11. Драган Я.П. Принципи лінійності моделі в теорії управління / Я.П. Драган // Автоматика-95 : праці Другої укр. конф. з автомат. керув. – Львів : Вид-во НВЦ "ІТІС", 1995. – Т. 1. – 143 с. – 7-8.

12. Драган Я.П. Системний аналіз стану та обґрунтування основ сучасної теорії стохастичних сигналів: енергетична концепція, математичний субстрат, фізичне тлумачення / Я.П. Драган, Я.С. Сікора, Б.І. Яворський. – Львів : Вид-во НВФ "Українські технології", 2014. – 240 с.

13. Дрогомирецька Х.Т. Інтегрування деяких Ateb-функцій / Х.Т. Дрогомирецька // Вісник Державного університету "Львівська політехніка". – Сер.: Фізико-математичні науки. – Львів : Вид-во ДУ "Львівська політехніка". – 1997. – Вип. 46. – С. 108-110.

14. Лабунец В.Г. Алгебраическая теория сигналов и систем / В.Г. Лабунец. – Красноярск : Изд-во Ун-та, 1984. – 244 с.

15. Левитан Б.М. Операторы обобщенного сдвига и их некоторые применения / Б.М. Левитан. – М. : Изд-во "Физматгиз", 1962. – 324 с.

16. Льюнг Л. Идентификация систем. Теория для пользователей / Л. Льюнг. – М. : Изд-во "Наука", 1991. – 472 с.

17. Назаркевич М.А. Методи підвищення ефективності поліграфічного захисту засобами Ateb-функцій / М.А. Назаркевич. – Львів : Вид-во Львівської політехніки, 2011. – 288 с.

18. Пойда В.П. Спектральный анализ в дискретных ортогональных базисах / В.П. Пойда. – Минск : Изд-во "Навука і тэхніка", 1978. – 136 с.

19. Пуанкаре А. О науке / А. Пуанкаре. – М. : Изд-во "Наука", 1983. – 560 с.

20. Сеник П.М. Про Ateb-функції / П.М. Сеник // Доповіді АН УРСР. – Сер. А. – 1968. – Вип. 1. – С. 23-27.

21. Скляревич А.Н. Операторные методы в статистической динамике автоматических систем / А.Н. Скляревич. – М. : Изд-во "Наука", 1965. – 460 с.

22. Сокіл Б.І. Нелінійні коливання механічних систем і аналітичні методи їх досліджень : автореф. дис. на здобуття наук. ступеня д-ра техн. наук: спец. 05.02.09 – "Динаміка та міцність машин" / Сокіл Богдан Іванович; НУ "Львівська політехніка". – Львів, 2001. – 36 с.

23. Хармут Х.Ф. Передача информации ортогональными функциями / Х.Ф. Хармут. – М. : Изд-во "Связь", 1975. – 268 с.

24. Хиршман И.И. Преобразование типа свертки / И.И. Хиршман, Д.В. Уиддер. – М. : Изд-во ИИЛ, 1958. – 313 с.

25. Delsarte J. Sur une extension de la formule de Taylor / J. Delsarte // Journ. de math. pures et appl. – 1938. – Vol. 17, ser. 9. – Pp. 213-231.

26. Lundberg E. Om hypergoniometriska funktioner af komplexa variabla / E. Lundberg // Stockholm, 1879. English translation: On hypergoniometric functions of complex variables. In Preparation.

27. Rosenberg R. The Ateb(h) – functions and their proporties / R. Rosenberg // Quarterly of Applied Mathematics. – 1963. – Vol. 21, issue 1. – Pp. 37-47.

Надійшла до редакції 07.12.2016 р.

Драган Я.П., Дронюк И.М. **Системный анализ негармонических сигналов и систем и Ateb-функции**

Сделан обзор приложений оператора обобщенного сдвига к теории негармонических сигналов. Классическая теория коммуникации и обработки сигналов основывается на формальном аппарате теории гармонических функций. Но для сетей специального назначения важно использовать другие функции. Показано, что в коммуникации широко использовались разложения по функциям Бесселя, а также любая полная ортонормированная система функций может быть использована для разложения в ряды или интегралы, что является обобщениями разложений Фурье. Поэтому предложено в качестве базиса разложения использовать Ateb-функции, как ортонормированную систему. Показано, что так введенные преобразования образуют алгебру.

Ключевые слова: оператор обобщенного сдвига, Ateb-функции, алгебра Ateb-преобразований, сети специальной коммуникации.

Dragan Ya.P., Droniuk I.M. **System Analysis of Non-harmonic Signals and Systems and Ateb-function**

The article reviews the application of the generalized shift operator to the theory of non-harmonic signals. The classical theory of communication and signal processing is based on the formal apparatus of the harmonic functions theory. But for special purpose networks it is important to use other functions. It is shown that for expansions in series or integrals can be used, which is a generalization of the Fourier expansions in communication is widely used for the expansion of the Bessel functions, as well as any complete orthonormal system of functions. Therefore as basis decomposition we suggest using Ateb-functions like orthonormal system. It is shown that Ateb-transformation forms algebra.

Keywords: generalized shift operator, Ateb-functions, Ateb-transformation algebra, special purpose networks.

УДК 007:343.9:351.86:659.2/.4

КІБЕРІНТЕРВЕНЦІЯ ТА КІБЕРБЕЗПЕКА УКРАЇНИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЇХ ПОДОЛАННЯ

Ю.І. Грицюк[1]

Розглянуто деякі проблеми кіберінтервенції та кібербезпеки України, а також перспективи їх подолання. Наведено пріоритетні засади державної політики у сфері забезпечення кібернетичної безпеки України в умовах проведення військових дій з Росією. На підставі аналізу правових джерел визначено шляхи формування засад сучасної державної політики у сфері забезпечення кібернетичної безпеки України. Деталізовано основні загрози та напрями деструктивної діяльності Російської Федерації в інформаційному просторі України на шкоду національним інтересам держави. Обґрунтовано доцільність розроблення організаційно-правових та методологічних засад щодо забезпечення кібернетичної безпеки України в умовах ведення війни з Росією, а також побудови національної системи кібербезпеки.

Ключові слова: державні інформаційні ресурси, інформаційний суверенітет, вітчизняний інформаційний простір, гібридна війна, антитерористична операція, інформаційна атака, державна політика у сфері забезпечення кібернетичної безпеки, кібертероризм, кіберзлочинність, вітчизняний сегмент кіберпростору, об'єкти критичної інфраструктури, соціальні мережі, спеціальна інформаційна операція, війська інформаційних операцій, національна система кібербезпеки.

Вступ. За останнє десятиліття значно зросла кількість суспільно небезпечних дій в кіберпросторі України, спрямованих на нанесення шкоди її державним інтересам [4, 6, 8, 25]. Вчинення насильницьких посягань з боку інших суб'єктів на державні, політичні чи економічні інтереси шляхом втручання у процес функціонування їх учасників містить ознаки інтервенції [7, 14, 20, 23]. Оскільки подібні дії здійснюються з використанням комп'ютерних систем і в кіберпросторі держави, то такий вид злочину називається кібернетичною війною[2,3] або кібернетичною інтервенцією (кіберінтервенцією) [29, 30].

Прикладом кіберінтервенції була триденна безперервна кібератака на сайт Президента України В.А. Ющенка, яка розпочалася 30 жовтня 2007 року і нараховувала близько 18 тис. точкових атак, які здійснювалися з території Росії, Казахстану, України, США, Ізраїлю та Великобританії. Проте у Службі безпеки

[1] проф. Ю.І. Грицюк, д-р техн. наук, НУ "Львівська політехніка", E-mail: yurii.i.hrytsiuk@lpnu.ua
[2] Кібер-війна і світ. https://day.kyiv.ua/uk/article/den-planeti/kiber-viyna-i-svit
[3] Російсько-українська кібервійна. https://uk.wikipedia.org/wiki/Російсько-українська_кібервійна

України такі дії не викликали особливого здивування, адже сайти президентів різних країн світу постійно піддаються подібним хакерським атакам, та й протидіяти їм у той час було практично нічим. Окрім цього, влітку та восени 2016 року на сервери штабу Гілларі Клінтон (претендента у президенти США) були влаштовані численні хакерські атаки найімовірніше російськими спецслужбами, які, як прийнято в таких випадках, заперечують свою безпосередню причетність до них.

Отже, функціонування та захист вітчизняного як інформаційного, так ы кіберпростору є важливим завданням держави в умовах проведення військових дій з Росією на Сході нашої країни [10]. Аналізуючи загрози інформаційній безпеці України з погляду геополітичних спрямувань суміжних з нею держав, насамперед Росії [21], необхідно відзначити вкрай негативну тенденцію до збільшення кількості інформаційних матеріалів із відвертою антиукраїнською спрямованістю та упередженим висвітленням фактично всіх внутрішніх і зовнішніх процесів, які відбуваються як в Україні, так і на міжнародній арені за її участю.

Адже відомо [27], що Російські мас-медіа продовжують діяти у фарватері зовнішньополітичної агресивної політики Російської Федерації та забезпечують інформаційну підтримку дій її керівництва щодо України та її міжнародних інтересів, насамперед геополітичних. Так звана "гібридна війна" на Донбасі постійно супроводжується інформаційно-психологічними атаками з боку терористів та російських військових, а також передбачає блокування трансляції українських телерадіомовників. Російські інформаційні операції для забезпечення медійної переваги в Україні набувають нових форм. Залежно від особливостей розвитку військово-політичної обстановки Росії використовує будь-який привід, щоб розпочати чергову інформаційну атаку.

Однак, у доступній науковій літературі [1, 2, 5, 11, 13 та ін.] немає адекватного теоретичного обґрунтування процесу побудови національної системи кібербезпеки за такими основними напрямами [24, с. 142]: протидія кіберзлочинності; захист вітчизняного інформаційного простору в комп'ютерних мережах; забезпечення інформаційної безпеки критичної інфраструктури. Тому аналіз проблеми кіберінтервенції та кібербезпеки України, а також перспективи їх подолання є актуальним науково-практичним завданням, що сприяло виконанню цієї роботи та вимагає реалізації подальших досліджень.

Аналіз попередніх досліджень. Актуальні питання інформаційної безпеки держави досліджували: А. Марущак, В. Петрик, В. Ліпкан та інші фахівці. Проблемні питання забезпечення кібербезпеки розглядали у своїх наукових працях А.С. Алпеєв [1], В. Бурячок [3], А. Бабенко, В. Бутузов [4], В. Гавловский, В. Голубєв, С. Гнатюк, Д. Дубов [6, 7], В. Номоконов, С.В. Мельник [11], В. Петров [15], М. Погорецький, В. Шеломенцев [30] та ін. Проте у працях зазначених фахівців не визначалися пріоритетні засади державної політики у сфері забезпечення кібербезпеки в умовах проведення військових дій з Росією на Сході України, що свідчить про актуальність тематики дослідження.

Мета роботи полягає в деталізації пріоритетних напрямів державної політики у сфері забезпечення кібербезпеки України в умовах проведення військових дій з Росією на Сході нашої країни та визначити шляхи вдосконалення концептуальних засад ведення державної політики у вказаній сфері.

Викладення основного матеріалу. Відомо [3, 15, 18], що за останні роки різні сектори української економіки та й суспільне життя пересічних громадян стали дуже вразливими у кіберпросторі. Постійно страждають від періодичних кібератак державні та приватні компанії, до яких вони зовсім, як виявилося, не були готові. Шкода, але доводиться констатувати також той факт, що Україна немає навіть й сьогодні будь-яких дієвих інструментів для запобігання атак і їх ефективній протидії, а всі наявні заходи кіберзахисту, в основному, є безсистемними і, як наслідок, безуспішними.

Загроза кібербезпеці держави у вигляді кіберінтервенції може бути як зовнішньою, так і внутрішньою. Про те, наскільки потужними є на сьогодні кіберзлочинці, свідчать результати дослідження ООН, опубліковані ще в 2013 році, в якому розглядалися етапи становлення хакерів. Виявляється, спочатку хакери були дослідниками кіберсередовища як свого, так і чужого, тобто, працювали і експериментували, здебільшого, з цікавості. Потім вони почали прагнути слави, визнання та грошей, внаслідок чого кіберзлочинність стала транснаціональною. Потрібно визнати, що й українські хакери нічим не відрізняються від інших, не пасуть задніх, успішно беруть участь у різних міжнародних кіберструктурах. Наприклад, після подій навколо акту вандалізму на Говерлі[1], сайти організації "Євразійської спілки молоді", яка взяла на себе відповідальність за його проведення, були атаковані проукраїнською кіберспільнотою. Відповідь не забарилася – зазнали потужних атак сайти президента України та Служби безпеки України.

Отже, питання кіберінтервенції як загрози кібербезпеці держави є абсолютно новим явищем, яке потребує його ретельного дослідження. Особливо варто зупинитись на тих кіберзагрозах, які існують у зв'язку із розвитком інформаційного суспільства в умовах військової агресії зі сторони Росії. Дослідженню цієї проблеми за останні роки присвячено значну кількість праць, серед яких особливої уваги заслуговують напрацювання Г.Г. Почепцова, О.А. Баранова [2], В.В. Івановського, В.В. Петрова [15] тощо. В цих працях під поняттям кіберінтервенція розуміється окрема група суспільно небезпечних дій, спрямованих на нанесення шкоди кібернетичній інфраструктурі держави, а також життєво важливим сферам існування суспільства та особи.

Також існують різні підходи багатьох науковців до визначення поняття кібербезпеки, під якою вони розуміють стан захищеності життєво важливих інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз, пов'язаних з використанням ресурсів інформаційно-телекомунікаційних систем, так званого кіберпростору, за наявності якого забезпечуються гарантовані умови для реалізації державної інформаційної політики.

Водночас, Указом Президента України від 15.03.2016 р., № 96/2016 була введена в дію постанова Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України", в якій *кібербезпека* визначена як "стан захи-

[1] Акт вандалізму на горі Говерла, скоєний 18 жовтня 2007 р. російською екстремістською організацією "Євразійська спілка молоді", що полягав у знищенні тризубу та гранітного пам'ятного знаку, присвяченого Конституції України.

щеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. А в Проекті Стратегії забезпечення кібербезпеки України це поняття визначено як стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування та розвиток, своєчасне виявлення, запобігання та нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави".

Незважаючи на те, що на даний час дію цього документа скасовано, відповідно до Доктрини інформаційної безпеки України, інформаційна (кібернетична) складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки держави. Оскільки інформаційна безпека розглядається як невід'ємна складова кожної зі сфер національної безпеки, тому кібербезпеку держави варто розглядати як невід'ємну складову інформаційної безпеки [13, 14, 16, 17, 19 тощо]. При цьому кібербезпека охоплює тільки той сектор інформаційної безпеки, в якій для оброблення інформації застосовуються інформаційно-телекомунікаційні системи.

Головною метою "Стратегії кібербезпеки України" є створення умов для безпечного функціонування кіберпростору держави, його використання в інтересах суспільства і особи. Документ також передбачає комплекс заходів, спрямованих на боротьбу із кіберзагрозами, поглиблення міжнародного співробітництва у цій сфері, забезпечення захисту державних електронних інформаційних ресурсів та інформаційної інфраструктури. Задля реалізації цієї стратегії РНБО утворило Національний координаційний центр кібербезпеки як робочий орган Ради.

Однак, багато науковців вважають [1, 4, 6, 10, 34, 41, 42 та ін.], що в Україні цей документ хоча і називається стратегією, проте визначені в ньому основні засади кібербезпеки у світовій практиці не зовсім вважаються стратегічними. Головним атрибутом у закордонних стратегіях передбачається перелік конкретних проектів забезпечення кібербезпеки із кінцевим терміном їх реалізації, з виділеним фінансуванням і, що найголовніше, конкретними відповідальними. У нас це нагадує більше концепцію – напрями, куди треба рухатися зі своїми тактиками дій, власним, а не державним, фінансуванням і без ніякої відповідальності. При цьому 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.

Стосовно визначення таких понять, як кіберзлочинність та кіберзахист, то ще й до сьогодні точаться постійні дискусії як серед науковців, так і практиків щодо правильності їх формулювань. У міжнародній практиці є три документи щодо кібербезпеки, які варті уваги: рекомендації Агенції з кібербезпеки ЄС, рекомендації Міжнародного союзу електрозв'язку і рекомендації НАТО, де ці поняття мають точні та зрозумілі формулювання [18, 43, 44 тощо].

Також у світовій практиці вважається [31, 32, 33, 35, 36, 38, 39 та ін.], наскільки у законодавстві визначена термінологія, настільки можливо говорити про покарання злочинців. Тут йдеться про кримінальний кодекс, в якому має іс-

нувати окремий розділ, який визначає відповідальність за кіберзлочини. Але проблема в тому, що цими злочинами в Україні займається не один, а декілька органів. Наприклад, після того, як поліція виконала свою роботу, справа про кримінальну відповідальність спочатку направляється до прокуратури, а вже потім до суду. Не секрет, що багато українських прокурорів часто навіть не розуміють, що таке IP-адреса, не кажучи вже про іншу специфічну кібертермінологію. А в багатьох судах протокол допиту звинуваченого ведеться на друкарських машинах, часто навіть не електронних. Тобто, немає так званої культури роботи з електронними доказами, які дуже легко підробити, змінити і, врешті-решт, безповоротно втратити. У судочинстві України кібербезпека має дуже низький рівень пріоритету.

В Україні простий кіберзлочин – "зламування" сайту, наприклад, сторінки у соцмережі, це справа кіберполіції. Організована групова злочинна діяльність, наприклад, атака на Інтернет-банкінг, також входить до юрисдикції кіберполіції. Однак, відімкненням електростанції від міської мережі вже займається СБУ як кібертероризмом [25]. Коли ж відбуваються кібератаки по всій країні, наприклад, потяги Hyundai починають сходити з рейок, і це супроводжується військовою агресією з боку Росії, тоді має оголошуватися військовий стан, а фізичну агресію мають нейтралізувати Збройні сили України.

Проблеми, які ускладнюють боротьбу з кіберзлочинами в Україні, насамперед, пов'язані з відсутністю чіткого правового регулювання національної державної політики в сфері кібербезпеки [9, 22, 26]. Також відсутня єдина державна структура з координації протидії кіберзлочинам чи кібератакам, внаслідок чого існує загроза, наприклад, критичній інфраструктурі держави, спостерігається значне зростання комп'ютерного піратства і порушення авторських прав. Водночас, широке використання сучасних інформаційних технологій у сфері оборони і безпеки, а також створення єдиної автоматизованої системи управління Збройними силами України призвели до того, що кіберзахист України стає все більш вразливим до кіберзагроз. Розроблення нагальних заходів щодо зміцнення кібербезпеки держави є першочерговим завданням сьогодення ще й через російську агресію.

Зрозуміло, й до російської агресії було багато кіберзлочинів, коли хакери атакували Інтернет-магазини, банки, сайти партій тощо. З агресією ж Росії кількість кіберзлочинів зросла врази, а їх інтенсивність та наслідки обходяться в чималу суму [15, 28]. Одна із причин такого зростання – злочинність іде у кіберпростір, позаяк там обертаються значні гроші. На сьогодні найпоширенішим видом кіберзлочину вважається кардінг – фінансовий злочин, крадіжка грошей з будь-яких електронних рахунків, банківських карток тощо. Понад це, російські спецслужби активно використовують як своїх хакерів, так і з інших країн для економічної дестабілізації тих країн, які на даний момент є ідейними супротивниками. В Росії за останнє десятиліття спостерігається дуже високий рівень інтеграції хакерів з військовими організаціями, державними і приватними структурами, позаяк там задіяні різні інтереси та крутяться чималі кошти [23, 30].

Також, джерелами кіберзагроз можуть бути міжнародні злочинні групи хакерів, окремі злочинці підготовлені у сфері інформаційних технологій, іноземні

державні органи та силові структури, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти інтересів України кіберзасобів як з середини держави, так і з-за її меж. Такою ж реальною є загроза використання української інформаційної інфраструктури як "транзитного майданчика" для приховування атак на інформаційну інфраструктуру третьої сторони [38, 40].

Іншими загрозами в сфері кібербезпеки держави можна виділити: кіберзлочинність, кібертероризм та кібершпигунство, кібервійна (в т.ч. й гібридна), а самі кіберінтервенції часто є невід'ємними складовими перерахованих злодіянь. Злочини із використанням сучасних інформаційно-телекомунікаційних систем стають все звичнішою практикою в житті українських громадян. Найбільша увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного та виробничого секторів.

Інформація з обмеженим доступом, що знаходиться в національних інформаційних ресурсах, є постійним об'єктом зацікавленості кіберзлочинців з боку інших держав, організацій та приватних осіб. Окрім цього, все більшого поширення набуває політично вмотивована діяльність кібергруп, заангажованих кіберактивістів, які здійснюють атаки на урядові та приватні сайти, що призводить до порушень роботи відповідних інформаційних ресурсів, а також фінансових і матеріальних збитків чи втрати репутації.

З урахуванням широкої інформатизації сектору безпеки і оборони, зокрема, створення Єдиної автоматизованої системи управління (ЄАСУ) ЗС України[1,2] , оборонний потенціал держави стає більш чутливим до кіберзагроз. Впровадження провідними країнами сучасних кіберозброєнь перетворює кіберпростір на окрему сферу ведення військових дій. Вважається, що в найближчому майбутньому рівень обороноздатності країни буде визначатись наявністю у неї ефективних підрозділів для ведення бойових дій в кіберпросторі та здатністю протидіяти кібератакам у сфері оборони [12, 17, 22]. Отже, нагальною проблемою є створення якщо не кібернетичних військ України, то хоча б кібернетичних підрозділів у кожній військовій структурі.

Згідно з положеннями Стратегії [22], удосконалення потенціалу сектора безпеки та оборони України в сфері кібербезпеки має здійснюватися за рахунок реалізації різних заходів, основними серед яких мають бути такі:

1) Захист на об'єктах критичної інфраструктури технологічних процесів від несанкціонованого втручання в їх роботу, на яких контроль або моніторинг відбувається за допомогою інформаційно-комунікаційних систем.
2) Державне стратегічне планування та управління в сфері електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту шляхом впровадження інформаційно-комунікаційних систем.

[1] Пащетник О.Д. Деякі проблемні питання створення автоматизованих систем управління військами і зброєю у збройних силах України / О.Д. Пащетник, Л.І. Поліщук // Системи озброєння і військова техніка : зб. наук. праць. – 2015. – № 2(42). – С. 31-33.

[2] Демідов Б.О. Концептуальні положення щодо створення автоматизованої системи управління протиповітряною обороною держави / Б.О. Демідов, О.Ф. Величко, Ю.Ф. Кучеренко // Наука і оборона : зб. наук. праць. – 2014. – Вип. 3. – С. 51-56.

3) Створення центру кіберуправління у Збройних силах України для забезпечення кібербезпеки і кіберзахисту на стратегічному, оперативному і тактичному рівнях, у яких всі процеси управління мають відбуватися за допомогою інформаційно-комунікаційних систем.
4) Створення підрозділів кібербезпеки і кіберзахисту у Збройних силах України, у СБУ, у Національній поліції України та інших силових структурах, досягнення їхньої сумісності з відповідними підрозділами держав-членів НАТО, у яких контроль та моніторинг за всіма процесам має відбуватися за допомогою інформаційно-комунікаційних систем.
5) Розроблення та впровадження протоколів спільних дій з названими підрозділами у відповідних силових структурах, в т.ч. й обмін інформацією в режимі реального часу, організація швидкого реагування на кіберзагрози та кібератаки за допомогою інформаційно-комунікаційних систем.
6) Обмеження участі в заходах щодо забезпечення кібербезпеки будь-яких об'єктів, які знаходяться під контролем держави-агресора, визнаної Верховною Радою України, або країн та осіб, щодо яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні, а також обмеження використання продуктів, технологій і послуг таких об'єктів для кіберзахисту державних інформаційних ресурсів, посилення державного контролю в цій сфері.

Через російську агресію найактуальнішим із вказаних вище заходів є 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, в т.ч. і хакерів як своїх, так і з-за кордону, що потребуватиме додаткових грошових витрат, які згодом у стократ окупляться. 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.

Висновки

1. Виявлено, що на сьогодні реальні прояви кібератак на інформаційні ресурси України можуть призвести до порушень функціонування інформаційно-телекомунікаційних систем як звичайної, так і критичної інфраструктури, які безпосередньо впливають на стан національної безпеки і оборони держави. У зв'язку із цим наявні загрози вимагають впровадження державою комплексних заходів щодо забезпечення її кібербезпеки.

2. Встановлено, що сучасна державна політика України у сфері забезпечення її кібербезпеки має бути спрямована на: забезпечення інформаційного суверенітету держави у кіберпросторі, створення надійного захисту національного сегменту кіберпростору в умовах ведення військових дій з Росією; зміцнення обороноздатності держави у кіберпросторі; боротьбу з кіберзлочинністю та кібертероризмом; недопущення та запобігання втручанню у внутрішні справи України і припинення посягань на її Інтернет-ресурси з боку інших держав, особливо Російської Федерації; забезпечення участі України в загальноєвропейській системі кібербезпеки з дотриманням стандартів НАТО, а також її участі в міжнародному співробітництві у сфері боротьби з кіберзлочинністю та кі-

бертероризмом; запобігання проявам сепаратизму та радикалізму в національному сегменті кіберпростору, захист вітчизняного інформаційного простору, побудову національної системи кібербезпеки.

3. Виявлено, що за умови ведення військових дій з Російською Федерацією, визначення концептуальних засад державної політики у сфері забезпечення кібербезпеки держави нагальною потребою є активізація нормотворчої діяльності як науковців, так і практиків у сфері інформаційної безпеки. У зв'язку із цим вважається доцільним: пришвидшити розбудову Національної системи кібербезпеки, створити в структурі Збройних Сил України за світовими аналогами війська інформаційних операцій для протидії будь-яким посяганням, насамперед сусідньої держави, на національний сегмент кіберпростору; посилити кібернетичний захист об'єктів критичної інформаційної інфраструктури, які перебувають як у районі проведення воєнних дій на сході країни, так і в масштабах держави загалом; протидіяти зовнішнім спеціальним інформаційним операціям, здійснювати моніторинг кібернетичного простору для своєчасного виявлення, нейтралізації кібернетичних загроз і запобігання їм, боротьби з кібертероризмом з використанням кібернетичної зброї, недопущення економічної злочинності з боку сусідніх держав у вітчизняному кіберпросторі.

Література

1. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность / А.С. Алпеев // Вопросы кибербезопасности : журнал. – 2014. – Вып. № 5(8). [Электронный ресурс]. – Доступный с http://wiki.informationsecurity.club/doku.php/публикации:terminologiya-bezopasnosti-kiberbezopasnost-informatsionnaya-bezopasnost
2. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека" / О.А. Баранов // Правова інформатика : зб. наук. праць. – 2014. – № 2(42). – С. 54-62.
3. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / А.Л. Бурячок // Сучасна спеціальна техніка : зб. наук. праць. – 2011. – № 3 (26). – С. 104-114.
4. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : Вид-во КИТ, 2010. – 408 с.
5. Горбань О.Ю. Інформаційна війна проти України та засоби її ведення / О.Ю. Горбань // Вісник НАДУ : зб. наук. праць. – 2015. – № 1. – С. 136-141.
6. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : Вид-во НІСД, 2011. – 30 с.
7. Дубов Д.В. Стратегічні аспекти кібербезпеки України / Д.В. Дубов // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К. : Вид-во НІСД. – 2013. – № 4 (29). – С. 119-126.
8. Заикин Андрей. Почему защита АСУ ТП сегодня стала критически важной?. [Электронный ресурс]. – Доступный с http://www.securitylab.ru/analytics/484730.php
9. Конвенція про кіберзлочинність (набула чинність 01.07.2006) // Верховна Рада України. [Електронний ресурс]. – Доступний з http://zakon4.rada.gov.ua/laws/show/994_575
10. Лук'янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук'янчук // Вісник НАДУ : зб. наук. праць. – 2015. – Вип. 3. – С. 110-116.
11. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., м. Київ, 22 березня 2011 р. – К. : Вид-во НА СБ України. – 2011. – Ч. 2. – С. 43-48.
12. Напрями діяльності ГУР МОУ // Головне управління розвідки Міністерства оборони України. [Електронний ресурс]. – Доступний з http://www.gur.mil.gov.ua/content/directions.html
13. Национальная стратегия кибербезопасности (NCSS). От понимания к возможности. – Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. [Electronic resource]. – Mode of access http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2 Engelseversie
14. Основні завдання Державної служби спеціального зв'язку та захисту інформації України // Державна служба спеціального зв'язку та захисту інформації України. [Електронний ресурс]. – Доступний з http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=89831&cat_id=89828
15. Петров В.В. Щодо формування національної системи кібербезпеки України / В.В. Петров // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К. : Вид-во НІСД. – 2013. – № 4 (29). – С. 127–130.
16. Про внесення змін до Закону України "Про основи національної безпеки України" : проект Закону України щодо кібернетичної безпеки України від 07.03.13 р., № 2483. [Electronic resource]. – Mode of access http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998
17. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р., № 514/2009 // Офіційний вісник України. – 2009. – № 52. – Ст. 1783. – С. 7-14. – 20 лип. [Електронний ресурс]. – Доступний з http://zakon2.rada.gov.ua/laws/show/514/2009
18. Про затвердження Річної національної програми співробітництва Україна – НАТО на 2015 рік [Електронний ресурс] : Указ Президента України від 23 квіт. 2015 р., № 238/2015. [Електронний ресурс]. – Доступний з http://www.prezident.gov.ua
19. Про затвердження Стратегії національної безпеки // Указ Президента України від 26 трав. 2015 р., № 287/2015. [Електронний ресурс]. – Доступний з http://www.prezident.gov.ua
20. Про кіберзлочинність : Конвенція Ради Європи // Офіційний вісник України. – 2007. – № 65. – Ст. 2535. – С. 107-112. – Код акту 40846/2007. – 10 верес.
21. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" / Указ Президента України від 1 трав. 2014 р., № 449/2014. [Електронний ресурс]. – Доступний з http://www.prezident.gov.ua
22. Про Стратегічний оборонний бюлетень України. [Електронний ресурс]. – Доступний з http:// zakon2.rada.gov.ua/laws/show/771/2012/print1361272038412688
23. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. – Женева : Изд-во МСЭ, 2009. – С. 55-62. [Электронный ресурс]. – Доступный с http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru
24. Рязанцева І.М. Проблемні питання розбудови національної системи кібербезпеки / І.М. Рязанцева, В.В. Тулупов // Право і Безпека : наук. журнал. – 2014. – № 2 (53). – С. 140-144.
25. СБУ : Головні проблеми для України – тероризм і кіберзлочинність // Українська Правда. [Електронний ресурс]. – Доступний з http://www.pravda.com.ua/news/2012/03/23/6961285/
26. Соловйов С.Г. Інформаційна складова державної політики та управління : монографія / С.Г. Соловйов, О.Є. Бухтатий, Ю.В. Нестеряк та ін.; за заг. ред. Н.В. Грицяк; Нац. акад. держ. упр. при Президентові України. – К. : Вид-во К.І.С., 2015. – 319 с.
27. Управління боротьби з кіберзлочинністю / Міністерство внутрішніх справ України. [Електронний ресурс]. – Доступний з http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754
28. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В.М. Фурашев // Інформація і право : зб. наук. праць. – 2012. – № 2. – С. 162-169.
29. Что же такое кибербезопасность? // Бизнес без опасности : блог. [Электронный ресурс]. – Доступный с http://lukatsky.blogspot.com/2013/01/blog-post_28.html
30. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : зб. наук. праць. – 2012. – № 1(27). – С. 312-320.
31. Canada's Cyber Security Strategy: For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada, 2010. – 14 c. [Electronic resource]. – Mode of access http://www.publicsafety.gc.ca/cnt/rsrcs/ pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf
32. Cyber Security Strategy for Germany. – Berlin : Federal Ministry of the Interior. – 2011. – 15 c. [Electronic resource]. – Mode of access http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_ download.pdf?__blob=publicationFile
33. Cyber security strategy. – Commonwealth of Australia: Australian Government, 2009. [Electronic resource]. – Mode of access http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG Cyber Security Strategy - for website.pdf
34. Franscella J. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term / J. Franscella. [Electronic resource]. – Mode of access http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html

35. Information systems defence and security: France's strategy. – French Network and Information Security Agency. – 2011. – С. 23. [Electronic resource]. – Mode of access http://www.gouvernement.fr/ sites /default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf

36. Inkster N. Chinese Intelligence in the Cyber Age / N. Inkster // Survival: Global Politics and Strategy. – 2013. – Vol. 55, issue 1. Pp. 45–66.

37. National Cyber Security Strategies. Practical Guide on Development and Execution. –ENISA, 2012. [Electronic resource]. – Mode of access http://www.enisa.europa.eu/activities/Resilience-and-CI-IP/national-cyber-secu rity-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

38. National Cyber Security Strategy and 2013-2014 Action Plan. – Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, 2013. – Pp. 47-52. [Electronic resource]. – Mode of access http://www.ccdcoe. org/strategies/TUR_CyberSecurity.pdf

39. NCAFP. Cyberpower and National Security // American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy. – 2013. – Vol. 35. – № 1. – Pp. 45–58.

40. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) // Official Journal L 077, 13/03/2004. – Pp. 0001-0011. [Electronic resource]. – Mode of access http://www.eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

41. Lewis James A. Securing Cyberspace for the 44th Presidency / James A. Lewis // Center for Strategic and International Studies. [Electronic resource]. – Mode of access http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

42. Stubley D. What is Cyber Security? / D. Stubley. [Electronic resource]. – Mode of access http://www.7elements.co.uk/resources/blog /what-is-cyber-security

43. The Battle for Power on the Internet. [Electronic resource]. – Mode of access http://www.theatlantic. com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/

44. The national strategy to secure cyberspace. – Washington, 2003. – 60 с. [Electronic resource]. – Mode of access http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Надійшла до редакції 16.11.2016 р.

Грыцюк Ю.И. **Киберинтервенция и кибербезопасность Украины: проблемы и перспективы их преодоления**

Рассмотрены некоторые проблемы киберинтервенции и кибербезопасности Украины, а также перспективы их преодоления. Приведены приоритетные принципы государственной политики в сфере обеспечения кибербезопасности Украины в условиях проведения войны с Россией. На основании анализа правовых источников определены пути формирования основ современной государственной политики в сфере обеспечения кибербезопасности Украины. Детализированы основные угрозы и направления деструктивной деятельности Российской Федерации в информационном пространстве Украины в ущерб национальным интересам государства. Обоснована целесообразность разработки организационно-правовых и методологических основ по обеспечению кибербезопасности Украины в условиях ведения войны с Россией, а также построения национальной системы кибербезопасности.

Ключевые слова: государственные информационные ресурсы, информационный суверенитет, отечественное информационное пространство, гибридная война, антитеррористическая операция, информационная атака, государственная политика в сфере обеспечения кибернетической безопасности, кибертерроризм, киберпреступность, отечественный сегмент киберпространства, объекты критической инфраструктуры, социальные сети, специальная информационная операция, войска информационных операций, национальная система кибербезопасности.

Gryciuk Yu.I. **Cyber Intervention and Cyber Security of Ukraine: Problems and Prospects of Overcoming Them**

Some problems cybernetic intervention and cyber security of Ukraine and the prospects for overcoming them. Are given priority principles of state policy in the field of cyber security of Ukraine in conditions of war with Russia. Based on the analysis of the legal sources of the ways of developing the foundations of a modern state policy in the field of cyber security in Ukraine. Refine major threats and areas of destructive activities of the Russian Federation in the information space of Ukraine at the expense of national interests. The expediency of development of organizational, legal and methodological bases to ensure the cyber security of Ukraine in conditions of war with Russia, as well as the construction of a national cyber security system.

Keywords: government information resources, information sovereignty, national information space hibridna war against terrorism, information attack, state policy in the field of cyber security, cyberterrorism, cybercrime, the domestic segment of cyberspace, critical infrastructure, social networks, special information operations, the troops information operations, national cyber security system..

УДК 351.861

МЕТОДИКА РОЗРОБЛЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ОХОЛОДЖУВАЛЬНОГО ЕФЕКТУ В ПРОЦЕСІ НАГРІВАННЯ ЗРАЗКА ДЕРЕВИНИ, ПРОСОЧЕНОГО ВОДНОЮ ВОГНЕБІОЗАХИСНОЮ РЕЧОВИНОЮ

С.М. Чумаченко[1], С.В. Жартовський[2], О.М. Тітенко[3]

Розроблено методику розроблення математичної моделі охолоджувального ефекту в процесі нагрівання зразка деревини, просоченого водною вогнебіозахисною речовиною. Результати математичного моделювання свідчать про істотний охолоджувальний ефект від використання запропонованих антипіренів для вогнезахисту деревини, оскільки інтервал часу від початку теплового впливу до моменту початку полум'яного горіння для вогнезахищеної деревини у два з половиною рази більший, ніж для невогнезахищеної. Представлена методика пов'язує охолоджувальний ефект від використання водних вогнебіозахисних речовин для вогнезахисту деревини із вкладом у прогнозне подовження часу початкової стадії розвитку пожежі, її доцільно використовувати під час розроблення компонентного складу водних вогнебіозахисних речовин.

Ключові слова: методика, модель, антипірени, вогнезахисне просочення, водна вогнебіозахисна речовина.

Актуальність теми. Аналіз світових тенденцій використання екологічно безпечних матеріалів у будівництві свідчить про те, що деревина була і залишається популярним будівельним матеріалом. Але при цьому треба пам'ятати, що деревина є горючим матеріалом, а продукти її термодеструкції є надзвичайно токсичними. Статистичний аналіз, виконаний в Науково-дослідному інституті пожежної охорони (СРСР, Росія), свідчить про те, що у XX ст. у більш ніж 70 % випадків на пожежах саме деревина була основним горючим матеріалом, і при цьому кількість загиблих від загальної кількості загиблих на пожежах становить 92 %. Природно такою статистикою не можна задовольнятися, особливо коли йдеться про об'єкти з масовим перебуванням людей та/або об'єктах критичної інфраструктури. Отже, не втрачає актуальності питання якісного вогнезахисту деревини, яка входить до складу будівельних конструкцій [1, 2].

Попередні дослідження за темою. Для створення відповідних заходів і засобів вогнезахисту потрібно мати уявлення про складний хіміко-фізичний про-

[1] ст. наук. співроб. С.М. Чумаченко, д-р техн. наук – Український НДІ цивільного захисту ДСНС України;
[2] ст. наук. співроб. С.В. Жартовський, канд. техн. наук – Український НДІ цивільного захисту ДСНС України;
[3] ст. наук. співроб. О.М. Тітенко, канд. техн. наук – Український НДІ цивільного захисту ДСНС України