Державне управління

УДК 351.865

Живило Євген Олександрович
аспірант кафедри інформаційних технологій і систем управління
Харківського регіонального інституту державного управління
Національної академії державного управління при Президентові України
Живило Евгений Александрович
аспирант кафедры информационных технологий и систем управления
Харьковского регионального института государственного управления
Национальной академии государственного управления
при Президенте Украины
Zhivilo Evgen
Postgraduate Student of the
Department of Information Technologies and Management Systems
Kharkiv Regional Institute of Public Administration of the
National Academy of Public Administration under the President of Ukraine

СУЧАСНІ ПІДХОДИ ФОРМУВАННЯ ВИМОГ ДО СПРОМОЖНОСТЕЙ СКЛАДОВИХ СИЛ КІБЕРОБОРОНИ ДЕРЖАВИ
СОВРЕМЕННЫЕ ПОДХОДЫ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К ВОЗМОЖНОСТЯМ СОСТАВЛЯЮЩИМ СИЛЫ КИБЕРОБОРОНЫ ГОСУДАРСТВА
MODERN APPROACHES TO CREATING REQUIREMENTS FOR THE CAPACITIES OF THE COMPONENTS FORCES OF THE CYBER DEFENSE OF THE STATE

Анотація. *У статті визначені ключові завдання створення умов для забезпечення кібернетичного суверенітету України, в умовах сучасних загроз у кіберпросторі держави. Проаналізовані суспільно-політичні, економічні та інші умови реалізації воєнної політики України у кіберпросторі. Сформовано цілі застосування Україною воєнної сили у кібернетичному просторі.*

Визначено механізми формування та реалізації державної політики кібернетичної безпеки, за якими доцільно розглядати, проводити аналіз, порівняння та узагальнення моделі національної системи кібернетичної безпеки України, а саме: розподіл повноважень суб'єктів, які безпосередньо відповідають за реалізацію заходів із забезпечення інформаційної та кібернетичної безпеки; центральні елементи (складові); призначення основних елементів структури в рамках забезпечення кібероборони держави; засади здійснення політики у сфері кібернетичної безпеки; методи прийняття рішень та постановка оперативних цілей, дій за умов функціонування системи моніторингу та реагування на кібернетичні загрози (моніторингу та оцінки загроз, реагування розслідування, тощо) під час виявлення кібератак та кіберінцидентів на об'єктах інформаційної інфраструктури; роль складових національної системи кібернетичної безпеки, яка об'єднала у форматі співробітництва центральні органи виконавчої влади, військові формування, правоохоронні органи, органи державного регулювання у сфері інформатизації, телекомунікацій та захисту інформації, органи місцевого самоврядування, наукові установи і організації, громадські організації, професійні асоціації, представників приватного сектору, а також підприємства, установи та організації незалежно від форм власності, які здійснюють діяльність, пов'язану із забезпеченням функціонування або безпеки національного сегмента кібернетичного простору.

Ключові слова: *кібернетичний простір, кібернетичні загрози, кібероборона держави.*

Аннотация. *В статье определены ключевые задачи создания условий для обеспечения кибернетического суверенитета Украины, в условиях современных угроз в киберпространстве государства. Проанализированы общественно-политические, экономические и другие условия реализации военной политики Украины в киберпространстве. Сформированы цели применения Украиной военной силы в кибернетическом пространстве.*

Определены механизмы формирования и реализации государственной политики кибернетической безопасности, по которым целесообразно рассматривать, проводить анализ, проводить сравнение и обобщать модели национальной системы кибернетической безопасности Украины, а именно: распределение полномочий субъектов, которые непосредственно отвечают за реализацию мероприятий по обеспечению информационной и кибернетической безопасности; определены центральные элементы (составляющие); назначение основных элементов структуры в рамках обеспечения кибероборонь государства; основы осуществления политики в сфере кибернетической безопасности; методы принятия решений и постановка оперативных целей, действий в условиях функционирования системы мониторинга и реагирования на кибернетические угрозы (мониторинга и оценки угроз, реагирования расследования и т.д.) при обнаружении кибератак и киберинцидентив на объектах информационной инфраструктуры; роль составляющих национальной системы кибернетической безопасности, которая объединила в формате сотрудничества центральные органы исполнительной власти, военные формирования, правоохранительные органы, органы государственного

регулирования в сфере информатизации, телекоммуникаций и защиты информации, органы местного самоуправления, научные учреждения и организации, общественные организации, профессиональные ассоциации, представителей частного сектора, а также предприятия, учреждения и организации независимо от форм собственности, осуществляющих деятельность, связанную с по печение функционирования или безопасности национального сегмента кибернетического пространства.

Ключевые слова: *кибернетическое пространство, кибернетические угрозы, кибероборона государства.*

Summary. *The article defines the key tasks of creating conditions for ensuring the cyber sovereignty of Ukraine, in the conditions of modern threats in the cyberspace of the state. Analyzed socio-political, economic and other conditions for the implementation of the military policy of Ukraine in cyberspace. Formed the purpose of the use of military force by Ukraine in cyberspace.*

The mechanisms of formation and implementation of the state cyber security policy are identified, according to which it is advisable to review, analyze, compare and summarize the model of the national cyber security system of Ukraine, namely: the distribution of powers of the subjects who are directly responsible for implementing measures to ensure information and cyber security; central elements (components); the appointment of the main elements of the structure within the framework of ensuring the cyber defense of the state; the basics of cyber security policy; decision-making methods and setting operational objectives, actions in the conditions of functioning of the system for monitoring and responding to cyber threats (monitoring and assessing threats, responding to investigations, etc.) when cyber attacks and cyber incidents are detected at information infrastructure facilities; the role of the components of the national cyber security system, which

united in the format of cooperation the central executive authorities, military formations, law enforcement agencies, government regulatory authorities in the field of informatization, telecommunications and information protection, local governments, scientific institutions and organizations, public organizations, professional associations, representatives of the private sector, as well as enterprises, institutions and organizations, regardless of the form of activities related to the maintenance or security of the national cyberspace.

Key words: *cyber space, cyber threats, cyber defense of the state.*

Постановка проблеми. Головною загрозою в умовах сучасності для України є висока ймовірність запровадження в кіберпросторі великомасштабної агресії РФ проти України.

Усунення (мінімізація) загроз у кіберпросторі за умов агресії РФ та створення умов для відновлення військово-технологічної переваги в національному сегменті кіберпростору потребує мобілізації всіх воєнних і соціальних кібернетичних можливостей держави і суспільства, що передбачає комплексного підходу до планування дій, централізованого керівництва та координацію зусиль складових сектору безпеки і оборони, державних і громадських організацій, об’єднаних спільними цілями.

Аналіз останніх досліджень і публікацій. Проблеми забезпечення кібернетичної безпеки України (далі – КБ) в умовах гібридної війни, актуальні напрями підвищення ефективності системи забезпечення КБ, її функції та завдання розглядаються у наукових працях вітчизняних дослідників, а саме: Є. Ю. Бабіч [1], Д. В. Дубов [2], Н. Є. Новікова, І. В. Діордіци, С. В. Мельника, В. І. Кащука та інших.

Проте, незважаючи на значну кількість робіт із даної тематики, натепер залишилось багато невирішених питань щодо формування вимог до спроможностей складових сил кібероборони (далі – КО) України [2, с.12].

Формулювання цілей статті (постановка завдання). Мета статті полягає у дослідженні та формуванні вимог до спроможностей складових сил КО України, для досягнення якої поставлені такі завдання: запропонувати авторське розуміння даного поняття, визначити спроможності сил КО, сутність та їх призначення.

Виклад основного матеріалу. Основою кризового реагування на воєнні загрози в кіберпросторі Україна розглядає такі основні заходи і дії: взаємоузгоджене використання політико-дипломатичних, інформаційних та силових інструментів держави для протидії в кіберпросторі деструктивному тиску агресора на Україну та примушення його до дотримання норм міжнародного права та власних зобов'язань; постійне проведення розвідувальної діяльності в інтересах підготовки та проведення Україною воєнних кібернетичних дій та операцій у кіберпросторі; своєчасне повне або часткове розгортання підрозділів КБ, суб'єктів забезпечення КБ сектору безпеки і оборони які забезпечують кібербезпеку держави та приведення їх у готовність до виконання завдань в умовах особливого періоду, в умовах воєнного, надзвичайного стану і при виникненні кризових ситуацій, що загрожують національній безпеці України; здійснення заходів щодо кібернетичного захисту критичної інформаційної інфраструктури; локалізація та нейтралізація воєнного кіберконфлікту з метою недопущення його ескалації; регулювання та контроль виконання скоординованих дій відповідно до законодавства всіма органами державної влади, органами місцевого самоврядування і громадян в інтересах ліквідації воєнного конфлікту і відсічі агресії в кіберпросторі; переведення національної системи зв'язку,

загальнодержавних автоматизованих систем управління, урядових мереж, систем зв'язку і управління зброєю, інформаційно-телекомунікаційних мереж і систем органів військового управління на функціонування в умовах особливого періоду, мобілізація додаткових ресурсів для організації бойових дій (операцій) у кіберпросторі.

Цілі застосування Україною воєнної сили у кіберпросторі: відсіч кіберагресії з застосуванням наявних сил і засобів, форм і способів кібернетичної боротьби, недопущення ескалації та поширення кіберагресії у кіберпросторі України, виявлення, блокування нанесення втрат противнику та примушення його до відмови від подальшого застосування воєнної сили у кіберпросторі з повним відновленням кібернетичного суверенітету України; у разі воєнного кіберконфлікту всередині національного сегменту кіберпростору – ліквідація (локалізація, нейтралізація) у кіберпросторі не передбачених законом кіберформувань, посилення кіберзахисту важливої державної критичної інформаційної інфраструктури через використання кіберпростору.

Основу матеріально-технічної бази системи КО України становитиме Національний центр КБ, до складу якого входять головний центр захисту інформації та КБ ЗС України, CERT-UA ДССЗЗІ України, центр протидії кібертероризму СБ України, центр протидії кіберзлочинності МВС України та підрозділи розвідувальних органів України [3, с.3].

Складовими матеріально-технічної бази системи КО України є мережа відомчих центрів у сфері КБ суб'єктів забезпечення КБ постійної готовності та аналогічних центрів органів державної влади та приватного сектору.

Україна залишає за собою право на застосування воєнної сили для КО, відсічі кіберагресії РФ та відновлення свого кібернетичного суверенітету [4, с.1].

Ключовими завданнями створення умов для забезпечення кібернетичного суверенітету України є: дієве реформування системи забезпечення воєнної безпеки кіберпростору України до рівня, прийнятного для членства в ЄС і НАТО; створення ефективного сектору безпеки і оборони, що забезпечує достатні спроможності КО для відсічі кіберагресії; розвиток підрозділів КБ ЗС України за західними стандартами та досягнення сумісності із підрозділами КБ збройних силам держав - членів НАТО.

Загальна чисельність сил КО та загальна кількість традиційних кіберозброєнь в умовах мирного часу повинна бути нарощена. Основні зусилля планується зосередити на підвищенні рівня спроможностей підрозділів КБ для ведення дій (операцій) у кіберпросторі з одночасним радикальним оновленням якісних характеристик кіберозброєння і програмного забезпечення КО та КБ, у тому числі прийняття на озброєння принципово нових зразків.

Передбачається розширення можливостей головного центру захисту інформації та КБ ЗС України для забезпечення координації і контролю діяльності органів виконавчої влади, правоохоронних органів та військових формувань у сфері національної КО у мирний час, в особливий період, в умовах воєнного, надзвичайного стану і при виникненні кризових ситуацій, що загрожують національній безпеці України [5, с.6].

Суспільно-політичні, економічні та інші умови реалізації воєнної політики України у кіберпросторі. Україна перебуває в умовах гібридної війни з РФ, що вимагає посилення всіх політичних, воєнних, дипломатичних та економічних засобів і заходів.

Економічне забезпечення воєнної безпеки кіберпростору України здійснюватиметься шляхом формування і реалізації основних векторів розвитку в воєнно-економічній, військово-промисловій та військово-технічній сфері, головними напрямами якої є: визначення на державному рівні

довгострокових планів наукової (інноваційної) діяльності та планів матеріально-технічного забезпечення КО, створення і модернізації програмного та апаратного забезпечення КБ та кіберозброєння для потреб безпеки і оборони відповідно до характеру і масштабів воєнних кіберзагроз, цілей, пріоритетів і завдань воєнної політики держави у кіберпросторі; нарощування та впровадження системи стратегічного планування розвитку ОПК у сфері КО, за спорідненими цілями та завданнями воєнної політики держави у кіберпросторі; формування збалансованої структури ОПК у сфері КО, визначення пріоритетних напрямів його реформування і розвитку, технічного переозброєння, забезпечення максимального завантаження і нарощування науково-виробничого потенціалу у сфері КО; упровадження комплексу заходів, спрямованих на зниження залежності України від імпорту програмного та апаратного забезпечення воєнного призначення, підвищення ефективності міжнародного науково-технічного співробітництва; забезпечення сучасними зразками програмного та апаратного забезпечення КБ науково-дослідних, технологічних та проектних установ, конструкторських бюро у сфері КБ та КО, їх розроблення та виробництво силами вітчизняного ОПК.

Курс досягнення цілей воєнної політики України у кіберпросторі. Визначальним фактором зміцнення воєнної КБ України є нарощування спроможностей сил КО. Нарощування спроможностей підрозділів КБ ЗС України, ДССЗЗІ України, утворених відповідно до законів України ІВФ та ПрО спеціального призначення здійснюється з метою створення ефективних підрозділів, мобільних груп, оснащених сучасним кіберозброєнням, програмним та апаратним забезпеченням сил КО, здатних гарантовано забезпечити КО держави [6, с. 8].

Національні оборонні спроможності у кіберпросторі: удосконалення законодавства з питань КО держави, унормування діяльності у воєнній сфері та адаптації базових законодавчих, концептуальних і програмних документів з питань КО до сучасних реалій; удосконалення питань взаємодії і координації дій органів державної влади і складових сектору безпеки і оборони з урахуванням особливостей сучасної боротьби у кіберпросторі; створення та впровадження єдиної стратегії КО суб'єктів сектору безпеки та оборони; удосконалення системи кризового планування та управління у сфері КО, впровадження стандартів управління, прийнятих у державах - членах НАТО; удосконалення засад застосування та підготовки сил КО до дій в умовах сучасної кібервійни; пріоритетного розвитку центрів КБ ЗС України відповідно до стандартів НАТО; створення єдиної уніфікованої системи підготовки персоналу для сил КО з урахуванням досвіду держав - членів НАТО, цивільного сектору і бізнесу; реформування системи військової освіти і підготовки кадрів у сфері КБ, задіяних у сфері КО військовослужбовців та працівників правоохоронних органів; створення високого бойового потенціалу КО, шляхом проведення модернізації, створення нових систем і уніфікації зразків кіберозброєння, програмного та апаратного забезпечення КБ; ефективного використання двостороннього та багатостороннього співробітництва з партнерами та союзниками у військовій сфері; розроблення нормативних документів щодо проведення кібернетичних дій та операцій, з узгодженням понятійного апарату, визначенням профільних структурних підрозділів державних органів та їх завдань і повноважень у мирний час, в особливий період, в умовах воєнного, надзвичайного стану і при виникненні кризових ситуацій, що загрожують національній безпеці України.

Чисельність і структура сил КО та їх складових визначатиметься з урахуванням стану безпекового рівня у кіберпросторі та потреб КО України,

необхідності відсічі кіберагресії РФ і запобігання очікуваним конфліктам у кіберпросторі, з урахуванням фінансово-економічних можливостей держави. Сили КО повинні забезпечити спроможності, які передусім визначають їх здатність до захисту України у кіберпросторі та відбиття кіберагресії.

Забезпечення воєнної безпеки України у кіберпросторі належить ЗС України [7, с. 2].

У розв'язанні завдань із забезпечення воєнної безпеки України у кіберпросторі, підготовки її до КО, інші складові сектору безпеки і оборони з урахуванням компетенції, визначеної законом, відіграватимуть таку роль:

Міністерство закордонних справ України - забезпечення дипломатичними засобами розвитку складових КО у відповідності до досвіду держав - членів ЄС та НАТО, дипломатичне супроводження процесу вирішення завдань щодо забезпечення КО та захисту національних інтересів у кіберпросторі;

Служба безпеки України – протидія кібертероризму та кіберзагрозам у сфері державної безпеки, здійснення контррозвідувального забезпечення суб'єктів КБ України;

Служба зовнішньої розвідки України – добування в кіберпросторі розвідувальної інформації, участь у боротьбі з кібертероризмом, міжнародною організованою кіберзлочинністю, незаконною торгівлею кіберзброєю і технологіями її виготовлення;

Національна поліція України – протидія кіберзлочинності та боротьба з іншими правопорушеннями, які вчиняються з використанням інформаційно-телекомунікаційних систем та їх ресурсів.

ДССЗЗІ України - забезпечення кіберзахисту органів державної влади, урядового зв'язку та державних об'єктів критичної інформаційної

інфраструктури, забезпечує функціонування системи захищеного доступу державних органів до Інтернету.

На ОПК покладаються завдання із забезпечення створення і модернізації кіберозброєння, програмного та апаратного забезпечення КБ та КО для виконання визначених завдань безпеки і оборони відповідно до цілей, пріоритетів і задач воєнної політики держави у кіберпросторі.

ЗС України взаємодіятимуть з іншими складовими сектору безпеки і оборони у виконанні визначених для них завдань з КО та повинні уникати дублювання функцій і завдань своїх структурних підрозділів з функціями і завданнями підрозділів інших складових сил безпеки і оборони. ЗС України залучатимуться до здійснення активних заходів з КО національного кіберпростору України, забезпечення КБ військових формувань, у разі потреби надання військової допомоги іншим країнам, а також братимуть участь у міжнародному співробітництві у сфері КО, спільних кібернетичних операціях з НАТО.

Виконуючи завдання із забезпечення воєнної безпеки України у кіберпросторі сили оборони та їх складові будуть взаємодіяти та координувати діяльність (за окремими напрямками) між собою та з іншими складовими сектору безпеки і оборони, державними органами, органами місцевого самоврядування, неурядовими організаціями та об’єднаннями, зокрема волонтерськими, установами і підприємствами, у тому числі ОПК, громадянами, відповідними суб’єктами інших держав.

Міжнародні договори та угоди, дають можливість Україні розраховувати на підтримку з боку міжнародної спільноти у розвитку кібернетичних оборонних можливостей, що гарантуватимуть Україні воєнну безпеку у національному сегменті кіберпростору, у тому числі шляхом отримання сучасних інформаційно-комунікаційних та кібернетичних технологій та

спільної розробки новітніх кіберозброєнь, отримання закордонної воєнної допомоги.

Зовнішні гарантії КБ України поставатимуть шляхом формування мережі союзництва як з окремими державами та регіональними організаціями (шляхом укладення угод про спільну КО або військову допомогу), так і з міжнародними безпековими організаціями.

Водночас у середньостроковій перспективі Україна використовуватиме насамперед власні можливості реалізації кібернетичного суверенітету держави.

Україна буде інтегруватися до європейського кіберпростору. Пріоритетним завданням поглиблення співпраці з НАТО у сфері КО є досягнення до 2020 року повної сумісності підрозділів КБ ЗС України з відповідними силами держав - членів НАТО [4, с. 4; 5, с. 2; 6, с.3].

Фінансування потреб КО. Фінансування потреб КО держави здійснюється за рахунок і в межах коштів, визначених у законі про Державний бюджет України на діючий рік.

Пріоритетними напрямами фінансування потреб КО є: проведення інтенсивної підготовки особового складу військових частин та підрозділів сил КО; реалізація державного оборонного замовлення з урахуванням пріоритетності закупівель та розроблення нових зразків кіберозброєння, програмного та апаратного забезпечення КБ; виконання державних цільових програм реформування та розвитку ОПК за напрямом КО, розроблення, освоєння і впровадження нових захищених інформаційно-комунікаційних та кібернетичних технологій; реалізація соціальних і правових гарантій задійяних у сфері КО військовослужбовців та працівників правоохоронних органів.

Розвиток системи КО України. В інтересах забезпечення зниження ризиків у сфері воєнної безпеки держави у кіберпросторі створюється інтегрована система КО України.

У короткостроковій перспективі головні зусилля будуть спрямовані на створення та забезпечення функціонування сил КО України, насамперед на: запровадження з урахуванням досвіду збройного конфлікту в східних регіонах України нових методів керівництва КО, які грунтуються на стандартах НАТО та відповідають критерію високої ефективності за прийнятних витрат; удосконалення законодавчої бази з питань воєнної безпеки у кіберпросторі і КО, розроблення ефективного механізму реагування на кризові ситуації у кіберпросторі, розвиток системи управління в кібернетичних бойових діях і операціях; уточнення ролі і завдань складових сил КО на стратегічному, оперативному і тактичному рівнях, поетапне створення нових та розвиток функціонуючих організаційних структур сил КО України, підвищення фахового рівня військовослужбовців та працівників правоохоронних органів у сферах КБ та КО; досягнення оперативної сумісності складових сил КО України, планомірний перехід до стандартів НАТО в організації, озброєнні та підготовці військ (сил), а також у системі оперативного прийняття рішень; організацію спільної підготовки сил КО з виконання покладених на них завдань, перегляд підходів до підготовки і навчання особового складу; створення нових систем і модернізацію зразків кіберозброєння, програмного та апаратного забезпечення КБ і КО.

З вирішенням першочергових проблем, відбиттям кіберагресії та за сприятливих умов міжнародної обстановки, воєнно-політичної ситуації та наявності відповідного ресурсного забезпечення будуть упроваджуватися додаткові заходи забезпечення належної обороноздатності держави у кіберпросторі.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Формування вимог до спроможностей складових сил кібероборони держави є основою для підготовки та прийняття воєнно-політичних, воєнно-стратегічних, воєнно-економічних і військово-технічних рішень у сфері КО, розроблення відповідних концепцій та програм.

Керівництво діяльністю суб'єктів забезпечення воєнної безпеки держави в кіберпросторі в частині відсічі кіберагресії проти України, реалізації заходів із запобігання виникненню воєнних конфліктів через використання кіберпростору, підготовки держави до КО, національного сегменту кіберпростору здійснюється Президентом України відповідно до Конституції та законів України.

Література

1. Бабич Є. Ю. Забезпечення кібербезпеки в Україні / Є. Ю. Бабич // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 77–78.
2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К: НІСД, 2014. – С. 328.
3. Матриця досягнення стратегічних цілей і виконання основних завдань оборонної реформи, додаток № 1 до Стратегічного оборонного бюлетеня України, схваленого Указом Президента України від 6 червня 2016 р. № 240/2016 // Офіційний вісник Президента України від 22.06.2016 – 2016 р., № 17, стор. 11, ст. 466.
4. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5. – С. 128. – Ст. 71.

5. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 р. № 96/2016 // Офіційний вісник Президента України від 05.04.2016 – 2016 р., № 10, стор. 39, ст. 198.
6. Указ Президента України №47/2017, Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України". URL: https://www.president.gov.ua/documents/472017-21374
7. Указ Президента України №555/2015 Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року, "Про нову редакцію Воєнної доктрини України". URL: https://www.president.gov.ua/documents/5552015-19443

References

1. Babych Je. Ju. Zabezpechennja kiberbezpeky v Ukrajini / Je. Ju. Babych // Aktualjni zadachi ta dosjaghnennja u ghaluzi kiberbezpeky : materialy Vseukr. nauk.-prakt. konf., m. Kropyvnycjkyj, 23–25 lystop. 2016 r. – Kropyvnycjkyj : KNTU, 2016. – S. 77–78.
2. Dubov D. V. Kiberprostir jak novyj vymir gheopolitychnogho supernyctva : monoghrafija / D. V. Dubov. – K: NISD, 2014. – S. 328.
3. Matrycja dosjaghnennja strateghichnykh cilej i vykonannja osnovnykh zavdanj oboronnoji reformy, dodatok # 1 do Strateghichnogho oboronnogho bjuletenja Ukrajiny, skhvalenogho Ukazom Prezydenta Ukrajiny vid 6 chervnja 2016 r. # 240/2016 // Oficijnyj visnyk Prezydenta Ukrajiny vid 22.06.2016 – 2016 r., # 17, stor. 11, st. 466.
4. Pro ratyfikaciju Konvenciji pro kiberzlochynnistj: Zakon Ukrajiny vid 7 veresnja 2005 roku # 2824-IV // Vidomosti Verkhovnoji Rady Ukrajiny. – 2006. – # 5. – S. 128. – St. 71.

5. Strateghija kiberbezpeky Ukrajiny, zatverdzhena Ukazom Prezydenta Ukrajiny vid 15 bereznja 2016 r. # 96/2016 // Oficijnyj visnyk Prezydenta Ukrajiny vid 05.04.2016 – 2016 r., # 10, stor. 39, st. 198.
6. Ukaz Prezydenta Ukrajiny #47/2017, Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 29 ghrudnja 2016 roku “Pro Doktrynu informacijnoji bezpeky Ukrajiny”. URL: https://www.president.gov.ua/documents/472017-21374.
7. Ukaz Prezydenta Ukrajiny #555/2015 Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 2 veresnja 2015 roku, “Pro novu redakciju Vojennoji doktryny Ukrajiny”. URL: https://www.president.gov.ua/documents/5552015-19443.