УДК 519.6

[1]*Олександр Олександрович Черноног*
[2]*Євген Олександрович Живило*
[1]*Вадим Віталійович Машталір (канд. істор. наук)*

[1]*Генеральний штаб Збройних Сил України, Київ, Україна*
[2]*Військовий інститут телекомунікацій та інформатизації, Київ, Україна*

СТРАТЕГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Стратегія воєнної безпеки кіберпростору України (далі – Стратегія) грунтується на результатах аналізу та прогнозування воєнно-політичної обстановки, принципах оборонної достатності, високої готовності до оборони, системності оборонного планування, а також визначених Верховною Радою України засадах внутрішньої та зовнішньої політики. Основні положення Стратегії є похідними від Воєнної доктрини України та Стратегії національної безпеки України, розвивають їх положення за напрямами забезпечення воєнної безпеки кіберпростору України та спрямовані на протидію агресії з боку Російської Федерації у кіберпросторі.

Саме тому виконання зазначених вище критеріїв є необхідним для набуття членства в Європейському Союзі та Організації Північноатлантичного договору, забезпечення рівноправного взаємовигідного співробітництва за напрямом кібербезпеки (кібероборони) у воєнній, воєнно-економічній та військово-технічній сферах з усіма заінтересованими державами-партнерами.

Ключові слова: *воєнний кіберконфлікт; кібервійна; кібероборона.*

Вступ

В умовах глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає кібернетичний простір.

Сучасні технології дають змогу державам реалізувати власні інтереси без застосування збройних сил, або з їх застосуванням, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних впливів в кібернетичному просторі.

Тому формування та розвиток сектору безпеки і оборони, який має забезпечити адекватне і гнучке реагування на кібернетичні загрози, раціонально використовуючи можливості і ресурси, є одним з пріоритетів політики національної безпеки.

Постановка проблеми. Комплексне вдосконалення законодавства з питань кібернетичної безпеки і оборони України, зокрема розробка та затвердження Стратегії, визначить основні напрямки та механізми реалізації коротко- та середньострокових заходів щодо підвищення обороноздатності за напрямами забезпечення воєнної безпеки кіберпростору України, унормує структуру і склад сектору безпеки і оборони, систему управління, систематизує координацію та взаємодію органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, а також правоохоронних органів.

Аналіз останніх досліджень і публікацій. Аналіз рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" введеного в дію Указом Президента України № 287/2015 від 26 травня 2015 року [1], вимагає розроблення документів стратегічного планування у сфері забезпечення національної безпеки, а саме Стратегії кібербезпеки, яка визначить загальні принципи і обов'язки, на яких можна побудувати воєнну кібернетичну оборону.

Мета статті. Головною метою воєнної політики України в кіберпросторі є забезпечення її кібернетичного суверенітету та кібербезпеки сектору безпеки і оборони. Отже створення Стратегії є основою розвитку теоретичних засад за напрямами забезпечення воєнної безпеки кіберпростору та підготовки протидії агресії у кіберпросторі України.

Виклад основного матеріалу дослідження

1. Стратегія визначає організаційні, організаційно-технічні та правові основи розвитку системи кібернетичної безпеки Збройних Сил України, як основи системи кібероборони держави з урахуванням сучасної безпекової обстановки, що склалася в кіберпросторі навколо України та можливостей суб'єктів забезпечення кібербезпеки України постійної готовності.

Кібероборона є складовою оборони України, яка відповідно до Конституції України покладена на Збройні Сили України.

2. Метою Стратегії є: розвиток боєздатних, мобільних, якісно підготовлених, всебічно забезпечених, професійних підрозділів кібернетичної безпеки Збройних Сил України, здатних вчасно виявляти та адекватно реагувати на кібернетичні загрози воєнної сфери та сфери оборони, ефективно стримувати та гарантовано

ліквідувати (локалізувати, нейтралізувати) кібернетичні конфлікти на ранніх стадіях їх виникнення, готових до відбиття кібернетичних атак, ударів та агресії проти України в кіберпросторі;

інтегрування та поєднання зусиль різних складових сектору безпеки і оборони держави для створення ефективної системи кібероборони України, досягнення та постійного підтримання ефективних спроможностей Збройних Сил України у сферах забезпечення кібербезпеки та кібероборони і готовності до виконання покладених на них завдань.

3. Основні зусилля з розвитку системи кібернетичної безпеки Збройних Сил України в сучасних умовах зосереджуватимуться на комплексній розробці та впровадженні заходів та засобів по забезпеченню кібернетичної безпеки Збройних Сил України, Міністерства оборони України та кібероборони інформаційно-телекомунікаційних систем воєнної сфери та сфери оборони для забезпечення та підтримання на належному рівні обороноздатності держави у кіберпросторі.

4. Терміни, що вживаються у Стратегії, мають таке значення:

воєнна політика Збройних Сил України у кіберпросторі – діяльність Збройних Сил України, пов'язана із запобіганням воєнним кіберконфліктам у кіберпросторі, організацією та здійсненням підготовки Збройних Сил України до кібероборони держави;

воєнний кіберконфлікт – форма розв'язання міждержавних або внутрішньодержавних суперечностей із двостороннім застосуванням у кіберпросторі воєнної сили; основними видами воєнних конфліктів є кібервійна та збройний кіберконфлікт;

кібервійна – протиборство непримиренних держав (регіонів) у кіберпросторі із застосуванням воєнної сили для досягнення воєнно-політичних цілей, що зачіпають інтереси цих держав (регіонів);

збройний кіберконфлікт – зіткнення між державами у кіберпросторі із застосуванням кіберзброї (міжнародний збройний кіберконфлікт) або між ворогуючими сторонами в межах національного сегменту кіберпростору однієї держави, як правило, за підтримки ззовні (внутрішній збройний кіберконфлікт);

кібероборона – сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, спрямованих на захист кібернетичного суверенітету та забезпечення обороноздатності держави у кіберпросторі;

сили кібероборони – Збройні Сили України, Державна служба спеціального зв'язку та захисту інформації України, інші утворені відповідно до законів України військові формування, а також правоохоронні та розвідувальні органи, в частині залучення їх до виконання завдань з кібероборони держави;

спроможності сил кібероборони – здатність досягти необхідного результату під час виконання завдань з питань кібероборони у певних умовах відповідно до визначених сценаріїв дій та з використанням наявних ресурсів;

II. Кібербезпекове середовище у контексті забезпечення кібербезпеки Збройних Сил України та кібероборони держави

5. Кібербезпекове середовище у кіберпросторі довкола України складне та динамічне. Через збройний конфлікт на Сході України, воєнно-політичну нестабільність на Близькому Сході, боротьбу за вплив на світові фінансові та енергетичні потоки посилюється глобальна воєнно-політична нестабільність. Провідні держави збільшують розміри воєнних витрат, активізують розробку нових зразків кіберозброєння, підвищують інтенсивність військових навчань у кіберпросторі.

6. Головними тенденціями, що впливають на воєнно-політичну обстановку у кіберпросторі довкола України, є:

поширення практики проведення воєнних і спеціальних кібернетичних операцій та дій провокаційного характеру для створення конфліктних ситуацій у кіберпросторі;

інтенсивна модернізація збройних сил сусідніми державами, активізація розробок кіберозброєння та військових засобів програмно-математичного впливу нового покоління з принципово новими можливостями ураження і управління;

активне нав'язування в кіберпросторі дестабілізуючої зовнішньої політики Російської Федерації щодо сусідніх держав, а також щодо міжнародних організацій, включаючи НАТО та ЄС;

модернізація та вдосконалення спеціальними службами іноземних держав систем і комплексів технічної розвідки, нарощування їх можливостей, спроби несанкціонованого доступу до об'єктів інформаційної інфраструктури України, реалізація кібератак, впровадження програмних закладних пристроїв та розповсюдження спеціально створеного шкідливого програмного забезпечення.

7. Актуальними воєнними загрозами у кіберпросторі для Збройних Сил України є:

кіберагресія у національному сегменті кіберпростору України, нарощування у кіберпросторі військової кіберпотужності Російської Федерації;

мілітаризація Російською Федерацією кіберпростору шляхом формування та застосування нових військових з'єднань і частин, призначених для ведення бойових дій та операцій у кіберпросторі;

активізація спеціальними службами Російської Федерації розвідувально-підривної діяльності в національному сегменті кіберпростору Україні з

метою дестабілізації внутрішньої соціально-політичної обстановки в Україні, а також з метою підтримки не передбачених законом збройних формувань у східних регіонах України і створення умов для розширення масштабів кіберагресії;

діяльність у національному сегменті кіберпростору України не передбачених законом кіберформувань, спрямована на дестабілізацію внутрішньої соціально-політичної ситуації в Україні, залякування населення, позбавлення його волі до опору, порушення функціонування органів державної влади, місцевого самоврядування, важливих об'єктів промисловості та інформаційної інфраструктури;

цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин;

посягання Російською Федерацією на кіберсуверенітет України.

порушення функціонування об'єктів критичної інформаційної інфраструктури та зростання ризиків виникнення масштабних надзвичайних ситуацій, зумовлених веденням воєнних дій у кіберпросторі.

8. В найближчих роках з високою ймовірністю найбільш актуальними для Збройних Сил України кіберзагрозами і кіберконфліктами стануть:

проведення збройними силами іншої держави проти України кібернетичних дій та операцій, направлених на підрив обороноздатності, деморалізацію особового складу ЗСУ та інших військових формувань;

проведення іншою державою проти України кібернетичних операцій направлених на створення негативного іміджу Збройних Сил України у світі, перешкоджання міжнародному співробітництву та послаблення міжнародної підтримки Збройних Сил України;

проведення іншою державою проти Збройних Сил України воєнних кібернетичних операцій, направлених на деструктивний (руйнівний) вплив на автоматизовані системи управління, системи зв'язку і управління зброєю, інформаційно-телекомунікаційні мережі і системи або об'єкти критичної інформаційної інфраструктури Збройних Сил України;

здійснення системних та масштабних дій проти інтересів Збройних Сил України у кіберпросторі іноземними державами (групами держав) в т.ч. із залученням кіберпідрозділів збройних сил іноземних країн шляхом використання спеціальних засобів (кіберозброєнь), спрямованих на порушення стабільної роботи автоматизованих систем управління, систем зв'язку і управління зброєю, інформаційно-телекомунікаційних мереж і систем або об'єктів критичної інформаційної інфраструктури Збройних Сил України;

здійснення в національному сегменті кіберпростору України суспільно небезпечної діяльності в кіберпросторі (або з використанням його технічних можливостей) з терористичною метою шляхом застосуванням сучасних інформаційно-комунікаційних технологій, вчинення протиправних дій на шкоду третім державам, що здійснюються з використанням інформаційної інфраструктури України, що загрожують сталому та безпечному функціонуванню державних інформаційно-телекомунікаційних систем;

несанкціоноване отримання інформації з метою одержання особистої, економічної, політичної чи військової переваги, здійснюване з використанням обходу (злому) систем комп'ютерної безпеки, з застосуванням шкідливого програмного забезпечення, включаючи шпигунські програми.

9. Загрози воєнній безпеці України у кіберпросторі можуть бути реалізовані за такими сценаріями:

повномасштабна кіберагресія Російської Федерації проти України з рішучими воєнно-політичними цілями;

окрема спеціальна кібернетична операція Російської Федерації проти України із застосуванням військових підрозділів та/або частин, кібернетичних атак та ударів, інформаційних, інформаційно-психологічних операцій (дій) у кіберпросторі в сукупності з використанням невоєнних заходів кібернетичного впливу;

збройний кіберконфлікт всередині держави, інспірований Російською Федерацією з намаганням вплинути на відокремлення від України адміністративно-територіальні одиниці у східних та південних регіонах України, за участю не передбачених законом кіберформувань, кібертерористичних угруповань у взаємодії з політичними, неурядовими, етнічними, релігійними або іншими організаціями;

кібервійна Російської Федерації проти України.

Загрози воєнній безпеці України у кіберпросторі у разі їх реалізації можуть сприяти зміні конституційного ладу України, подальшої окупації України або її окремих територій, встановлення прямого або опосередкованого контролю над Україною та втрати нею державного суверенітету і територіальної цілісності.

10. На спроможності Збройних Сил України щодо адекватного реагування на виклики та ризики воєнній безпеці у кіберпросторі негативно впливають внутрішні економічні та соціально-політичні фактори:

розбалансованість і незавершеність системних реформ у сфері національної безпеки і оборони, недостатність ресурсного забезпечення сил кібероборони та неефективне використання наявних ресурсів;

недостатній рівень готовності Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, інших утворених відповідно до законів України військових формувань, а також правоохоронних органів спеціального призначення до ведення сучасної кібернетичної боротьби;

низька ефективність державних органів, що провадять розвідувальну і контррозвідувальну діяльність у кіберпросторі;

недостатній рівень координації і узгодженості дій органів державної влади, органів місцевого самоврядування, низький рівень підготовки їх спеціалістів з питань кібербезпеки і кібероборони;

недостатні та непрофесійні зусилля органів державної влади України у сфері протидії у кіберпросторі пропаганді та інформаційно-психологічним операціям Російської Федерації.

III. Сценарії реагування Збройних Сил України на кризові ситуації у кіберпросторі спільно зі складовими сектору безпеки і оборони

11. Ймовірність створення кризових ситуацій в національному сегменті кіберпростору зумовлена такими основними причинами:

збереження ймовірності використання противником у кіберпросторі як власних збройних сил, так і підтримуваних ними банд, груп іррегулярних сил та найманців як інструмента досягнення у кіберпросторі нашої держави власних інтересів;

прихована незаконна присутність підрозділів збройних сил Російської Федерації у кіберпросторі України**,** зовнішня підтримка нею діяльності терористичних та злочинних організацій у національному сегменті кіберпростору України, громадських і політичних об'єднань радикального спрямування;

12. Тенденції розвитку безпекового середовища, що склалося навколо України, визначають ймовірні сценарії реагування Збройних Сил України спільно зі складовими сектору безпеки і оборони на кризові ситуації, а саме:

кібероборона України, захист її кібернетичного суверенітету;

забезпечення воєнної безпеки кіберпростору України, у тому числі у сфері боротьби з кібертероризмом;

внесок у міжнародну стабільність та безпеку кіберпростору;

забезпечення інформаційної та кібернетичної безпеки кіберпростору України.

IV. Оцінка стану складових систем кібербезпеки Збройних Сил України та кібероборони держави

13. Нинішній стан складових систем кібербезпеки Збройних Сил України та кібероборони держави не дозволяє забезпечити ефективне реагування на сучасні виклики і загрози національній безпеці України в кіберпросторі.

Основними причинами є недостатній рівень підготовки керівного складу органів державного та військового управління у сфері кібернетичної безпеки, недосконаліть та незахищеність автоматизованих систем управління, систем зв'язку і управління зброєю, інформаційно-телекомунікаційних мереж і систем воєнної сфери та сфери оборони від програмно-математичних впливів (кібератак, кібердарів) на керуючі та ресурсні дані, інформацію і технологічні процеси цих систем, низький рівень соціального та нормативно-правового забезпечення задіяних у сфері кібербезпеки військовослужбовців, а також обмежені законодавчі повноваження та технічні спроможності сектору оборони по веденню активних (бойових) дій (операцій) у кіберпросторі.

14. Невирішеними проблемами у сфері забезпечення кібербезпеки Збройних Сил України та кібероборони держави є:

відсутність механізму концентрації можливостей/спроможностей складових системи кібероборони та основних її ресурсів для запобігання сучасним загрозам воєнній сфері та сфері оборони України у кіберпросторі;

недосконала нормативно-правова база в частині, що регламентує застосування методів та засобів кібербезпеки та кібероборони, необґрунтоване обмеження на час дії особливого періоду прав і можливостей військових підрозділів кібербезпеки на догоду дотриманню загально гуманітарних норм та наявність подекуди вузьковідомчого підходу керівництва складових сектору безпеки і оборони в питаннях забезпечення кібероборони держави;

недосконала система спільної діяльності складових сектору безпеки і оборони щодо прогнозування та упередження потенційних ризиків, викликів і загроз обороноздатності України в кіберпросторі;

недосконала система планування та спільного застосування військ (сил) та засобів сектору безпеки і оборони, їх підготовки та забезпечення для виконання завдань в кіберпросторі.

15. Основна мета розвитку сектору безпеки і оборони України у сфері кібероборони є забезпечення під єдиним керівництвом спроможності його складових для спільного виконання суб'єктами кібербезпеки постійної готовності завдань щодо кібероборони України, захисту кібернетичного суверенітету та забезпечення обороноздатності держави в кіберпросторі з дотриманням принципу оборонної достатності.

V. Цілі та основні завдання воєнної політики Збройних Сил України у кіберпросторі

16. Головною метою воєнної політики Збройних Сил України у кіберпросторі є координація кібероборони держави та забезпечення кібербезпеки Збройних Сил України.

17. Головною метою воєнної політики Збройних Сил України у кіберпросторі в системі кібероборони є забезпечення кібернетичного суверенітету України та кібербезпеки сектору безпеки і оборони.

18. Основними цілями воєнної політики Збройних Сил України у кіберпросторі є:

участь у відбитті у кіберпросторі агресії іноземних держав проти України;

участь у забезпеченні обороноздатності України у кіберпросторі на рівні, достатньому для запобігання виникненню воєнного кіберконфлікту, а у разі воєнного кіберконфлікту – для його локалізації і нейтралізації;

ведення кібервійни, локалізація і нейтралізація збройних кіберконфліктів у разі їх настання;

участь Збройних Сил України у реалізації спільної політики безпеки і оборони кіберпростору Європейського Союзу;

удосконалення системи забезпечення воєнної безпеки кіберпростору України, яка б відповідала критеріям членства України в ЄС і НАТО та гарантувала надійний захист держави від зовнішніх та внутрішніх кіберзагроз.

19. Виходячи із засад внутрішньої і зовнішньої політики, з урахуванням характеру актуальних кіберзагроз воєнній безпеці, основними завданнями воєнної політики Збройних Сил України у кіберпросторі у найближчий час і в середньостроковій перспективі є:

постійне, комплексне та цілеспрямоване вжиття заходів по забезпеченню воєнної політики Збройних Сил України у кіберпросторі як в мирний час, так і в особливий період;

участь у створенні єдиної системи кібероборони з відповідною інфраструктурою отримання та обробки даних в режимі часу, наближеного до реального (рисунок 1);

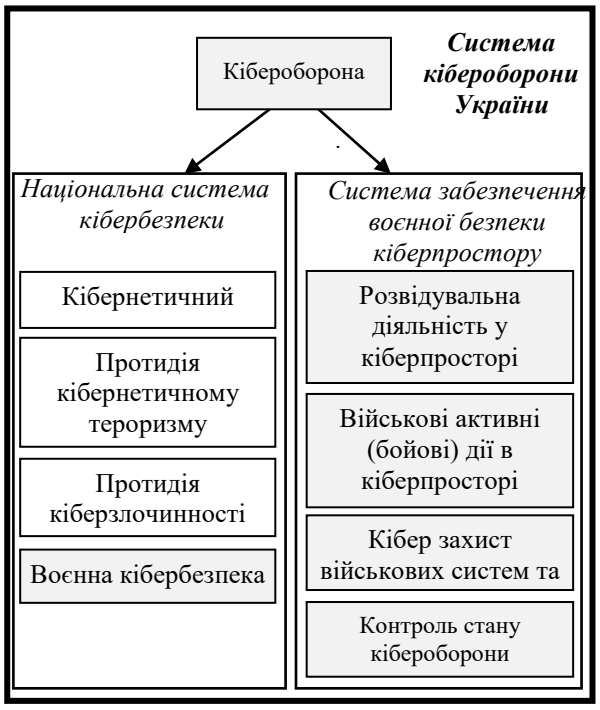

Рис. 1. Участь Збройних Сил України у забезпеченні воєнної політики України у кіберпросторі

участь у створенні національної системи кібербезпеки України за напрямом забезпечення воєнної кібербезпеки та в інтеграції спроможностей її складових для своєчасного і ефективного реагування на наявні та потенційні кіберзагрози сектору безпеки держави;

створення цілісної системи забезпечення воєнної безпеки кіберпростору держави зі складовими: розвідувальна діяльність у кіберпросторі; кіберзахист військових систем та об'єктів; військові активні (бойові) дії в кіберпросторі; контроль стану кібероборони. Інтеграція спроможностей складових цієї системи для своєчасного і ефективного реагування на наявні та потенційні кіберзагрози сектору оборони держави;

створення цілісної системи забезпечення кібербезпеки Збройних Сил України з функціями (рисунок 2): координація кібероборони; організація та забезпечення воєнної кібербезпеки; участь в розвідувальної діяльності у кіберпросторі; організація та забезпечення кіберзахисту військових систем та об'єктів; організація та забезпечення військових активних (бойових) дій в кіберпросторі; організація та забезпечення контролю стану кібероборони. Інтеграція спроможностей складових цієї системи для своєчасного і ефективного реагування на наявні та потенційні кіберзагрози Збройних Сил України;

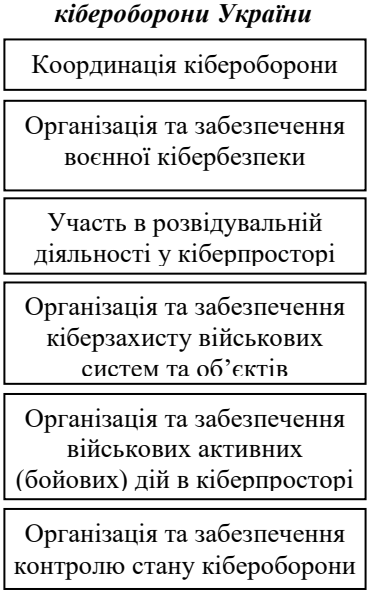

Рис. 2. Функції системи кібербезпеки Збройних Сил України в системі кібероборони держави

забезпечення підвищення спроможностей Збройних Сил України, необхідних для досягнення цілей воєнної політики Збройних Сил України у кіберпросторі;

блокування в кіберпросторі діяльності незаконних військових формувань, спрямованих на порушення діяльності Збройних Сил України та обороноздатності України;

координація Генеральним штабом Збройних Сил України діяльності добровольчих кіберформувань, що були утворені або самоорганізувалися для інформаційного або кібернетичного захисту незалежності, суверенітету та територіальної цілісності України;

реформування Збройних Сил України з метою досягнення оперативної і технічної сумісності підрозділів кібербезпеки зі збройними силами держав - членів НАТО;

визначення завдань та розробка замовлень вітчизняному оборонно-промисловому комплексу на розробку новітніх захищених інформаційно-комунікаційних та кібернетичних технологій, програмно-математичних зразків кіберозброєння, засобів кібербезпеки та кіберзахисту в інтересах Збройних Сил України та сфери кібероборони;

удосконалення воєнної політики Збройних Сил України у кіберпросторі за напрямком кібероборони;

попередження та ефективна протидія кібернетичним впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, діяльності Збройних Сил України;

забезпечення підвищення рівня соціальних гарантій військовослужбовців Збройних Сил України, задіяних у забезпеченні воєнної безпеки кіберпростору держави;

залучення наукового та науково-технічного потенціалу Збройних Сил України до розробки сучасних захищених інформаційно-комунікаційних та кібернетичних технологій, апаратного та програмного забезпечення засобів кібербезпеки та кібероборони;

нарощення можливостей Збройних Сил України за напрямом державно-приватної взаємодії у сфері кібербезпеки та кібероборони, в тому числі із залученням волонтерської допомоги;

підвищення рівня взаємодії зі складовими сектору безпеки і оборони для забезпечення воєнної безпеки кіберпростору України;

підвищення ролі та авторитету Збройних Сил України в глобальному кіберпросторі.

Визначені цілі та завдання воєнної політики Збройних Сил України у кіберпросторі відповідають сучасному стану і середньостроковому прогнозу воєнно-політичної обстановки та можуть уточнюватися з урахуванням змін безпекового середовища, умов соціально-економічного розвитку України, спроможностей сил кібероборони.

20. Збройні Сили України підтримують такий рівень обороноздатності держави у кіберпросторі, який одночасно з повним використанням можливостей щодо мирного врегулювання воєнних кіберконфліктів відповідатиме рівню воєнних кіберзагроз та водночас забезпечуватиме воєнно-стратегічний паритет в національному сегменті кіберпростору.

21. Підготовка Збройних Сил України до кібероборони орієнтується на ведення ними як оборонних, так і контрнаступальних та наступальних дій у кіберпросторі. Згідно з цим розробляються програми та плани бойової і оперативної підготовки, бойові статути і настанови Збройних Сил України.

22. Головним принципом застосування Збройних Сил України у воєнному кіберконфлікті є активна оборона з метою завдання противнику поразки та примушення його до припинення воєнних (бойових) дій в кіберпросторі. Особлива увага приділяється кібероборoні найбільш важливих стратегічних загальнодержавних автоматизованих систем управління, урядових мереж, систем зв'язку і управління зброєю, інформаційно-телекомунікаційних мереж і систем органів військового управління.

23. Під час застосування Збройних Сил України для виконання завдань за призначенням, основним завданням кібероборони є підтримка виконання військовими формуваннями поставлених завдань. Основою сил кібероборони є підрозділи Збройних Сил України, інших утворених відповідно до законів України військових формувань, а також правоохоронних органів спеціального призначення.

24. Ураховуючи наявність на території України критичної інформаційної інфраструктури, ураження якої через використання кіберпростору може призвести до виникнення надзвичайних ситуацій та катастроф, а також певну ймовірність застосування з боку противника кібернетичної зброї, Збройні Сили України готуються до дій в умовах масованого впливу кібернетичних атак та ударів на об'єкти як цивільної так і військової критичної інформаційної інфраструктури.

25. Не виключається можливість застосування воєнної сили в кіберпросторі також для локалізації та ліквідації внутрішнього збройного кіберконфлікту. Для ліквідації в кіберпросторі внутрішнього збройного кіберконфлікту залучаються Збройні Сили України, Державна служба спеціального зв'язку та захисту інформації України, інші утворені відповідно до законів України військові формування, а також правоохоронні органи спеціального призначення згідно з Конституцією і законами України.

26. Збройні Сили України мають бути також готовими відповідно до рішень Ради Безпеки ООН та міжнародних договорів України, згоду на обов'язковість яких надано Верховною Радою України, до підтримки в глобальному кіберпросторі багатонаціональних операцій з підтримання миру і безпеки під егідою уповноважених на це міжнародних організацій, а також антитерористичних операцій в кіберпросторі, реалізації в кіберпросторі інших завдань, визначених законами України.

27. Окремим напрямом діяльності Збройних Сил України є участь у підготовці національних (спеціальних) контингентів для забезпечення

участі України в організаціях і заходах, пов'язаних з міжнародною колективною безпекою та міжнародним військовим співробітництвом.

28. Збройні Сили України вважатимуть своїм воєнним противником в кіберпросторі збройні сили іншої держави (коаліції держав), дії яких кваліфікуються законами України або міжнародно-правовими актами як агресія у кіберпросторі.

Потенційним воєнним противником в кіберпросторі Україна визнаватиме збройні сили іншої держави (коаліції держав), дії або наміри яких матимуть ознаки загрози застосування в кіберпросторі воєнної сили проти України.

29. В умовах, що склалися через агресивні дії Російської Федерації в Автономній Республіці Крим та місті Севастополі та інспірування і підтримку нею сепаратистського руху у східних регіонах України, підготовка держави до кібероборони здійснюється одночасно з веденням бойових дій в кіберпросторі проти не передбачених законом кіберформувань. У ході відбиття агресії продовжується нарощування кібероборонних можливостей Збройних Сил України шляхом координації та участі у заходах з переведення національної системи зв'язку, стратегічних 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.

30. Найвищий ступінь небезпеки має загроза державному кібернетичному суверенітету України. Головною такою загрозою є ймовірність запровадження в кіберпросторі великомасштабної агресії Російської Федерації проти України.

Усунення (мінімізація) цієї загрози, забезпечення відсічі у кіберпросторі агресії Російської Федерації 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 комплексне планування дій, централізоване керівництво та координацію зусиль складових сектору безпеки і оборони, державних і громадських організацій, об'єднаних спільними цілями.

31. Збройні Сили України залишають за собою право на використання з метою відбиття агресії у кіберпросторі всіх можливих форм, способів та наявних засобів кібернетичної боротьби, а також завдання кібернетичних атак та ударів противнику на його території з дотриманням принципів і норм міжнародного права.

32. Як основу кризового реагування на воєнні загрози та недопущення ескалації воєнних конфліктів в кіберпросторі, Збройні Сили України розглядають такі основні заходи і дії:

взаємоузгоджене використання сил кібероборони держави для протидії в кіберпросторі деструктивному тиску агресора на Україну та примушення його до дотримання норм міжнародного права та власних зобов'язань;

посилення розвідувальної діяльності в інтересах підготовки та проведення Збройними Силами України воєнних кібернетичних дій та операцій у кіберпросторі;

підвищення ефективності військових кібернетичних заходів впливу на підтримку проведення антитерористичної операції в Донецькій та Луганській областях і на тимчасово окупованій території та зосередження сил і засобів для організації ефективної протидії проведенню ворожих воєнних кібернетичних дій та операцій проти України;

своєчасне повне або часткове розгортання підрозділів кібернетичної безпеки Збройних Сил України 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 Збройних Сил України;

локалізація та нейтралізація воєнного кіберконфлікту з метою недопущення його ескалації;

координація відповідно до законодавства діяльності всіх органів державної влади, органів місцевого самоврядування і громадян в інтересах ліквідації воєнного конфлікту і відсічі агресії в кіберпросторі;

координація заходів з 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.

33. Основними цілями застосування Збройними Силами України воєнної сили у кіберпросторі є:

відсіч кіберагресії з використанням усіх необхідних сил і засобів, форм і способів кібернетичної боротьби, недопущення ескалації та поширення кіберагресії у кіберпросторі України, завдання агресору поразки (втрат) 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 критичної інформаційної інфраструктури Збройних Сил України, а також демонстрація готовності і рішучості щодо

недопущення втручання іншої держави (коаліції держав) у внутрішні справи України через використання кіберпростору.

34. Збройні Сили України здійснюють стратегічний перегляд концепції кібероборони з урахуванням досвіду подолання поточної кризи, запровадження нових методів воєнного керівництва кібероборoною, які ґрунтуються на євроатлантичному досвіді. Одночасно передбачається створення результативного механізму формування і реалізації державної політики з питань забезпечення воєнної кібербезпеки, здійснення військово-політичного, адміністративного та безпосереднього військового керівництва силами кібероборони. До першочергових завдань належить створення дієвої системи управління системою кібероборони держави.

35. Основу матеріально-технічної бази системи кібероборони України становитиме Національний центр кібербезпеки, до складу якого входять головний центр захисту інформації та кібернетичної безпеки Збройних Сил України.

Складовими матеріально-технічної бази системи кібербезпеки Збройних Сил України є мережа відомчих центрів захисту інформації та кібербезпеки, можливості яких будуть нарощені з метою досягнення більш високого рівня бойового застосування у сфері кібероборони.

36. Збройні Сили України залишають за собою право на застосування воєнної сили для кібероборони, відсічі кіберагресії та відновлення кібернетичного суверенітету держави.

37. Ключовими завданнями створення умов для забезпечення кібернетичного суверенітету України є:

нарощування можливостей системи кібербезпеки Збройних Сил України до рівня, прийнятного для членства в ЄС і НАТО;

розвиток підрозділів кібербезпеки Збройних Сил України за західними стандартами та досягнення сумісності із підрозділами кібербезпеки збройних силам держав - членів НАТО.

38. Загальна чисельність підрозділів кібербезпеки Збройних Сил України та загальна кількість традиційних кіберозброєнь в умовах мирного часу повинна бути нарощена. Основні зусилля планується зосередити на підвищенні рівня бойової та оперативної підготовки підрозділів кібербезпеки для ведення дій (операцій) у кіберпросторі з одночасним радикальним оновленням якісних характеристик кіберозброєння і програмного забезпечення кібероборони та кібербезпеки, у тому числі прийняття на озброєння принципово нових зразків, розроблених на основі сучасних технологій.

39. Передбачається розширення можливостей головного центру захисту інформації та кібербезпеки Збройних Сил України для забезпечення координації і контролю діяльності органів виконавчої влади, правоохоронних органів та військових формувань у сфері національної кібероборони у мирний час, в особливий період, в умовах воєнного, надзвичайного стану і при виникненні кризових ситуацій, що загрожують національній безпеці України.

40. З метою досягнення у кіберпросторі воєнно-технічної переваги над воєнним противником мають бути посилені заходи з реалізації воєнної політики Збройних Сил України у кіберпросторі тимчасово окупованих противником територій.

VI. Суспільно-політичні, економічні та інші умови реалізації воєнної політики Збройних Сил України у кіберпросторі

41. Збройні Сили України перебувають на передових рубежах боротьби з агресивною політикою Російської Федерації у кіберпросторі, що вимагає посилення всіх воєнних, воєнно-політичних та воєнно-економічних засобів і заходів.

42. Збройний конфлікт у східних регіонах України проявив серйозні недоліки воєнно-економічної політики нашої держави у сфері кібероборони, зокрема тривале недофінансування потреб сил кібероборони, відсутність державної підтримки реформування і розвитку оборонно-промислового комплексу у сфері кібероборони. У військово-технічній сфері проблемними залишаються питання нестачі сучасних програмних та апаратних засобів кібербезпеки та кіберзброї.

43. Економічне забезпечення системи кібербезпеки Збройних Сил України здійснюватиметься шляхом формування і реалізації принципово нової єдиної воєнно-економічної, військово-промислової та військово-технічної політики, основними напрямами якої є:

визначення наукових та матеріально-технічних потреб системи кібербезпеки Збройних Сил України, забезпечення створення і модернізації програмного та апаратного забезпечення кібербезпеки та кіберозброєння для задоволення потреб безпеки і оборони відповідно до характеру і масштабів воєнних кіберзагроз, цілей, пріоритетів і завдань воєнної політики держави у кіберпросторі;

створення системи безперервного забезпечення наукових установ Збройних Сил України інформаційними, аналітичними та іншими матеріалами щодо світових досягнень у сфері науки, техніки і технологій, розвитку озброєння, військової та спеціальної техніки у сфері кібербезпеки;

забезпечення Збройних Сил України сучасними зразками програмного та апаратного забезпечення кібербезпеки;

44. Для досягнення своїх інтересів у кіберпросторі Збройні Сили України будуть нарощувати військову могутність, братимуть участь у заходах з підтримання міжнародної

безпеки у кіберпросторі, а в разі потреби будуть застосовувати воєнну силу.

VII. Шляхи досягнення цілей воєнної політики Збройних Сил України у кіберпросторі

45. Визначальним фактором зміцнення воєнної кібербезпеки України є нарощування спроможностей сил кібероборони. Нарощування спроможностей підрозділів кібербезпеки Збройних Сил України здійснюється з метою створення ефективних, мобільних, оснащених сучасним кіберозброєнням, програмним та апаратним забезпеченням сил кібероборони, здатних гарантовано забезпечити кібероборону держави.

46. Формування національних оборонних спроможностей у кіберпросторі буде здійснюватися шляхом:

удосконалення нормативно-правового забезпечення Збройних Сил України з питань кібероборони та забезпечення кібербезпеки та адаптації базових концептуальних і програмних документів з цих питань до сучасних реалій;

покращення взаємодії і координації дій Збройних Сил України з іншими органами державної влади і складовими сектору безпеки і оборони з урахуванням особливостей сучасної боротьби у кіберпросторі, у ході якої широко використовуються не лише традиційні військові операції (дії), але й різноманітні невоєнні сили та засоби;

створення та впровадження єдиної стратегії кібероборони суб'єктів сектору безпеки та оборони;

удосконалення системи кризового планування та управління у сфері кібероборони, впровадження стандартів управління військами, прийнятих у державах - членах НАТО;

удосконалення засад застосування та підготовки сил кібероборони до дій в умовах сучасної кібервійни;

упереджувального забезпечення високого рівня бойової підготовки особового складу та бойового злагодження військових підрозділів кібербезпеки із наступним виконанням ними реальних бойових завдань у кіберпросторі;

розвитку центрів кібербезпеки Збройних Сил України відповідно до стандартів НАТО;

реформування системи військової освіти і підготовки кадрів у сфері кібербезпеки, підвищення престижу військової служби, поліпшення фінансового і соціального забезпечення задіяних у сфері кібероборони військовослужбовців;

створення бойового потенціалу кібероборони, проведення модернізації, створення нових систем і уніфікації зразків кіберозброєння, програмного та апаратного забезпечення кібербезпеки;

ефективного використання двостороннього та багатостороннього співробітництва з партнерами та союзниками у військовій сфері, у тому числі шляхом отримання військової допомоги від них;

розроблення комплексного нормативного документа щодо проведення кібернетичних дій та операцій, передбачивши узгодження понятійного апарату, визначення завдань і повноважень підрозділів кібербезпеки Збройних Сил України у мирний час, в особливий період, в умовах воєнного, надзвичайного стану і при виникненні кризових ситуацій, що загрожують національній безпеці України.

47. Чисельність і структура підрозділів кібербезпеки Збройних Сил України та їх складових визначатиметься з урахуванням стану безпекового середовища у кіберпросторі та потреб кібероборони України, необхідності відсічі кіберагресії Російської Федерації і запобігання очікуваним конфліктам у кіберпросторі, а також фінансово-економічних можливостей держави. Підрозділи кібербезпеки Збройних Сил України намагатимуться забезпечити спроможності, які передусім визначають їх здатність до застосування у кіберпросторі воєнної сили та відбиття кіберагресії.

48. Збройні Сили України у взаємодії з іншими складовими сектору безпеки і оборони дотримуватимуться прийнятих у державах - членах ЄС і НАТО стандартів щодо діяльності і розподілу функцій та основних завдань у кіберпросторі.

Головна роль у забезпеченні воєнної безпеки України у кіберпросторі належить Збройним Силам України [2].

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

50. Збройні Сили України будуть поглиблювати співпрацю з НАТО у сфері кібероборони для досягнення за цим напрямом критеріїв, необхідних для набуття членства у цій організації.

51. Пріоритетним завданням поглиблення співпраці з НАТО у сфері кібероборони є досягнення до 2020 року повної сумісності підрозділів кібербезпеки Збройних Сил України з відповідними силами держав - членів НАТО.

52. Поглиблення співпраці з НАТО передбачає:

розвиток багатосторонніх відносин у сфері кібероборони у рамках сучасних механізмів НАТО, зокрема в рамках Спільної з ЄС політики безпеки і оборони, Хартії про особливе партнерство між Україною та Організацією Північно-Атлантичного договору, програми "Партнерство заради миру", Концепції

оперативних можливостей НАТО (КОМ/ОСС), Процесу планування та оцінки Сил НАТО (ППОС/PARP) і середземноморського діалогу;

розвиток двосторонніх відносин Збройних Сил України зі збройними силами держав - членів НАТО у сфері кібероборони;

надійне виконання взятих на себе партнерських зобов'язань, взяття на себе пропорційної частки відповідальності у спільних з НАТО кібернетичних операціях;

забезпечення підготовленості особового складу, технічної сумісності кіберозброєння, а також оперативної сумісності підрозділів кібербезпеки Збройних Сил України і держав - членів НАТО в рамках Програми перевірки та зворотного зв'язку Концепції оперативних можливостей НАТО (КОМ/ОСС).

53. Поглиблення кооперації та співробітництва з НАТО і ЄС у сфері кібероборони в частині протидії у кіберпросторі агресивній політиці Російської Федерації, міжнародним терористичним, релігійно-екстремістським та злочинним організаціям, передбачає залучення допомоги кібероборонних структур НАТО і ЄС, а також держав - членів НАТО і ЄС з питань створення та розвитку військових центрів та підрозділів кібербезпеки, залучення для ресурсного забезпечення таких заходів коштів трастових фондів НАТО, отримання доступу до інформаційних мереж держав - членів НАТО і ЄС з кібероборони.

54. Поглиблення співпраці з НАТО, надійне виконання взятих на себе партнерських зобов'язань, трансформація й адаптація документів оборонного планування, оперативного і бойового управління та досягнення повної сумісності підрозділів кібербезпеки Збройних Сил України з відповідними підрозділами держав - членів НАТО сприятимуть досягненню необхідних критеріїв для набуття Україною повноправного членства в НАТО.

55. Розвиток технічних спроможностей підрозділів кібербезпеки Збройних Сил України буде здійснюватися шляхом впровадження комплексних технічних рішень та заходів з розвідувальної діяльності у кіберпросторі, кіберзахисту військових систем та об'єктів та забезпечення військових активних (бойових) дій у кіберпросторі.

VIII. Розвиток системи кібербезпеки Збройних Сил України

56. В інтересах забезпечення зниження ризиків у сфері воєнної безпеки держави у кіберпросторі створюється інтегрована система забезпечення кібербезпеки Збройних Сил України.

57. У короткостроковій перспективі головні зусилля будуть спрямовані на створення та забезпечення функціонування підрозділів кібербезпеки Збройних Сил України, насамперед на:

запровадження з урахуванням досвіду збройного конфлікту в східних регіонах України нових методів керівництва кібероборо ною, які ґрунтуються на стандартах НАТО та відповідають критерію високої ефективності за прийнятних витрат;

удосконалення нормативно-правового забезпечення з питань воєнної безпеки у кіберпросторі і кібероборони, розроблення ефективного механізму реагування на кризові ситуації у кіберпросторі, розвиток системи управління в кібернетичних бойових діях і операціях;

досягнення оперативної сумісності складових системи кібербезпеки Збройних Сил України, планомірний перехід до стандартів НАТО в організації, озброєнні та підготовці військ (сил), а також у системі оперативного прийняття рішень;

створення нових систем і модернізацію зразків кіберозброєння, програмного та апаратного забезпечення кібебезпеки і кібероборони.

Висновки й перспективи подальших досліджень

Стратегія забезпечення кібернетичної безпеки Збройних Сил України є основою для підготовки та прийняття воєнно-політичних, воєнно-стратегічних, воєнно-економічних і військово-технічних рішень у сфері реформування і розвитку Збройних Сил України, розроблення відповідних концепцій та програм.

Реалізація положень Стратегії забезпечення кібернетичної безпеки Збройних Сил України забезпечується Радою національної безпеки і оборони України, Кабінетом Міністрів України, іншими органами державної влади відповідно до повноважень, визначених Конституцією та законами України.

Положення Стратегії забезпечення кібернетичної безпеки Збройних Сил України коригуватимуться в установленому порядку з урахуванням змін воєнно-політичної обстановки у світі, характеру загрози застосування воєнної сили у кіберпросторі, умов соціально-економічного розвитку України.

Література

1. Указ Президента України „Про Стратегію національної безпеки України" № 287/2015 від 26 травня 2015 року [Електронний ресурс].– Режим доступу : http://zakon.rada.gov.ua/287/2015; **2. Закон** України „Про Збройні Сили України" від 06.12.1991 № 1934-XII (Із змінами, поточна редакція – Редакція від 21.06.2014) [Електронний ресурс].– Режим доступу : http://zakon.rada.gov.ua/laws/show/1934-12.

СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСТНОСТИ ВООРУЖЕННЫХ СИЛ УКРАИНЫ

[1]Александр Александрович Черноног
[2]Евгений Александрович Живило
[1]Вадим Витальевич Машталир (канд. истор. наук)

[1]Генеральный штаб Вооруженных Сил Украины, Киев, Украина
[2]Военный институт телекоммуникаций и информатизации, Киев, Украина

Стратегия военной безопасности киберпространства Украины (далее – Стратегия) основывается на результатах анализа и прогнозирования военно-политической обстановки, принципах оборонной достаточности, высокой готовности к обороне, системности оборонного планирования, а также определенные Верховым Советом Украины принципы внутренней и внешней политики. Основные положения Стратегии являются производными от Военной доктрины Украины и Стратегии национальной безопасности Украины, развивают их положения по направлениям обеспечения военной безопасности киберпространства Украины и направлены на противодействие агрессии со стороны Российской Федерации в киберпространстве. Именно поэтому выполнение указанных выше условий является необходимым для обретения членства в Европейском Союзе и Организации Североатлантического договора, обеспечения равноправного, взаимовыгодного сотрудничества по направлению кибербезопасности (кибероборонь) в военной, военно-экономической и военно-технической сфере со всеми заинтересованными государствами-партнерами.

Ключевые слова: *военный киберконфликт; кибервойна; кибероборона.*

THE STRATEGY FOR ENSURING THE CYBER SECURITY OF THE ARMED FORCES OF UKRAINE

[1]Oleksandr O. Chernonoh
[2]Yevhen O. Zhyvylo
[1]Vadym V. Mashtalir (Candidate of Historical Sciences)

[1]The General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine
[2]Military Institute of Telecommunications and Informatization, Kyiv, Ukraine

The military security strategy of Ukraine cyberspace (hereinafter – the Strategy) is based on the results of the military-political situation analysis and forecasting, the defense sufficiency principles, high availability to defense, system defense planning, as well as defined of the Supreme Council of Ukraine the domestic and foreign policy principles. The main provisions of the Strategy are derived from the Military doctrine of Ukraine and the national security Strategy of Ukraine, and develop their position in the areas of ensuring military security of the Ukraine cyberspace and are aimed at countering aggression by the Russian Federation in cyberspace. That is why the fulfilment of the above conditions is necessary for gaining membership in the European Union and the North Atlantic Treaty Organization, ensuring equitable and mutually beneficial cooperation in the field of cyber security (cyber defense) in the military, military-economic and military-technical cooperation with all interested States-partners.

Keywords: *military cyber warriors; cyber warfare; cyber defense.*

References

1. The decree of the President of Ukraine "On Strategy of national security of Ukraine", available at: http://zakon.rada.gov.ua/287/2015; **2. The law** of Ukraine "About Armed Forces of Ukraine", available at: http://zakon.rada.gov.ua/laws/show/1934-12.

Отримано: 03.11.2015 р.