УДК 004.056(477)

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В РОБОТАХ УКРАЇНСЬКИХ НАУКОВЦІВ: ДЖЕРЕЛЬНИЙ АНАЛІЗ

ОСТРОВИЙ О. В.,
здобувач PhD Донецького державного університету управління
(м. Маріуполь)

У статті розглядаються напрацювання українських науковців з питань реалізації державної політики України в забезпеченні кібернетичної безпеки України. Розглянуто коло проблемних питань стосовно розвитку кібербезпекового сектору України. Наведено позиції вітчизняних дослідників щодо розбудови національної системи кібернетичного захисту.

Ключові слова: *кібернетична безпека, стратегія, нормативно-правові акти, система, кіберзагрози, аналіз.*

В статье рассматриваются наработки украинских ученых по вопросам реализации государственной политики Украины в обеспечении кибернетической безопасности Украины. Рассмотрен круг проблемных вопросов относительно развития кибербезопасного сектора Украины. Приведены рекомендации отечественных исследователей касающиеся развития национальной системы кибернетической безопасности.

Ключевые слова: *кибернетическая безопасность, стратегия, нормативно-правовые акты, система, киберугроза, анализ.*

The article examines the achievements of Ukrainian scientists on the implementation of Ukraine's state policy in ensuring cyber security of Ukraine. The range of problematic issues regarding the development of the cybersecurity sector of Ukraine is considered. The recommendations of Russian researchers on the development of the national cyber security system are given.

Keywords: *cyber security, strategy, regulations, system, cyber threat, analysis.*

Постановка проблеми. Динамічність світових процесів, розвиток інформаційного суспільства, військова агресія зі сторони Росії вимагають особливого ставлення до забезпечення кібербезпеки. Недосконаліть дієвих інструментів ефективної протидії кібератакам, незахищеність секторів вітчизняної економіки, державних структур, громадськості потребують застосування системного підходу до процесу формування системи кібербезпеки України.

Україна у 2006 році ратифікувала Конвенцію Ради Європи про кіберзлочинність (Будапештська конвенція), яка є першим і найбільш визнаним міжнародно-правовим документом у сфері боротьби з міжнародною і національною кіберзлочинністю. Загальна кількість країн, що ратифікували Конвенцію Ради Європи про кіберзлочинність, сягає 55, і, звісно, не

обмежується країнами-членами Ради Європи (Конвенцію ратифікували також США, Канада, Японія, Мексика, Австралія та багато інших країн), ігнорують підписання лише Росія та Китай.

В прийнятій у 2016 році «Стратегії кібербезпеки України» зазначено, що національна система кібербезпеки має, насамперед, забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури. Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи [1-2].

Даний документ слід розглядати як базовий, що визначає концептуальні засади, але разом з тим, мають бути також розроблені і конкретні державні програми, проекти, з чіткими організаційними механізмами, реалізація яких дозволить сформувати надійну систему кібербезпеки, враховуючи виклики сьогодення. Захист суспільства, державних інституцій вимагають комплексних зусиль від органів державної влади. Таким чином саме держава відіграє провідну роль в формуванні системи кібербезпеки в Україні.

Аналіз останніх досліджень та публікацій. Виходячи з цього спостерігається посилена увага до питань національної безпеки з боку наукового середовища. Так, дослідженню і розробці теоретичних, методологічних та практичних аспектів, механізмів державного управління, вирішенню ключових питань реалізації державної політики в сфері забезпечення кібернетичної безпеки присвячено роботи Горбаня О., Грицюка Ю., Діордіци І., Дубова Д., Ліпкана В., Шеломенцева В. та багатьох інших.

Метою статті є вивчення існуючих напрацювань і теоретичне обґрунтуванням забезпечення кібернетичної безпеки в Україні.

Виклад основного матеріалу досліджень. З наукової точки зору особливого значення набувають дослідження Ліпкана В.А., та його авторські дефініції, такі як, «кібербезпека», «система забезпечення безпеки», «система забезпечення національної безпеки», що є важливим для формування понятійно-категоріального апарату даної сфери. Так, під кібербезпекою розуміється «стан захищеності кіберпростору від кібератак, за якого забезпечується його сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз функціонуванню його елементів» [3, с. 188]. Система забезпечення безпеки трактується як «сукупність організаційно об'єднаних органів управління, сил і засобів, призначених для вирішення завдань щодо забезпечення національної безпеки» [4, с. 315].

Професор Грицюк Ю. І. наголошує, що національна система кібербезпеки має розглядатися як сукупність політичних, соціальних, економічних та інформаційних відносин разом з адміністративними і технологічними заходами, реалізація яких видається можливою тільки у тісній взаємодії державного і приватного секторів, а також розвинутого громадянського суспільства. Через

російську агресію, серед найактуальніших завдань, автор [5] виділяє необхідність створення спеціального центру кіберуправління у Збройних Силах України, який би мав його інтегрувати з іншими державними органами та усіма силовими структурами; такий центр має передбачати залучення до роботи ІТ-фахівців найвищої кваліфікації, при цьому дуже важливо, щоб такі фахівці мали достатню кваліфікацію, можливість постійного навчання, з метою здійснення надійного кіберзахисту як держави суспільства загалом, так і конкретної особи зокрема.

Шеломенцев В. П. серед основних загроз життєво важливим інтересам людини, суспільства, держави, які реалізуються за допомогою інформаційних, телекомунікаційних інформаційно-телекомунікаційних систем, наводить наступні:

– посягання на Інтернет-ресурси державних органів України з боку спецслужб інших держав, розвідувально-підривна діяльність іноземних спеціальних служб з використанням кіберпростору;

– використання кіберпростору у військових цілях, розробка іноземними державами нових видів зброї кібернетичного характеру;

– можливість втягування України у збройні конфлікти чи у протистояння з іншими державами через використання національного сегменту кіберпростору для здійснення кібератак на об’ єкти критичних інформаційних інфраструктур інших держав;

– зростаючі масштаби поширення кіберзлочинності;

– активізація проявів кібертероризму;

– негативні інформаційно-психологічні впливи на суспільну свідомість і маніпулювання нею з кіберпростору;

– несанкціонований доступ і розголошення за допомогою кіберпростору інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації;

– зростання загальної уразливості національного сегменту кіберпростору через значну відмінність у рівнях кіберзахисту державних інформаційних ресурсів, ресурсів комерційних структур, громадських об’ єднань та окремих користувачів [6].

Також цілком слушними є рекомендації Шеломенцева В. П. щодо забезпечення належного рівня кібербезпеки повинні бути сформовані:

– загальнодержавна система протидії кіберзлочинності та кібертероризму як сукупності спеціальних суб’єктів протидії кіберзлочинності і кібертероризму, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов’язаних правових, організаційних і технічних заходів, що ними здійснюються;

– загальнодержавна система кібернетичного захисту об’єктів національної критичної інфраструктури як сукупності спеціальних суб’єктів забезпечення кібернетичного захисту об’єктів національної критичної інфраструктури, засобів і методів, що ними використовуються, а також комплекс відповідних взаємопов’язаних правових, організаційних і технічних заходів [7].

Заслуговують на увагу наведені професором Гайворонським М. В. класифікація кіберзагроз, які автор пропонує поділити на наступні види:

таргетовані атаки (advanced persistent threat). Залежно від цілей можна

виділити дві протилежні тактики атак на комп'ютерні системи. Перший варіант – застосувати для атаки програмне забезпечення (вірус, троянський кінь), маючи на меті компрометацію якомога більшої кількості систем. Другий варіант – проводити атаку прицільно (звідки й назва «таргетовані», тобто націлені) для компрометації комп'ютерів конкретної установи або навіть конкретних користувачів (як правило, посадових осіб високого рангу або їхніх помічників, науковців, взагалі людей, які мають справу з особливо цінною інформацією);

кібертероризм (вплив на системи керування). Те, що називають власне кібертероризмом, – можливість впливу через комп'ютерну мережу (зокрема, Інтернет) на системи керування транспортом, промисловими об'єктами, будинками та будь-якими технологічними процесами. ІКТ надають терористам кілька інструментів: застосування комп'ютерних мереж для керування, координації дій і підготовки терактів; можливість терористів напряму звертатись до широкого кола людей, використовуючи сервіси сучасного Інтернету; потенційно будь-який технологічний процес, яким керує цифрова система керування (або SCADA), може стати об'єктом атаки кібертерористів;

кібервійни – Stuxnet – це є прообраз кіберзброї для ведення кібервійни, використовується для здійснення диверсій або відключення систем (наприклад, комплексів протиповітряної чи протиракетної оборони);

хактивізм – зловживання інформацією у соціальних мережах (вплив на суспільство). Деякі хакерські угруповання ставлять за мету видобування конфіденційної (іноді таємної) інформації і розкриття її шляхом розміщення в Інтернеті у вільному доступі. Як правило, йдеться про викриття таємних операцій, змов, корупції та інших дій на рівні урядів чи окремих політичних сил, які суперечать закону, принципам демократії й іншим загальнолюдським цінностям;

атаки на банківські системи (викрадення грошей). Чим ширше у банківській сфері застосовуються інформаційно-комунікаційні технології, тим більше можливостей для махінацій у цій сфері. Дуже поширеними є фішинг, викрадення і використання атрибутів платіжних карток, а також застосування дуже складного і досконалого шкідливого програмного забезпечення для втручання в роботу систем клієнт-банк;

атаки на електронний уряд. «Електронний уряд» – інформаційно-комунікаційна система, або об'єднання інформаційно-комунікаційних систем, що автоматизує інформаційну взаємодію органів державної влади та органів місцевого самоврядування з громадянами та суб'єктами господарювання з метою підвищення ефективності надання державних послуг. Атаки на електронний уряд можуть зашкодити функціонуванню такої системи, а у країнах з низьким рівнем впровадження інформаційно-комунікаційних технологій – підірвати довіру до демократичних перетвореньі технічного прогресу;

апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання [8].

Розглядаючи зміст національної системи кібербезпеки, Діордіца І. зазначає, що, вибір конкретних засобів і шляхів забезпечення кібернетичної безпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кібернетичних загроз. А організаційне забезпечення системи кібербезпеки автор розглядає як

цілеспрямовану діяльність суб'єкта забезпечення кібербезпеки, пов'язану зі: – створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі; – впорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації [9].

Проблема захисту критичної інфраструктури від кібернетичних загроз, на думку дослідника, повинна бути складовою частиною загальнодержавної системи кібернетичної безпеки. Для протидії сучасним загрозам у кіберпросторі системи захисту повинні мати змогу швидко адаптуватися до змін.

Проте, Діордіца І., зазначає, що в чинних нормативно-правових актах відсутня дефініція «кіберзагроза», і під «легітимацією кіберзагроз» пропонує розуміти їх узаконення або закріплення у нормативно правових актах. «Загрози кібербезпеці або кіберзагрози» – наявні та потенційно можливі явища і чинники, які створюють небезпеку для життєво важливих інтересів людини і громадянина, суспільства і держави в кібернетичній сфері. За відсутності єдиного уніфікованого визначення кіберзагроз актуальним є перегляд чинних нормативно-правових актів та їх доповнення. Нині існує низка таких документів, в яких вживається термін «кіберзагроза», але не дається його тлумачення, що може призвести до його неправильного застосування, помилок у притягненні до відповідальності та інших негативних наслідків [10-11].

Окремі питання адміністративно-правового та організаційного забезпечення кібернетичної безпеки розглядає Демедюк С. В., так, автор зазначає що, зарубіжний досвід правового та організаційного забезпечення кібербезпеки свідчить про зростання ролі науки у сфері захисту кіберпростору, про що свідчить створення у Великій Британії нового Інституту віртуальних досліджень (Virtual Research Institute). Досліджуючи дієвість адміністративно-правового регулювання забезпечення та організації кібербезпеки в зарубіжних країнах, автор доходить висновку, про те, що саме збільшення чисельності відповідних підрозділів у системі кіберзахисту сприяє високому рівню захисту. Так, у Великій Британії створено три регіональних поліцейських кіберпідрозділи The Police Central e-crime Unit, HMRC. У США оголошено про додатковий набір 1000 співробітників у спеціальний департамент кібербезпеки Управління національної безпеки (Department of Homeland Security). У січні 2013 р. у Гаазі було відкрито Європейський центр боротьби з кіберзлочинністю [12].

Питанням забезпечення кібернетичної безпеки присвячено ряд наукових праць Лук`янчука Р. В., в яких автор, розглядаючи шляхи вдосконалення кібернетичної безпеки, наголошує на тому, що держава повинна прискорити розробку та впровадження новітніх конкурентоспроможних ІКТ в усіх сферах суспільного життя; посилити відповідальність в контексті забезпечення неухильного дотримання власниками об'єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та технічного захисту інформації, захисту персональних даних; визначити напрямки розвитку національної інформаційної інфраструктури та її інтеграції до світової [13].

Серед перспектив наукових досліджень, враховуючи проведення антитерористичної операції, Лук`янчук Р. В., акцентує увагу на тому, що у найближчій перспективі прогнозується вжиття РФ подальших спеціальних

заходів щодо інформаційного впливу та можливих кібернетичних атак на національний сегмент кіберпростору з метою завдання шкоди об'єктам критичної інфраструктури, підриву авторитету чинної влади в нашій країні шляхом поширення неправдивої або викривленої інформації щодо діяльності центральних органів влади, військового командування, правоохоронних органів, а також стимулювання населення до участі в протестних акціях, насамперед використовуючи соціально-економічну проблематику. За таких умов політичне керівництво РФ ставить за мету нагнітання інформаційної істерії, до якої підсвідомо або цілеспрямовано долучаються й сепаратисти так званих ДНР та ЛНР. Виходячи з цього, автор наполягає на подальші наукові дослідження у контексті розробки дієвого механізму державного регулювання та забезпечення кібернетичної безпеки [14].

Джерелами загроз та викликів національній безпеці України в інформаційній сфері можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері ІТ злочинці, іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти інтересів України кібернетичних засобів як із середини держави, так і з-за меж її кордонів, зазначає Косогов О. М. та окремо виділяє загрозу використання української інформаційної інфраструктури як «транзитного майданчику» для приховування атаки на інформаційні ресурси третьої сторони, що може розцінюватись провідними країнами як дії держави з відповідними наслідками політичного, економічного, правового, а в перспективі, не виключено, і воєнного характеру [15].

Висновки і перспективи подальших досліджень. Проведений аналіз дає нам підстави стверджувати, що українськими дослідниками здійснено значні розробки в напрямі вирішення проблем реалізації ефективної державної політики забезпечення кібернетичної безпеки. Можна впевнено констатувати, що в цей час створено достатнє наукове підґрунтя для поступового формування національної системи кібернетичної безпеки. Разом з тим, виходячи з необхідності забезпечення високого рівня кібернетичної безпеки, наукові дослідження з даної проблематики мають поглиблюватись. При формуванні належного рівня системи кібернетичної безпеки України в сучасних умовах має приділятись увага удосконаленню методології стратегічного планування; методології прогнозування; розробці (використанню зарубіжних аналогів) методів моніторингу та контролю за дотриманням вимог до забезпечення кібернетичної безпеки, що і є перспективами подальших досліджень.

Література:

1. Стратегія кібербезпеки України від 15.03.2016 р. URL: http://zakon3.rada.gov.ua/laws/show/96/2016.

2. Горбань О. Ю. Інформаційна війна проти України та засоби її ведення. Вісник НАДУ: зб. наук. праць. 2015. № 1. С. 136-141.

3. Стратегічні комунікації: [словник] / Т. В. Попова, В. А. Ліпкан / за заг.ред. В. А. Ліпкана. К.:ФОП О.С.Ліпкан, 2016. С. 188.

4. Ліпкан В. А. Національна та міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан. – Вид. 2-ге, доп. і перероб. К.: Текст, 2008. С. 315

5. Грицюк Ю. І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. Науковий вісник НЛТУ України. 2016. Вип. 26.8. С. 327-337.

6. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 312–320.

7. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). Київ: Міжвідом. наук.-дослід. Центр з проблеми боротьби з організ. Злочинністю. 2012. № 2 (28). С. 299–309.

8. Грайворонський М. В. Сучасні підходи до забезпечення кібернетичної безпеки. Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (Київ, 21-23 травня 2015). Київ: НТУУ «КПІ», 2015. С. 10–17.

9. Діордіца І. В. Класифікація кіберзагроз та їх легітимізація у нормативно-правових актах України. Підприємництво, господарство і право. 2017. № 10. С 206-211.

10. Діордіца І. В. Поняття та зміст системи забезпечення кібербезпеки. Актуальні проблеми юриспруденції. №2. Том 1. 2017 р. С. 62-68.

11. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки Україною Підприємство, господарство і право. 2017. № 5. С.174-180.

12. Демедюк С. В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. Південноукраїнський правничий часопис. 2015. №2. С. 144-147.

13. Лук`янчук Р. В. Державне управління кібернетичною безпекою: шляхи вдосконалення в сучасних умовах. Електронне наукове фахове видання «Державне управління: удосконалення та розвиток». URL: http://www.dy.nayka.com.ua/?op=1&z=893

14. Лук`янчук Р. В. Державна політика в сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. Вісник НАДУ. № 3. 2015 р. С. 110-116.

15. Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору. Збірник наукових праць Харківського університету Повітряних Сил. 2014. Вип. 3. С. 127–130.

The article deals with the best practice of Ukrainian scholars on the Ukrainian state policy implementation as of the cybernetic security ensuring in Ukraine. The range of issues concerning the cyber-business sector development in Ukraine is considered. The positions of domestic researchers concerning the national system of

cybernetic protection development are presented.

Cybersecurity usually refers to activities and actions aimed at protecting cyberspace in the civilian and military spheres from threats that may damage or be associated with interconnected networks and information infrastructure. Cybersecurity aims to preserve the availability and integrity of networks and infrastructure, as well as the confidentiality of information contained therein.

Cybersecurity exists in the areas of information and traditional security to combat the sharp increase in cybercrime and, in some cases, in the presence of signs of cyberwarfare. There are three key factors that require global cybersecurity: widespread use of broadband network access, IT-based business and society, and social stratification of IT skills. In order to combat cybercrime and in response to social change, a lot of governments and institutions have launched a variety of cyber security initiatives, from guidance and standardization to comprehensive legislation and regulations.

The classification of cybernetic threats has been given in the article. The sources and threats to the national security of Ukraine have been identified. It has been proved that, based on the need to ensure a high level of cybernetic security, scientific research on this issue ought to be thoroughly studied. In forming the proper level of the cybernetic security system in Ukraine, in today's conditions attention has to be paid to improving the methodology of strategic planning; forecasting methodology; the development (use of foreign analogues) of monitoring and monitoring methods for compliance with the requirements as of the cybernetic security provision, which is the prospect of further research.