інформації); Прийняття покращеної стратегії кібербезпеки Японії (основна ідея – створення кібербезпечної нації із захищеним і провідним у світі, за різними критеріями, КбП) [55]; Європарламент прийняв директиву, направлену на боротьбу з кіберзлочинністю (основною тезою є посилення покарань кіберзлочинців); координатор спецслужб США Дж. Клаппер включив КбА у перелік головних загроз США.

Враховуючи історію розвитку КбТ та досвід боротьби з цим явищем найбільш розвинених світових держав, можна сформулювати рекомендації щодо заходів, які необхідно реалізувати Україні для мінімізації впливу загроз у КбП на нормальне функціонування і сталий розвиток держави в усіх галузях народного господарства.

Рекомендовані контрзаходи. З огляду на сучасні тенденції у боротьбі найрозвинутіших держав світу з КбТ, а саме прийняття стратегій кібербезпеки, проведення кібернавчань, створення загонів кібервійськ тощо, а також враховуючи національні особливості, нашій державі, перш за все, необхідно: ***1)*** *Розробити єдиний понятійний апарат у галузі кібербезпеки,* який має ґрунтуватися на стандартах та кращих світових практиках, а також бути гармонізованим з відповідними європейськими та світовими аналогами. ***2)*** *Удосконалити вітчизняне законодавство* у цій галузі: прийняти концепцію кібербезпеки, закон про боротьбу із кіберзлочинністю (на сьогодні існує лише законопроект, який вже протягом довгого часу «блукає» законодавчими інстанціями), внести відповідні (до пп. 1-2) зміни до чинних законів «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», «Про захист персональних даних» та ін. ***3)*** *Розробити і затвердити цільову науково-технічну програму,* стимулювати і підтримувати фундаментальні та прикладні наукові дослідження у галузі створення сучасних технологій виявлення та запобігання несанкціонованим впливам на кібернетичні (інформаційні) системи, віднести питання, пов'язані із розробкою методів та засобів забезпечення безпеки у КбП до пріоритетних напрямів розвитку науки і техніки України. ***4)*** *Створити спеціалізовані підрозділи щодо боротьби з кіберзлочинністю та КбТ* із ефективною системою координації їх взаємодії. Чітко та прозоро розподіляти обов'язки спеціальних державних інституцій щодо захисту КбП держави (на сьогодні у системі забезпечення кібербезпеки держави задіяні такі органи: СБУ, ДССЗЗІ, МВС, МО, СЗР та ін.). ***5)*** *Удосконалити багаторівневу систему підготовки кадрів у галузі кібербезпеки*. Сьогодні в Україні система підготовки кадрів у галузі інформаційної безпеки є досить розвиненою, чіткою і структурованою (для порівняння у Росії немає окремої галузі знань). Галузь знань 1701 «Інформаційна безпека» містить три напрямки 6.170101 «Безпека інформаційних і комунікаційних систем», 6.170102 «Системи технічного захисту інформації» та 6.170103 «Управління інформаційною безпекою», після чого випускники можуть отримати освітньо-кваліфікаційний рівень «Магістр» за однією з відповідних освітньо-професійних програм. Крім того, є можливість продовжити навчання в аспірантурі та докторантурі за спеціальностями 05.13.21 – «Системи захисту інформації» та 21.05.01 – «Інформаційна безпека держави». Проте, безперечно, є необхідність удосконалення навчальних планів та програм відповідно до тенденцій розвитку КбП, узгодження з відповідними програмами провідних країн світу тощо. ***6)*** *Мінімізувати відсоток застосування програмних та апаратних засобів іноземного виробництва,* стимулювати розвиток відповідного вітчизняного сектору з метою створення власних операційних систем, антивірусних комплексів, телекомунікаційного обладнання (особливо це стосується об'єктів критичної інформаційної інфраструктури держави). У крайньому випадку використовувати засоби з відкритими кодами та інфраструктурою, що захистить від прихованих закладок чи інших можливих втручань у роботу таких засобів з боку неавторизованої сторони. ***7)*** *Створити систему (мережу) центрів реагування на*

кіберінциденти (типу CERT/CSIRT [56]), яка буде включати як загальнодержавні, так і локальні та галузеві центри (у таких критичних галузях як атомна енергетика, цивільна авіація тощо). На сьогодні Україна входить до восьми країн Європи (разом з Мальтою, Ісландією, Словаччиною, Болгарією, Грузією, Словенією та Литвою), які мають на своїй території тільки по одному такому центру, а для найбільшої за територією європейської країни, яка до того ж щорічно готує значну кількість фахівців у галузі інформаційної безпеки, це критично мало.

Висновки. Таким чином, у цій роботі проведено аналіз ключових понять у галузі кібербезпеки – КбП, КбТ та КбА, що містяться у міжнародних стандартах, нормативних документах провідних держав Європи і світу, а також у вітчизняних та закордонних наукових публікаціях. У результаті проведеного аналізу за різними критеріями було сформульовано узагальнені визначення зазначених понять. Також, висвітлено історію розвитку КбТ з моменту зародження обчислювальної техніки, появи перших примітивних засобів несанкціонованого доступу до інформації і до потужних КбА сьогодення. Проведено дослідження контрзаходів світової спільноти (зокрема, наведено характеристику стратегій кібербезпеки провідних держав світу) у відповідь на акти КбТ та з метою попередження інших нелегітимних дій у КбП. Крім того, ґрунтуючись на світовому досвіді і національних особливостях, сформульовано рекомендації щодо забезпечення кібербезпеки України, що включають у себе модернізацію законодавства, системи підготовки кадрів, створення підрозділів по боротьбі з кіберзлочинністю та центрів реагування на кіберінциденти, а також підтримку наукових досліджень та виробництва у цій галузі. 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.

Література

[1] Харченко В.П. Кибертерроризм на авиационном транспорте / В.П. Харченко, Ю.Б. Чеботаренко, О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк // Проблеми інформатизації та управління: Зб. наук. пр. : Вип. 4 (28). — К. : НАУ, 2009. — С. 131-140.

[2] Корченко О.Г. Ознаковий принцип формування класифікацій кібератак / О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк, В.М. Кінзерявий, С.В. Казмірчук // Вісник Східноукраїнського національного університету імені Володимира Даля — №1, 2010. — С. 32-38.

[3] ISO/IEC 27032, Information technology — Security techniques — Guidelines for cybersecurity. — 2012. — 50 p.

[4] National Military Strategy for Cyberspace Operations [Electronic resource]. — URL : http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

[5] Glossary and Acronyms (Archived) / European Commission [Electronic resource]. — URL : http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c

[6] Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space [Electronic resource]. — URL : // http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

[7] German Cyber Security Strategy [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

[8] Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. — К. : НАУ. — 2013. — 432 с.

[9] Погорецький М.А. Поняття кіберпростору як середовища вчинення злочину / М.А. Погорецький, В.П. Шеломенцев // Інформаційна безпека людини, суспільства, держави — №2 (2), 2009. — С. 80.

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

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

[12] Шеломенцев В.П. До концепції законопроекту про кібернетичну безпеку / В.П. Шеломенцев // Боротьба з Інтернет-злочинністю : матеріали міжнар. наук.-техн. конф. — Донецьк : ДЮІ МВС України, 2013. — С. 12-14.

[13] Компьютерная преступность и кибертерроризм / под ред. В.А. Голубева, Э.В. Рыжкова. — Запорожье : Центр исслед. компьютерной преступности, 2005. — Вып. 3. — 448 с.

[14] Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії / С.Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика) [Електронний ресурс]. — Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/bozk/2009_20/20text/g20_01.htm

[15] Pollitt M.M. «A Cyberterrorism Fact or Fancy?», Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285-289.

[16] Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хлань // Інформаційна безпека людини, суспільства, держави — №3 (7), 2011. — С. 49-53.

[17] Denning D.E. The Terrorism Research Center [Електронний ресурс] / D.E. Denning. — Режим доступу: http://www.washprofile.org/en/node/686

[18] Травников Ю. Преступления в паутине: границы без замков [Електронный ресурс] /

Ю. Травников. — Режим доступа: http://www.pl-computers.ru/article.cfm?Id=742&Page=3

[19] Климчик О.О. Кримінально-правова кваліфікація використання комп'ютерних технологій для вчинення терористичних актів / О.О. Климчик, Р.М. Кравченко // Інформаційна безпека людини, суспільства, держави — №1 (3), 2010. — С. 26-30.

[20] Малышенко Д.Г. Противодействие компьютерному терроризму — важнейшая задача современного общества и государства / Д.Г. Малышенко // ВНИИ МВД России, «Вестник РАЕН». — № 4 — Т. 3. — 2004.

[21] Старостина Е. Терроризм и кибертерроризм — новая угроза международной безопасности [Электронный ресурс]. — Режим доступа : http://www.crime–research.ru/articles/starostina

[22] Kerr K. Putting cyberterrorism into context [Electronic resource]. — URL : http://www.auscert.org.au/ render.html?it=3552

[23] Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно структурний аналіз): Монографія / В.М. Бутузов. — К. : КИТ, 2010. — 145 с.

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

[25] 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.

[26] Супертерроризм: новый вызов нового века / Научный записки ПИР-Центра // Под общей редакцией Федорова А.В. — М. : Изд-во «Права человека». — 2002. — С. 92-109.

[27] Пилипчук В.Г. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації / В.Г. Пилипчук, О.П. Дзьобань // Стратегічна пріоритети. — №4 (21), 2011. — С. 12-17.

[28] Тропина Т.Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Сборник научных трудов Международной конференции «Информационные технологии и безопасность». — Вып. 3. — К. : Национальная академия наук Украины, 2003. — С. 173-181.

[29] Гаврилов Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю.В. Гаврилов, Л.В. Смирнов. — М. : ЮИ МВД РФ, 2003. — 66 с.

[30] Старостина Е. Подход к выработке единого понятия «кибертерроризм» [Электронный ресурс]. — Режим доступа : http://rudocs.exdat.com/docs/index-198810.html

[31] Роговский Е.А. Россия в борьбе с международным тероризмом: грани повышения позитивного образа страны [Электронный ресурс]. — Режим доступа : http://www.rusus.ru/?act=read&id=66

[32] Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. — К. : ВІКНУ, 2011. — Вип. 30. — С. 159-165.

[33] McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, p. 217.

[34] Gemignani, Computer Crime: The Law in '80, Indiana Law Review, Vol. 13, 1980, p. 681.

[35] Per Concordiam, Журнал по проблемам безопасности и обороны Европы, Том 2, Выпуск 2, Garmisch-Partenkirchen, Germany, 68 с.

[36] Информационные вызовы национальной и международной безопасности / Под общей редакцией Федорова А.В. и Цыгичко В.Н. — М. : ПИР-Центр. — 2001. — 328 с.

[37] Anti-Malware [Electronic resource]. — URL : http://www.anti-malware.ru/

[38] SecurityLab [Electronic resource]. — URL : http://www.securitylab.ru/

[39] National Strategy to Secure Cyberspace [Electronic resource]. — URL : http://www.dhs.gov/national-strategy-secure-cyberspace

[40] IT Emergency and Crisis Exercises in Critical Infrastructures [Electronic resource]. — URL : http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf

[41] Cyber Security Strategy [Electronic resource]. — URL : http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

[42] Government Resolution on National Information Security Strategy [Electronic resource]. — URL : http://www.lvm.fi/c/document_library/get_file?folderId=57092&name=DLFE-5405.pdf&title=Valtioneuvoston%20 periaatep%C3%A4%C3%A4t%C3%B6s%20kansalliseksi%20tietoturvastra

[43] Canada's Cyber Security Strategy [Electronic resource]. — URL : http://publications.gc.ca/site/eng/379746/publication.html

[44] Information Security Research and Development Strategy [Electronic resource]. — URL : http://www.nisc.go.jp/eng/pdf/R_and_D_Strategy_eng.pdf

[45] Cyber Security Strategy of the Czech Republic for the 2011 – 2015 period [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

[46] Strategie de la France: Défense et sécurité des systèmes d'information [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

[47] Cyber Security Strategy for Germany [Electronic resource]. — URL : http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

[48] On the approval of the programme for the development of electronic information security (cyber-security) for 2011–2019 [Electronic resource]. — URL : http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

[49] Strategie nationale en matiere de cyber securite [Electronic resource]. — URL :

http://www.gouvernement.lu/salle_presse/actualite/2011/11-novembre/23-biltgen/dossier.pdf

[50] The National Cyber Security Strategy (NCSS): Success through cooperation [Electronic resource]. – URL : http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

[51] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World [Electronic resource]. – URL : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyber space.pdf

[52] Проведено перший у світі навчальний курс щодо захисту цивільної авіації від кіберзагроз [Електронний ресурс]. – Режим доступу: http://bit.nau.edu.ua/news.php?page=62

[53] Корченко О.Г. Актуальні проблеми забезпечення кібербезпеки цивільної авіації / О.Г. Корченко, С.О. Гнатюк // Захист інформації і безпека інформаційних систем : матеріали II міжнар. наук.-техн. конф. – Львів : Національний університет «Львівська політехніка», 2013. – С. 10-12.

[54] Корченко О.Г. Протидія кібертероризму на авіаційному транспорті / О.Г. Корченко, С.О. Гнатюк // Боротьба з Інтернет-злочинністю : матеріали міжнар. наук.-техн. конф. – Донецьк : ДЮІ МВС України, 2013. – С. 85-87.

[55] Cyber Security Strategy – A world-leading, resilient and vigorous cyberspace [Electronic resource]. – URL : http://www.nisc.go.jp/eng/pdf/CyberSecurityStrategy.pdf

[56] Гнатюк С.О. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки / Гнатюк С.О., Хохлачова Ю.Є., Охріменко А.О., Гребенькова А.К. // Захист інформації. – №1 (54). – 2012. – С. 121-126.

УДК 004.056.5:343.326 (045)

Гнатюк С.А. Кибертерроризм: история развития, современные тенденции и контрмеры

Аннотация. *Проблема кибертерроризма носит глобальный характер и достаточно остро стоит в современном информационном обществе. Кибератаки за достаточно короткий промежуток времени превратились из редких случаев в один из главных бизнес-рисков для организаций во всем мире. В глобальном контексте ведущие государства мира все больше внимания уделяют защите критических информационных ресурсов и возможности влияния на информационные ресурсы других государств. Однако существует ряд проблем различного характера, которые необходимо решить государствам как в национальных сегментах, так и во всем киберпространстве. Учитывая это, приведены различные толкования таких понятий как киберпространство, кибератака и кибертерроризм, предложено собственное видение каждого из понятий. Освещено обобщенную хронологию развития кибертерроризма и эволюции кибератак с момента зарождения вычислительной техники до настоящего времени. Также, приведены меры мирового сообщества в ответ на акты кибертерроризма и с целью предупреждения других нелегитимных действий в киберпространстве. Проведен анализ принятых ведущими государствами мира стратегий кибербезопасности и приведено их краткую характеристику. Кроме этого, основываясь на мировом опыте и национальных особенностях, сформулированы рекомендации по обеспечению кибербезопасности Украины.*

Ключевые слова: *киберпространство, кибербезопасность, кибертерроризм, кибератака, киберпреступление, стратегия кибербезопасности, критическая информационная инфраструктура государства, рекомендованные контрмеры.*

Gnatyuk S.O. Cyberterrorism: development history, current trends & countermeasures

Abstract. *The problem of cyberterrorism is global and quite acute in today's information society. Cyberattacks turned from single cases to one of the major business risks for organizations worldwide in a short period of time. In the global context leading world states are increasingly focused on critical information resources protection and possibilities to influence the information resources of other states. However, there are a number of different problems to be solved by states in national segments and throughout cyberspace. With this in mind, different interpretations of such concepts as cyberspace, cyberattack and cyberterrorism were showed, own vision of each concept were also offered. Generalized chronology of the cyberterrorism & cyberattacks since the computer technology emergence to today was highlighted. The measures of the international community responses to acts of cyberterrorism and to prevent other illegitimate actions in cyberspace were also showed. The analysis of adopted by the world's leading states cybersecurity strategies was carried out and a brief description of them was also given. In addition, the recommendations to provide cybersecurity of Ukraine, based on international experience and national features, were formulated.*

Key words: *cyberspace, cybersecurity, cyberterrorism, cyberattacks, cybercrime, cybersecurity strategy, critical information infrastructure of the state, recommended countermeasures.*

Отримано *20 травня 2013 року*, затверджено редколегією *10 червня 2013 року*