УДК 004.056.53

АРХИПОВ Олександр Євгенійович
БРОВКО Володимир Дмитрович

КІБЕРБЕЗПЕКА – ВИНИКНЕННЯ, ФОРМУВАННЯ, РОЗУМІННЯ

Постановка проблеми. Введена в дію Указом президента України в січні 2016 року Стратегія кібербезпеки України [1] являє собою базовий документ, що дозволяє почати узгоджену роботу зі створення системи кібербезпеки в Україні. Проте успішному виконанню цієї роботи явно не сприятиме відсутність єдиної термінології у сфері інформаційної/кібернетичної безпеки, яке, схоже, стає вже традиційною. До неоднозначного трактування деяких термінів в інформаційній сфері [2; 3] тепер приєднується невизначеність ще низки понять, які згадуються в стратегії кібербезпеки без будь-яких пояснень або посилань: ***кібернетична безпека, кібернетичний простір, кібернетична загроза*** і т. п. Слід зазначити, що відсутність єдиної термінології для будь-якої сфери діяльності є явищем суттєво негативним, до того ж аналіз публікацій стосовно змісту таких базових понять, як ***кіберпростір, кібербезпека*** свідчить про їх іноді абсолютно суперечливе розуміння фахівцями. Подібна ситуація є неприпустимою для повноцінного існування та ефективного розвитку сфери кібербезпеки. У запропонованій статті зроблено спробу порозумітися хоча б за деякими аспектами проблеми, що виникла.

Аналіз останніх досліджень і публікацій. На поточний момент кількість публікацій, які стосуються сфери кібербезпеки, стрімко зростає, причому багато з них містять матеріали за термінологічною тематикою, що є цілком зрозумілим, зважаючи на її актуальність. Автори, які вивчають це питання, пропонують різні підходи до його дослідження. Зокрема, достатньо поширена практика «колекціонування» не співпадаючих тлумачень певного терміна з наступним структуруванням цих тлумачень за деяким набором характерних аспектних відзнак (фасет) (наприклад [4, с. 10–11]), підрахунку рейтингів (частот входження) цих фасет у тлумачення, введенні до колекції з наступним намаганням сконструювати шляхом об’єднання найбільш рейтингових аспектних відзнак нового, більш досконалого визначення. На жаль, через таку «фасетну» збірку вдосконалене визначення терміна може втратити свою семантичну цілісність і трансформуватися в абсолютно безглуздий опис. Іноді корисним видається аналіз пар «полярних» або «дивних» одиничних визначень, наприклад [5]: «кібербезпека являє собою окремий ємний напрям, що існує поряд з інформаційною безпекою і вимагає самостійної проробки»,

«кібербезпеку слід також розглядати як частину духовної, а саме інформаційно-психологічної безпеки», «кіберзлочинність – це, серед іншого, поширення дитячої порнографії через сотовий зв'язок»; у іншого автора: «кібероб'єкт – будь-який об'єкт, функціонування якого здійснюється за участю засобів, що програмуються» [6].

Отже, **метою статті** є дослідження трактування деяких термінів в інформаційній сфері, а саме: кібербезпека, кіберпростір, кіберзагроза і т. п.

Для успішного проведення такого аналізу, зокрема, встановлення спроможності наведених вище висловлювань (принаймні хоча б їх частини), а також для формування загальних уявлень про зміст та основні визначення у сфері кібербезпеки, доцільно переглянути певні історичні події та факти, пов'язані з процесами виникнення і розвинення інформаційного та кіберпротиборства.

Виклад основного матеріалу. ***Ретроспектива стану інформаційного та кіберпротиборства з 1992 року.*** На початку 90-х років минулого століття військово-політичне керівництво США за підсумками оцінки результатів війни в районі Перської затоки прийняло рішення про доповнення традиційної програми захисту інформації у збройних силах США заходами з проникнення в системи державного і військового управління потенційних супротивників і економічних конкурентів. На практиці це було реалізовано через створення спеціальних організаційно-штатних структур і розробки відповідних документів, що регламентують їх діяльність. Першим з цих документів стала директива міністра оборони США TS-3600.1, прийнята в 1992 році [7], у якій дано поняття інформаційної війни, поставлені завдання перед міністерством оборони і комітетом начальників штабів (КНШ), визначені питання розвитку форм і способів ведення інформаційної війни, порядок розробки статутних документів та проведення наукових досліджень. Наступного року з'явилася директива КНШ МОР № 30-93, головний зміст якої склала нова концепція, що дістала назву «боротьби з системами бойового управління» [8]. Директива МОР № 30-93 фактично виокремила боротьбу з системами управління в самостійний вид оперативного забезпечення бойової діяльності військ. Теорія боротьби з системами управління отримала свій подальший розвиток у документах КНШ ЗС США «Спільні дії різнорідних сил по боротьбі з системами управління супротивника» [9] та «Єдина перспектива-2020» [10], які визначили основні напрямки розвитку оперативно-стратегічних концепцій застосування збройних сил в XXI столітті, наголосивши, що головною рисою збройної боротьби в наступному столітті буде перенесення акценту до сфери інформаційного протиборства (ІП). Практична реалізація концепції ІП здійснюється шляхом комплексного проведення за єдиним задумом і планом психологічних операцій, заходів із оперативної маскування, радіоелектронної боротьби та фізичного знищення пунктів управління і систем зв'язку з метою позбавлення противника інформації,

виведення з ладу або знищення його систем управління при одночасному захисті своїх від аналогічних дій» [8].

У подальшому, в період з 1995 по 2003 рік, корпорацією RAND Corporation на замовлення міністерства оборони США виконано низку дослідницьких робіт, які показали роль і місце ІП у збройній боротьбі, широкі можливості інформаційної зброї, стратегію її застосування [11]. Паралельно в міністерстві оборони США здійснено опрацювання та введення статутними документами нових способів застосування збройних сил, видів збройних сил і родів військ, у яких відображені концептуальні погляди військово-політичного керівництва на ведення інформаційної війни.

Були визначені практичні можливості впливу інформаційної зброї на національну безпеку, виявлені основні напрямки діяльності в області інформаційної політики, координація діяльності наукових і промислових організацій, визначено основні напрямки вдосконалення стратегії забезпечення безпеки національних інформаційних систем [12]. Результати цих робіт представлено в звіті MR-661-OSD (Strategic Information Warfare. A New Face of War) [13], де вперше з'являється термін «стратегічне інформаційне протиборство», зміст якого полягає у використанні державами глобального інформаційного простору та інфраструктури для проведення стратегічних військових операцій і зменшення сторонніх впливів на власний інформаційний ресурс». У звіті йдеться про те, що зміни в суспільно-політичному житті деяких держав, викликані швидкими темпами інформатизації та комп'ютеризації суспільства, ведуть до перегляду геополітичних поглядів керівництва, до виникнення нових стратегічних інтересів та важелів (перш за все в інформаційній сфері), наслідком чого є зміна політики, що проводиться цими країнами [12].

У 1998 році в звітах MR-963-OSD (The Day After ... in the American Strategic Infrastructure) [14] і MR-964-OSD (Strategic Information Warfare Rising) [15] відображається тогочасне розуміння стратегії ведення ІП та робиться спроба прогнозу динаміки формування ситуації у світі. Стає очевидним виокремлення в ІП кількох тенденцій, зокрема так званого ІП другого покоління: «принципово новий тип стратегічного протиборства, покликаний до життя інформаційною революцією, що вводить у коло можливих сфер протиборства інформаційний простір … і триває довгий час: тижні, місяці і роки» [15].

ІП другого покоління передбачає [16]:

– створення атмосфери бездуховності і аморальності, негативного ставлення до культурної спадщини серед громадян країни-супротивника;

– маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни-супротивника з метою створення політичної напруженості та хаосу;

– дестабілізацію політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалення недовіри,

підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни серед населення країни-супротивника;

– дезінформацію населення про роботу державних органів, підрив їхнього авторитету, дискредитацію органів управління;

– провокування соціальних, політичних, національних і релігійних зіткнень;

– ініціювання страйків, масових заворушень та інших акцій економічного протесту серед населення країни-супротивника;

– підрив міжнародного авторитету країни-супротивника, її співпраці з іншими країнами;

– будь-які дії соціально-політичного тиску на населення країни-супротивника.

Поступом у цьому напрямі для стратегічного ІП стала директива президента США PDD-68 від 30 квітня 1999 [17] про створення нової структури під назвою International Public Information (IPI), завданням якої є професійне використання розвідувальної інформації з метою здійснення впливу «на емоції, мотиви, поведінку іноземних урядів, організацій і окремих громадян». Вважається цілком можливим досягнення в майбутньому глобальної переваги в інформаційній боротьбі в психологічній сфері, що дозволить вирішувати конфлікти без збройного втручання [12].

Порівняно із наведеним вище, ІП першого покоління вважається більше орієнтованим на комплексні дії, пов'язані зі знищенням або дезорганізацією діяльності систем управління супротивника, ключових елементів систем його національної інфраструктури та реалізацією акцій із забезпечення військових операцій, що проводяться традиційними силами і засобами. Саме цей вид ІП, значно розширивши межі свого застосування поза мілітарної сфери, сприяв формуванню нового перспективного напряму, який через кілька років отримає назву боротьби у кіберпросторі. Розглянемо це питання дещо детальніше.

Нові погляди на стратегічне ІП змусили провідні країни світу переглянути оцінки вразливості щодо інформаційних загроз критичним елементам національної інфраструктури, зокрема інформаційної, та роль держави з координації робіт із протидії загрозам в інформаційній сфері.

У рамках розробки нової парадигми стратегії національної оборони у 1996 році президентом США Біллом Клінтоном була створена Комісія з питань захисту критичної інфраструктури (у користуванні вперше з'явився термін «критична інфраструктура») – President's Commission on Critical Infrastructure Protection (PCCIP). Метою її роботи стала перевірка залежності американської економіки і соціальної сфери від стану елементів критичної інфраструктури. У жовтні 1997 року Комісія видала свій звіт [18], у якому закликала до зміцнення безпеки США щодо постійно зростаючої вразливості взаємозалежних елементів її інфраструктури, таких як телекомунікації, енергетика, банківська сфера і фінанси, транспорт і основні державні служби. У тексті звіту були

використані терміни з приставкою **кібер**: «…У минулому ми були захищені від нападів ворога на інфраструктури широкими океанами й дружніми сусідами. Сьогодні еволюція **кіберзагроз** разюче змінила ситуацію. У **кіберпросторі** національні кордони відсутні. Електрони не зупиниш для того, щоб перевірити паспорт. Потенційно небезпечні **кібернапади** можуть бути задумані та підготовлені заздалегідь, а для їх втілення в життя знадобиться не більше кількох хвилин або й навіть секунд…». На підставі звіту PCCIP було створено Національний центр захисту інфраструктур, Офіс безпеки критичних інфраструктур, Національну раду із захисту інфраструктур, відкрито Комп'ютерну судову лабораторію міністерства оборони. У травні 1998 року президент Б. Клінтон підписав директиву PDD-63 [19], спрямовану на захист критичної інфраструктури. У січні 2001 року Рада національної та внутрішньої безпеки США ухвалила Національний план захисту інформаційних систем, у 2003 році було прийнято Національну стратегію захисту кіберпростору і фактично легітимізовано термін «кібербезпека».

Першими на ці заходи відгукнулися збройні сили США. Боротьба в кіберпросторі – вид бойових дій, що не відповідає традиційним канонам військового мистецтва і вимагає від армії, флоту і військово-повітряних сил специфічної підготовки, створення нових організаційних структур і ретельного концептуального обґрунтування. У листопаді 2006 року в США було створено кібернетичне командування військово-повітряних сил – AFCYBER (скорочення від англ. Air Force Cyber Command) [20], на базі якого із залученням інших підрозділів у 2009 році формується кібернетичне командування США (англ. United States Cyber Command, USCYBERCOM), завданням якого є забезпечення сталого і неперервного управління військами, стійкого взаємообміну інформацією, захисту відповідної інформаційної інфраструктури, що є необхідною гарантією стійкості і неперервності управління [21].

Структурно-логічне узагальнення викладених матеріалів. Наведена детальна ретроспектива розвинення інформаційного протиборства, зародження та формування в його межах нових напрямів, зокрема кіберпротиборства, дозволяє стверджувати наступне [3]: система термінів, утворених за допомогою приставки кібер – скороченої форми прикметника кібернетична, є похідною від терміна «кібернетика» – науки про управління, отримання, передачу та перетворенні інформації в кібернетичних системах (кіберсистемах) [22]. Вихідним поняттям кібернетики є управління, що представляє собою результат виконання цілеспрямованої впорядкованої послідовності перетворень інформації, які саме і забезпечуються кіберсистемою. З іншого боку, кіберсистема – це сукупність елементів, що реалізують набір інформаційних технологій, тобто кіберсистема є окремим видом більш загального родового поняття – інформаційної системи. Зважаючи на те, що кіберсистема зберігає базові

ознаки і структурні властивості інформаційної системи, спроба розрізнення інформаційної та кіберсистеми шляхом типового завдання дефініцій, що ґрунтується на результатах узагальненого структурного аналізу кожної з цих систем, приречена на невдачу [3]. Більш вдалим буде введення в дефініції відомостей про функціональне призначення відповідних систем, наприклад: кібернетична система – інформаційна система, призначена для виконання функції управління (зокрема прийняття рішень) у різних сферах діяльності. Сфера функціонування інформаційних систем – інформаційний простір, кіберсистем – кіберпростір. Через це кіберсистемам, як сегменту інформаційних систем, відповідає деяка обмежена ділянка ширшого інформаційного простору, яка і представляє кіберпростір. До речі, в одному з ключових доктринальних документів ВВС США, випущеному в 2010 році під назвою «Операції в кіберпросторі» [23], термін «кіберпростір» конкретизовано як «глобальна сфера (домен) всередині інформаційного простору, що представляє собою взаємопов'язану сукупність інфраструктур і інформаційних технологій, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані процесори та контролери». Переходячи до визначення терміна «кібербезпека», зазначимо, що чинний нині стандарт ISO/IEC 27032:2012 [24] містить таке визначення: «кібербезпека або безпека кіберпростору (cybersecurity, cyberspace security) – це збереження конфіденційності, цілісності та доступності інформації в кіберпросторі». Таке визначення можна трансформувати в більш коротку форму: безпека кіберпростору – безпека інформації в кіберпросторі. Сенс цього формулювання стає абсолютно зрозумілим, якщо прийняти до уваги те, що кіберпростору, як це було з'ясовано вище, відповідає лише деяка обмежена сфера інформаційного простору. Знов-таки, посилаючись на вже цитовану вище доктрину «Операції в кіберпросторі» [23], наведемо ще одне визначення, запозичене із неї: «кіберзахист – комплекс заходів щодо забезпечення сталої роботи комп'ютерних систем і мереж в умовах ведення противником боротьби в кіберпросторі. Включає запобігання загрозам, що виходять з кіберпростору, усунення наслідків їх здійснення, в тому числі захист, спостереження, виявлення та реагування на несанкціоновану активність в інформаційних системах і комп'ютерних мережах, інші заходи із забезпечення безпеки інформації».

Наведені вище визначення не є директивними, проте вони становлять значний інтерес як носії первинного, вихідного розуміння низки термінів з приставкою кібер-. Зважаючи на це зауваження, зазначимо стосовно прикладів окремих визначень, наведених у розділі *аналіз останніх досліджень і публікацій,* наступне: наявність на будь-якому об'єкті засобів, що програмуються, не є достатньою підставою приналежності цього об'єкта до кіберсистем; поширення дитячої порнографії через сотовий зв'язок, зважаючи на те, що останній виконує роль транспортного засобу, до кібербезпеки

відношення немає. Приймаючи до уваги, що до системи управління може бути включена людина, її психологічний стан здатний впливати на якість управління, однак навряд чи кібербезпеку слід розглядати як частину духовної, а саме інформаційно-психологічної безпеки людини. Очевидно, що останні два приклади мають безпосереднє відношення до інформаційної безпеки людини.

Висновки. Аналіз ретроспективи розвинення інформаційного протиборства, процесу зародження, формування та розвитку в його межах нового напряму – кіберпротиборства, дозволяє стверджувати наступне.

1 Протиборство (боротьба) в кіберпросторі – це складова інформаційного протиборства, суть якої становить процес суперництва конфліктуючих сторін, в якому кожна проводить стосовно іншої операції, заходи та акції, пов'язані зі знищенням, або дезорганізацію діяльності систем управління та зв'язку супротивника (кіберсистем), та, відповідно, залежних від них ключових елементів національної інфраструктури.

2 Мета функціонування кіберсистем – забезпечення вирішення управлінських завдань у різних видах діяльності.

3 Захисту в кіберсистемі підлягає специфічний вид інформації – управлінська інформація. Незахищеність цієї інформації може спричинити погіршення якості управління аж до настання катастрофічних наслідків як для об'єкта управління, так і для його оточення, зокрема персоналу і населення. Для сучасних кіберсистем, особливо систем управління критично важливими об'єктами, першочерговим завданням є забезпечення якості управління, зокрема його стійкості і безперервності.

4 Кібербезпека, безпека кіберпростору (cybersecurity, cyberspace security) – збереження цілісності, конфіденційності та доступності інформації, що циркулює в кіберсистемі (тобто інформації, що надходить в кіберсистему, накопичується та зберігається в ній для подальшої обробки), з метою забезпечення стійкості і безперервності реалізації кіберсистемою управлінських функцій щодо відповідних об'єктів управління.

5 Кіберпростір – простір, утворений інформаційними потоками і інформаційними полями, що зароджуються в процесі функціонування кібернетичних систем.

Список використаних джерел

1 Про Стратегію кібербезпеки України : Указ Президента України від 27 січня 2016 року № 96/2016.

2 Архипов О. Є. Положення про інформаційну безпеку в міжнародних стандартах / О. Є. Архипов, Є. О. Архипова // Інформаційна безпека людини, суспільства, держави. – 2010. – № 2(4). – С. 62–65.

3 Архипов А. Е. Приставка кибер-: все ли очевидно? / А. Е. Архипов // Захист інформації. – 2016. – Т. 18, № 3. – С. 203–209.

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

5 Тонконогов А. В. Кибернетическая безопасность: понятие и сущность феномена // Право и кибербезопасность. – 2013. – № 2.

6 Алеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. – 2014. – № 5(8). – С. 39–42.

7 DoD Directive TS-3600.1, «Information Warfare (U)», December 21, 1992.

8 МОР № 30-93, 1993 р. [Електронний ресурс]. – Режим доступу : https://fas.org/irp/offdocs/.

9 Directive № 3-13.1, 1995 р. [Електронний ресурс]. – Режим доступу : https://fas.org/irp/offdocs/.

10 Жуков В. Ведение информационной войны (взгляды военного руководства США) [Електронний ресурс]. – Режим доступу : http://www.psychomedia.org/index.php?page=psy&art=3209.

11 Анисько А.И. Реализация концепции информационной войны в США / А. И. Анисько, А.П. Бобовик // Наука и военная безопасность. – 2004. – № 3. – С. 59–63.

12 Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства / С. Гриняев // Зарубежное военное обозрение. – 2001. – № 8.

13 Roger C. Molander, Andrew S. Riddile, Peter A. Wilson. Strategic Information Warfare: A New Face of War. 1996. Edition: 1; RAND Corporation. Pages: 113 [Електронний ресурс]. – Режим доступу : https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf.

14 MR-963-OSD. The Day After ... in the American Strategic Infrastructure.

15 MR-964-OSD. Strategic Information Warfare Rising.

16 Стюгин М. А. Оценка информационной безопасности системы управления Российской Федерации [Електронний ресурс] / М. А. Стюгин. – Режим доступу : http://psyfactor.org/lib/styugin0.htm.

17 Presidential Decision Directive PDD 68 30 April 1999, International Public Information (IPI).

18 PCCIP. The Commission's Report [Електронний ресурс]. – Режим доступу : http://www.iwar.org.uk/cip/resources/pccip/info.html.

19 Critical Infrastructure Protection (PDD 63) [Електронний ресурс]. – Режим доступу : https://fas.org/irp/offdocs/pdd/pdd-63.htm.

20 Мединн А. Силы ВВС США, предназначенные для ведения боевых действий в киберпространстве, и взгляды командования на их применения / А. Мединн, С. Маринин // Зарубежное военное обозрение. – 2012. – № 6. – С. 54–59.

21 Мединн А. Силы кибероперацийВМС США и основные направления их применения / А. Мединн, С. Маринин // Зарубежное военное обозрение. – 2012. – № 9. – С. 67–72.

22 Большая Советская Энциклопедия. – изд. 3-е. – М. : Советская Энциклопедия, 1973. – Т. 12. – 624 с.

23 CYBERSPACE OPERATIONS. Air Force Doctrine Document 3-12. 15 July 2010 . Incorporating Change 1, 30 November 2011. Pages: 60 [Електронний ресурс]. – Режим доступу : http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-060.pdf.

24 ISO/IEC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity.

Теоретико-методологічні засади забезпечення інформаційної безпеки людини, суспільства, держави

Рецензенти:
доктор фізико-математичних наук
М. Савчук,
доктор технічних наук, професор,
заслужений діяч науки і техніки України
Є. Мачуський

Аннотация: Рассматривается сложившаяся на сегодняшний день ситуация, связанная со становлением терминологии в области кибербезопасности. Для понимания этой проблемы проанализирована ретроспектива развития сферы информационного противоборства, зарождение и развитие кибербезопасности.

Основной акцент в статье сделан на применении терминов с приставкой кибер-. Показано, что с ее помощью выделяется класс киберсистем, используемых для решения задач управленческого характера в самых разных видах деятельности. Однако по сравнению с традиционными системами управления, в которых для осуществления управления реализуется совокупность взаимоувязанных процессов сбора, накопления и обработки информации, в киберсистемах на первое место выдвигается требование непрерывности и устойчивости управления. Это требование может быть выполнено лишь при обеспечении условий кибербезопасности, то есть доступности, целостности и конфиденциальности исходной информации, привлекаемой для выработки управленческого решения.

В статье анализируются основные свойства современных киберсистем, содержание и взаимосвязь понятий «киберпространство», «кибербезопасность», «киберугроза».

Ключевые слова: информационное пространство, киберпространство, киберпротивоборство, киберсистема, кибербезопасность, киберугроза.

Abstract: The current situation, related to the cybersecurity terminology formation was considered in the article. To understand this problem, the retrospective of the information warfare development, the origin and formation of cybersecurity was analyzed.

The main emphasis in the article was on the use of terms with the cyber- prefix. It was shown that with its help the class of cybersystem, used to solve managerial problems in a variety of activities had been distinguished. However, in comparison with traditional management systems in which a set of interrelated processes of data collection, accumulation and processing is implemented, in cybersystems the requirement of continuity and sustainability of management is put first. This requirement can only be met if cybersecurity is ensured, i.e. accessibility, integrity and confidentiality of the initial information involved in the development of a management decision.

The main properties of modern cybersystems, the content and interrelation of the concepts «cyberspace», «cybersecurity», «cyberthreat» were analyzed in the article.

Key words: information space, cyberspace, cyber-opposition, cybersystem, cybersecurity, cyberthreat.