лише предметом наукових дискусій, але і елементом нашого інформаційного простору.

Сьогодні однозначно можна сказати, що ні держави, ні інші світові професійні інституції не можуть самостійно боротися в повній мірі із тими викликами, які постали у зв'язку із розширенням Інтернету. До них слід віднести наступні: виклики щодо кіберзлочинності, захист авторського права в мережі, хакерство в економічній та політичних сферах, тощо. Відповіді на них повинні бути дані із врахуванням основних стандартів Ради Європи і практики Європейського Суду з прав людини, які мають стати в законотворчій роботі напрямком щодо реформування законодавства щодо забезпечення інформаційної безпеки України. Особливої актуальності заслуговує питання вдосконалення програмного забезпечення діяльності основних державних інституцій, організацій та підприємств. Паралельно, усе вищевикладене свідчить про потребу прийняття нормативно-правових актів в яких був би передбачений механізм захисту інформаційних прав громадян від протиправних дій третіх осіб щодо інформації та обмеження її впливу на особу, в тому числі і в мережі Інтернет та посили роботу відповідних органів, що відповідають за інформаційну безпеку держави, особливо в такий небезпечний історичних період розвитку держави.

Література

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д.т.н., проф. В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2163-19.

УДК 34:004(043.2)

Татарінцева А. В., студентка,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Гусар О. А., к.ю.н.

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ЧАСТИНА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У процесі розвитку високих технологій виникло принципово нове середовище – кіберпростір, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережевокомп'ютерної складової частини.

Кіберпростір одночасно виступає як суб'єкт та об'єкт впливу. Сучасна успішна геополітика неможлива без стійкого домінування у кіберпросторі. Кіберборотьба набула стратегічного управлінського спрямування. Вона

проводиться без міжнародних правових обмежень у просторі та часі і характеризується високою ефективністю щодо досягнення воєнно-політичної мети. Вирішальним чинником досягнення успіху у світовому протиборстві стає інформаційно-технічна дезорганізація систем державного і воєнного управління та інформаційно-психологічна деморалізація населення країн, насамперед, складу їх збройних сил. Кіберпростір став невід'ємною частиною інформаційного простору та п'ятою сферою ведення збройної боротьби. Сама збройна боротьба, завдяки інформаційному чиннику, набула високого ступеня керованості [2, с. 174-175].

Відповідно до Указу Президента України від 1 травня 2014 року № 449/2014 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», з метою удосконалення правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері наголошувалося на необхідності прискорення розробки Стратегії кібернетичної безпеки України, положення якої мали визначати комплексні заходи організаційно-інформаційного і роз'яснювального характеру щодо всебічного висвітлення заходів з реалізації державної політики у сфері забезпечення інформаційної безпеки; запровадження посиленого контролю за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки, створення нової редакції Доктрини інформаційної безпеки України. Зазначені правові документи розроблені, проте заходи державної політики у сфері забезпечення кібернетичної безпеки чітко не окреслені, відсутній механізм реалізації самих положень, можна помітити брак міжвідомчого координування з питань забезпечення кібербезпеки держави [3, с. 112].

Я. Волков слушно зазначає, що сама «система національної безпеки нині постає об'єктом теорії геополітики. Такий характер взаємозв'язку теорії геополітики та безпеки обумовлений, з одного боку, усталеним у науці розширеним розумінням безпеки як системи, що забезпечує не тільки захист держави від загроз, а і її стабільний розвиток в економічному, політичному, соціальному та гуманітарному просторах. З іншого боку – змінився погляд на геополітику і передусім на роль фізико-географічного простору в розвитку держав. З'явилися поняття економічного, політичного, інформаційного, цивілізаційного просторів, по-новому розглядається характер протиборства держав та їх союзників на міжнародній арені».

І. Кефелі зазначає, зокрема, що наразі можна констатувати «встановлення міждисциплінарних зв'язків між кібернетикою й теорією інформації (в сучасному їх розумінні) і геополітикою в тій сфері знань,

яка отримала назву інформаційна (віртуальна) геополітика. Дослідження останньої в геостратегії набуває форми інформаційно-психологічної війни» [1, с. 45].

Проаналізувавши сучасний стан забезпечення кібербезпеки, можна зазначити, що складовою проблематики кібердобровольців є не унормовані в українському законодавстві та практиці механізми взаємовідносин держави (державних органів) із середовищем ІТ-фахівців безпекового спрямування (яких часто і відносять до «хакерів»).

Розв'язати проблеми стратегічного значення кібербезпекової сфери неможливо без однозначного розуміння стану, в якому перебуває умовний «вітчизняний кібербезпековий сектор». Принциповий огляд має однозначно й директивно вказати на системні проблеми та можливі способи їх розв'язання, на моменти дублювання функцій відомствами, причетними до інформаційної (кібер) безпеки або на функції, непритаманні певним відомствам, а також на елементи кібербезпекової сфери, які залишилися поза увагою цього сектору безпеки.

Крім проблем суто нормативно-правового напряму, доводиться констатувати брак міжвідомчого координування з питань забезпечення кібербезпеки держави. Наразі в Україні відсутні загальнонаціональні міжвідомчі координаційні структури, спроможні узгоджувати й координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі та створення ефективної системи захисту вітчизняного кіберпростору (в тому числі у військовій сфері). Водночас координування з питань забезпечення кібербезпеки держави має відбуватися на двох рівнях – стратегічному та оперативному. Стратегічне координування вочевидь є зоною відповідальності Ради національної безпеки і оборони, оперативне – спеціально уповноваженої структури (можливо, новоствореної спеціально для цих цілей).

Література

1. Дубов Д. В. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України: дис. ... д-ра політ. наук : спец. 21.01.01 «Основи нац. безпеки держави (політ. науки)» / Д. В. Дубов ; Нац. ін-т стратег. дослідж. - Київ, 2016. - 434 с.

2. Ліпкан В., Діордіца І., Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України / В. Ліпкан, І. Діордіца // Підприємництво, господарство і право. – № 5. – 2017. – С. 174-180.

3. Лук`янчук Р. В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук`янчук // Вісник Національної академії державного управління при Президентові України. - 2015. - № 3. - С. 110-116.