Живило Є.О. (ВІТІ)
Черноног О.О. (ГШ ЗСУ)
к.і.н. Машталір В.В. (ГШ ЗСУ)

СТРАТЕГІЯ ВОЄННОЇ БЕЗПЕКИ КІБЕРПРОСТОРУ 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. Розробка, впровадження та виконання теоретичних засад у зазначеній галузі спрямовано на попередження та усунення загроз воєнній безпеці України у кіберпросторі.

Живило Є.О., Черноног О.О., Машталір В.В. Стратегия военной безопасности кибернетического пространства Украины. *Угрозы военной безопасности Украины в киберпространстве в случае их реализации могут способствовать изменению конституционного строя Украины , дальнейшей оккупации Украины или ее отдельных территорий , установление прямого или опосредованного контроля над Украиной и потери ею государственного суверенитета и территориальной целостности. Разработка и выполнение теоретических основ в указанной области направлено на предупреждение и устранение угроз военной безопасности Украины в киберпространстве.*

O. Chernonog, E. Zhivilo, V. Mashtalir Ukraine's military security cyberspace strategy. *The threats of military security of Ukraine in cyberspace in case of their implementation can contribute to changing the constitutional order of Ukraine and further occupation of Ukraine or its separate territories , the establishment of direct or indirect control over Ukraine and its loss of the state sovereignty and territorial integrity. Development and implementation of theoretical foundations in this region aimed at preventing and eliminating threats to the military security of Ukraine in cyberspace.*

Ключеві слова: *кібервійна, збройний кіберконфлікт, кібероборона.*

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

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

Основні положення.

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

воєнна політика України у кіберпросторі – діяльність суб'єктів забезпечення КБ, пов'язана із запобіганням воєнним кіберконфліктам у кіберпросторі, організацією та здійсненням підготовки Збройних Сил України (далі – ЗС України), Державної служби спеціального зв'язку та захисту інформації України (далі – ДССЗЗІ України), утворених відповідно до законів України інших військових формувань та правоохоронних органів (Далі – ІВФ та ПрО) спеціального призначення до кібероборони (далі – КО) 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 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);

КО – 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 КО –ЗС України, ДССЗЗІ України, утворені відповідно до законів України ІВФ та ПрО та розвідувальні органи, в частині залучення їх до виконання завдань з КО держави;

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

1.2. Безпекове середовище у контексті воєнної безпеки України у кіберпросторі

Безпекове середовище у кіберпросторі довкола України складне та динамічне.

Формування та розвиток безпекового середовища у світі відбувається під впливом таких головних тенденцій:

посилення суперечностей щодо поділу у кіберпросторі сфер впливу між світовими центрами сили, збільшення їх агресивності, непоступливості, прагнення порушити на свою користь воєнно-стратегічну рівновагу, зокрема загострення протистояння між США і ЄС та РФ і КНР;

загострення безпекової ситуації в кіберпросторі країн Близького Сходу та Північної Африки, активізація релігійного екстремізму та поширення ідей радикального ісламу в кіберпросторі країн Центральної Азії, суперечності між азіатсько-тихоокеанськими державами щодо належності острівних зон;

перенесення ваги у воєнних кіберконфліктах на асиметричне застосування воєнної сили не передбаченими законом збройними формуваннями, зміщення акцентів у веденні воєнних кіберконфліктів на комплексне використання воєнних і невоєнних інструментів (економічних, політичних, інформаційно-психологічних тощо), що принципово змінює характер кібернетичної боротьби;

розширення масштабів кібертероризму та кіберзлочинності.

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;

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.

Актуальними воєнними загрозами у кіберпросторі для України є:

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

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

активізація спеціальними службами РФ 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 РФ на кіберсуверенітет України.

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

повномасштабна кіберагресія РФ проти України з рішучими воєнно-політичними цілями;

окрема спеціальна кібернетична операція РФ 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 РФ 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;

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. На спроможності 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 КО та неефективне використання наявних ресурсів;

недостатній рівень готовності ЗС України, ДССЗЗІ України, утворених відповідно до законів України ІВФ та ПрО спеціального призначення до ведення кібернетичної боротьби;

низька ефективність державних органів, що проводять 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 КБ і КО;

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

Воєнно-економічне та військово-технічне забезпечення воєнної безпеки держави безпосередньо залежить від оборонно-промислового комплексу (Далі- ОПК) країни, основними проблемами функціонування якого є:

низька ефективність реалізації військово-технічної політики і політики військово-технічного співробітництва у сфері КО;

відсутність державного регулювання та недостатня підтримка стратегічно важливих для КО держави наукових установ і організацій, діяльність яких спрямована на задоволення потреб ЗС України, ДССЗЗІ України та інших утворених відповідно до законів України

військових формувань, а також правоохоронних органів спеціального призначення, в кіберозброєнні, програмному та апаратному забезпеченні КБ та КО;

відсутність підприємств ОПК та військових наукових установ, спрямованих на створення та дослідження сучасних захищених інформаційно-комунікаційних та кібернетичних технологій;

критичний стан забезпечення підприємств ОПК та військових наукових установ висококваліфікованими ІТ-спеціалістами.

1.3. Цілі та основні завдання воєнної політики України у кіберпросторі

Україна прагне підтримувати дружні відносини з усіма державами світу на основі міжнародних договорів у сфері КО (КБ), укладених на принципах рівноправності, невтручання у внутрішні справи, взаємоповаги до кібернетичного суверенітету.

Основними цілями воєнної політики України у кіберпросторі є:

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

участь України у реалізації спільної політики безпеки і оборони кіберпростору ЄС;

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.

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

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

створення єдиної системи КО з відповідною інфраструктурою отримання та обробки даних в режимі часу, наближеного до реального (рисунок 1);

створення національної системи КБ України, інтеграція спроможностей її складових для своєчасного і ефективного реагування на наявні та потенційні кіберзагрози сектору безпеки держави;

удосконалення системи забезпечення воєнної безпеки кіберпростору держави, інтеграція спроможностей її складових для своєчасного і ефективного реагування на наявні та потенційні кіберзагрози сектору оборони держави;

забезпечення підвищення спроможностей сил КО, необхідних для досягнення цілей воєнної політики України у кіберпросторі;

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

координація військовим командуванням діяльності добровольчих кіберформувань, що були утворені або самоорганізувалися для інформаційного або кібернетичного захисту незалежності, суверенітету та територіальної цілісності України;

реформування ЗС України з метою досягнення оперативної і технічної сумісності підрозділів КБ зі збройними силами держав – членів НАТО;

підвищення спроможностей вітчизняного ОПК за рахунок впровадження новітніх захищених інформаційно-комунікаційних та кібернетичних технологій, створення максимально можливих замкнених циклів розроблення і виробництва найважливіших програмно-математичних зразків кіберозброєння, засобів КБ та кіберзахисту, використання можливостей військово-технічного співробітництва з державами - стратегічними партнерами України;

удосконалення воєнної політики України у кіберпросторі за напрямком КО;

залучення наукового та науково-технічного потенціалу країни до розробки сучасних захищених інформаційно-комунікаційних та кібернетичних технологій, апаратного (мікропроцесорного) та програмного забезпечення засобів КБ та КО;

нарощення можливостей державно-приватної взаємодії у сфері КБ та КО, в тому числі із залученням волонтерської допомоги;

підвищення рівня координованості складових сектору безпеки і оборони та вдосконалення механізмів їх консолідованого розвитку та посилення відповідних оперативних спроможностей для забезпечення воєнної безпеки кіберпростору України.

Визначені цілі та завдання воєнної політики 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 КО. Підготовка КО України за змістом, спрямованістю і масштабом здійснюється відповідно до Закону України "Про оборону України". Підготовка сил КО України орієнтується на ведення ними як оборонних, так і контрнаступальних та наступальних дій у кіберпросторі. Головним принципом застосування сил КО у воєнному конфлікті в кіберпросторі є активна оборона з метою завдання противнику поразки та примушення його до припинення воєнних (бойових) дій. Особлива увага приділяється КО найбільш важливих стратегічних

Рисунок 1 – Воєнна політика України у кіберпросторі

загальнодержавних автоматизованих систем управління, урядових мереж, систем зв'язку і управління зброєю, інформаційно-телекомунікаційних мереж військового управління.

Під час застосування ЗС України, основним завданням КО є підтримка виконання військовими формуваннями поставлених завдань. Основою сил КО є підрозділи ЗС України, утворених відповідно до законів України ІВФ та ПрО спеціального призначення.

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, сили безпеки і оборони готуються до дій в умовах масованого впливу кібернетичних атак та ударів на об'єкти як цивільної так і військової критичної інформаційної інфраструктури. Україна не виключає можливості застосування воєнної сили в кіберпросторі також для локалізації та ліквідації внутрішнього збройного кіберконфлікту. Для ліквідації в кіберпросторі внутрішнього збройного кіберконфлікту Україна залучає ЗС України, ДССЗЗІ України, Державну спеціальну службу транспорту, утворені відповідно до законів України ІВФ та ПрО спеціального призначення згідно з Конституцією і законами України. ЗС України, утворені відповідно до законів України ІВФ та ПрО спеціального призначення 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. Окремим напрямом діяльності сил КО 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. Україна вважатиме своїм воєнним противником в кіберпросторі іншу державу (коаліцію держав), дії якої (яких) кваліфікуються законами України або міжнародно-правовими актами як агресія у кіберпросторі. Потенційним воєнним противником в кіберпросторі Україна визнаватиме державу (коаліцію держав), дії або наміри якої (яких) матимуть ознаки загрози застосування в кіберпросторі воєнної сили проти України. В умовах, що склалися через агресивні дії РФ в Автономній Республіці Крим та місті Севастополі та інспірування і підтримку нею сепаратистського руху у східних регіонах України, підготовка держави до КО здійснюється одночасно з веденням бойових дій в кіберпросторі проти не передбачених законом кіберформувань. У ході відбиття агресії продовжується нарощування КО можливостей держави шляхом 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. Найвищий ступінь небезпеки має загроза державному кібернетичному суверенітету України. Головною такою загрозою є ймовірність запровадження в кіберпросторі великомасштабної агресії РФ проти України. Усунення (мінімізація) цієї загрози, забезпечення відсічі у кіберпросторі 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 комплексне планування дій, централізоване керівництво та координацію зусиль складових сектору безпеки і оборони, державних і громадських організацій, об'єднаних спільними цілями. Україна залишає 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. Як основу кризового реагування на воєнні загрози та недопущення ескалації воєнних конфліктів 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;

посилення розвідувальної діяльності в інтересах підготовки та проведення Україною воєнних кібернетичних дій та операцій у кіберпросторі;

підвищення ефективності 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 кібернетичних дій та операцій проти України;

своєчасне повне або часткове розгортання підрозділів КБ ЗС України, інших утворених відповідно до законів України військових формувань, правоохоронних органів спеціального призначення 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;

координація відповідно до законодавства діяльності всіх органів державної влади, органів 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.

Основними цілями застосування Україною 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 важливої державної критичної інформаційної інфраструктури, а також демонстрація готовності і рішучості щодо недопущення втручання іншої держави (коаліції держав) у внутрішні справи України через використання кіберпростору. Україна здійснює стратегічний перегляд концепції КО з урахуванням досвіду подолання поточної кризи, запровадження нових методів воєнного керівництва КО, які ґрунтуються на євроатлантичному досвіді та відповідають єдиному критерію – висока ефективність за прийнятних витрат. Одночасно передбачається створення результативного механізму формування і реалізації державної політики з питань забезпечення воєнної КБ, здійснення військово-політичного, адміністративного та безпосереднього військового керівництва силами КО. До першочергових завдань належить створення дієвої системи управління системою КО держави.

Основу матеріально-технічної бази системи КО України становитиме Національний центр КБ, до складу якого входять головний центр захисту інформації та кібернетичної безпеки ЗС України, CERT-UA ДССЗЗІ України, центр протидії кібертероризму Служби безпеки України, центр протидії кіберзлочинності Міністерства внутрішніх справ України та підрозділи розвідувальних органів України. 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, які будуть реформовані з метою досягнення більш високого рівня взаємодії у сфері КО.

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

Ключовими завданнями створення умов для забезпечення кібернетичного суверенітету України є:

комплексне 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 бойової та оперативної підготовки 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, розроблених на основі сучасних технологій. 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. Об’єднаний комітет з питань розвідувальної діяльності при Президентові України забезпечуватиме координацію діяльності розвідувальних органів України за напрямом кіберрозвідки.

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

1.4. Суспільно-політичні, економічні та інші умови реалізації воєнної політики України у кіберпросторі

Україна перебуває на передових рубежах боротьби з агресивною політикою РФ у кіберпросторі, що вимагає посилення всіх політичних, воєнних, дипломатичних та економічних засобів і заходів. Збройний конфлікт у східних регіонах України проявив серйозні недоліки воєнно-економічної політики нашої держави у сфері КО, зокрема тривале недофінансування потреб сил КО, відсутність державної підтримки реформування і розвитку ОПК у сфері КО. У військово-технічній сфері проблемними залишаються питання нестачі сучасних програмних та апаратних засобів КБ та кіберзброї. Економічне забезпечення воєнної безпеки кіберпростору України здійснюватиметься шляхом формування і реалізації принципово нової єдиної воєнно-економічної, військово-промислової та військово-технічної політики, основними напрямами якої є:

визначення на державному рівні довгострокових наукових та матеріально-технічних потреб КО, забезпечення створення і модернізації програмного та апаратного забезпечення КБ та кіберозброєння для задоволення потреб безпеки і оборони відповідно до характеру і масштабів воєнних кіберзагроз, цілей, пріоритетів і завдань воєнної політики держави у кіберпросторі;

упровадження системи стратегічного планування розвитку ОПК у сфері КО, взаємопов’язаного з 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 організаційних, технічних, економічних, правових та інших заходів, спрямованих на зниження залежності України від критичного імпорту програмного

та апаратного забезпечення воєнної сфери, підвищення ефективності міжнародного науково-технічного співробітництва, насамперед з державами – членами ЄС та НАТО;

створення системи безперервного забезпечення наукових установ і виробничих підприємств ОПК інформаційними, аналітичними та іншими матеріалами щодо світових досягнень у сфері науки, техніки і технологій, розвитку озброєння, військової та спеціальної техніки у сфері КБ;

створення системи державного замовлення на підготовку робітничих, технічних та інженерних кадрів для задоволення потреб ОПК у сфері КО, сприятливих умов для ефективного функціонування і розвитку науково-дослідних, технологічних та проектних установ, конструкторських бюро у сфері КБ та КО;

забезпечення сучасними зразками програмного та апаратного забезпечення КБ, зокрема їх розроблення та виробництво силами вітчизняного ОПК, у тому числі за закордонними ліцензіями, розроблення і виробництво разом з іноземними партнерами, імпорт програмного та апаратного забезпечення КБ, розроблення і виробництво яких в Україні недоцільне або технологічно неможливе. Для досягнення своїх інтересів у кіберпросторі Україна розвиватиме національну економіку, нарощуватиме військову могутність, братиме участь у підтриманні міжнародної безпеки, використовуватиме всі можливі мирні шляхи для вирішення конфліктів і кризових ситуацій у кіберпросторі, а в разі потреби застосовуватиме воєнну силу.

1.5. Шляхи 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, мобільних, оснащених сучасним кіберозброєнням, програмним та апаратним забезпеченням сил КО, здатних гарантовано забезпечити КО держави.

Формування національних оборонних спроможностей у кіберпросторі буде здійснюватися шляхом:

удосконалення законодавства з питань КО України, належного унормування діяльності у воєнній сфері та адаптації базових законодавчих, концептуальних і програмних документів з питань КО до сучасних реалій;

покращення взаємодії і координації дій органів державної влади і складових 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 КО суб'єктів сектору безпеки та оборони, визначення єдиного органу для координації та контролю її реалізації;

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

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

розвитку в рамках створення перспективної системи управління сектором безпеки і оборони системи управління КО України для забезпечення надійного управління військами (силами) КО в особливий період без перебудови та проведення масштабних організаційних заходів;

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

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, підвищення престижу військової служби, поліпшення фінансового і соціального забезпечення задіяних у сфері КО військовослужбовців та працівників правоохоронних органів;

створення бойового потенціалу КО, 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, у тому числі шляхом отримання військової допомоги від них;

розроблення комплексного нормативного документа щодо проведення кібернетичних дій та операцій, передбачивши узгодження понятійного апарату, визначення 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 середовища у кіберпросторі та потреб КО України, необхідності відсічі кіберагресії РФ і запобігання очікуваним конфліктам у кіберпросторі, а також фінансово-економічних можливостей держави. Сили КО намагатимуться забезпечити спроможності, які передусім визначають їх здатність до захисту України у кіберпросторі та відбиття кіберагресії. ЗС 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.

Забезпечення воєнної безпеки України у кіберпросторі належить ЗС України.

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 задоволення потреб безпеки і оборони відповідно до цілей, пріоритетів і завдань воєнної політики держави у кіберпросторі.

ЗС України взаємодіятимуть з іншими складовими сектору безпеки і оборони у виконанні визначених для них завдань з КО та уникатимуть 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, надання військової допомоги іншим країнам, а також братимуть участь у міжнародному співробітництві у сфері КО, спільних кібернетичних операціях з НАТО. Для розв’язання завдань із забезпечення воєнної безпеки України у кіберпросторі сили оборони та їх складові

будуть взаємодіяти та координувати діяльність 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. Відмова України від одного з найпотужніших у світі ядерного арсеналу дає їй право 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, утворення у кіберпросторі військових союзів та отримання закордонної воєнної допомоги. Зовнішні гарантії КБ України створюватимуться 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 (шляхом участі у застосуванні механізмів колективної безпеки кіберпростору). Водночас у середньостроковій перспективі Україна використовуватиме насамперед власні можливості та залишає за собою право обирати спосіб гарантування державного кібернетичного суверенітету. З відмовою від політики позаблоковості Україна вибудовує нові підходи до забезпечення національної КО, надаватиме пріоритет участі в удосконаленні та розвитку євроатлантичної та європейської систем колективної безпеки кіберпростору. Для цього Україна буде інтегруватися до європейського кіберпростору з метою набуття членства в ЄС, а також поглиблювати співпрацю з НАТО у сфері КО для досягнення за цим напрямом критеріїв, необхідних для набуття членства у цій організації. 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.

Поглиблення співпраці з НАТО передбачає:

розвиток багатосторонніх відносин у сфері КО 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 України з державами – членами НАТО у сфері КО;

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 КБ ЗС України і держав – членів НАТО в рамках Програми перевірки та зворотного зв'язку Концепції оперативних можливостей НАТО (КОМ/ОСС). Поглиблення кооперації та співробітництва з НАТО і ЄС у сфері КО в частині протидії у кіберпросторі агресивній політиці Російської Федерації, міжнародним терористичним, релігійно-екстремістським та злочинним організаціям, передбачає залучення допомоги КО структур НАТО і ЄС, а також держав – членів НАТО і ЄС з питань створення та розвитку військових центрів та підрозділів КБ, залучення для ресурсного забезпечення таких заходів коштів трастових фондів НАТО, отримання доступу до інформаційних мереж держав – членів НАТО і ЄС з КО. 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 сил КО України з відповідними силами держав – членів НАТО сприятимуть досягненню необхідних критеріїв для набуття Україною повноправного членства в НАТО.

1.6. Фінансування потреб КО

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

Пріоритетними напрямами фінансування потреб КО є:

проведення інтенсивної бойової підготовки 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, створення, розширення номенклатури та обсягів випуску наукоємної конкурентоспроможної продукції в секторі КО;

реалізація соціальних і правових гарантій задійяних у сфері КО військовослужбовців та працівників правоохоронних органів.

1.7. 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;

перегляд концепції бюджетного планування і системи забезпечення ресурсами, радикальне покращення забезпечення ведення бойових дій і операцій у кіберпросторі.

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.

Висновок. Стратегія воєнної безпеки кіберпростору України є основою для підготовки та прийняття воєнно-політичних, воєнно-стратегічних, воєнно-економічних і військово-технічних рішень у сфері КО, розроблення відповідних концепцій та програм. Реалізація положень Стратегії забезпечується Президентом України, Радою національної безпеки і оборони України, Кабінетом Міністрів України, іншими органами державної влади відповідно до повноважень, визначених Конституцією та законами України. 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. Положення Стратегії коригуватимуться в установленому порядку з урахуванням змін воєнно-політичної обстановки у світі, характеру загрози застосування воєнної сили у кіберпросторі, умов соціально-економічного розвитку України.