DOI:**10.33099/2311-7249/2023-46-1-32-40**

УДК: 351.865

Євген Олександрович Живило *(кандидат наук з державного управління)*[1]
Валентин Миколайович Докіль[2]

[1] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

МОДЕЛЬ МЕТОДИКИ ОЦІНЮВАННЯ СПРОМОЖНОСТЕЙ ВІЙСЬК ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ ЩОДО ВИКОНАННЯ ЗАВДАНЬ З ВІДБИТТЯ ВОЄННОЇ АГРЕСІЇ В КІБЕРПРОСТОРІ

Інновації керували військовою стратегією з часу появи людства. Винахід пороху, органної гармати та двигуна внутрішнього згоряння мали величезний вплив не лише на тенденції розвитку військової стратегії, а й на всю хронологію світової історії. Не стало винятком і XX століття. Інтернет, що розвивається, продовжує розширювати можливості інформаційних технологій. Але, як й інші великі винаходи, його можливості часто використовуються задля досягнення негативних цілей та результатів. Сьогодні, в ході повномасштабного російського вторгнення в Україну, наше суспільство і держава зіткнулися з новою загрозою, що має значний військовий і геополітичний потенціал. За короткий проміжок часу, вразливості системи управління технологічними процесами, що мають єдині системи електронних комунікацій, перетворились на ефективний імовірний набір реальних і потенційних загроз національній безпеці України у кіберпросторі. Зазначені загрози здатні порушити штатний режим функціонування комунікаційних систем спеціальних користувачів, у тому числі зрив та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами. За таких умов, ключову роль у підтриманні сталого функціонування таких систем у складі сил безпеки та оборони України відіграють Війська зв'язку та кібербезпеки Збройних Сил України. Так, порядок організації проведення оцінювання спроможностей у Збройних Силах України, як елемент планування на основі спроможностей, здійснюється з урахуванням підходів, прийнятих у держав-членів НАТО. Зазначена сфера застосування охоплює питання методології процесу організації проведення оцінювання спроможностей, визначення учасників цього процесу, процедури і порядку його проведення, взаємозв'язку з іншими процесами, використання результатів цієї діяльності.

Наразі Законом України «Про національну безпеку України» внормовано питання оцінювання спроможностей, в рамках якого поставлено завдання до розроблення відповідних методик щодо прогнозування, виявлення та надання оцінки загрозам національної безпеки держави в кіберпросторі та через кіберпростір. Окремо слід підкреслити необхідність визначення порядку організації проведення оцінювання спроможностей, розроблення методики оцінювання спроможностей військ зв'язку та кібербезпеки Збройних Сил України із виконання завдань з відбиття воєнної агресії в кіберпросторі.

Ключові слова: *цифрове суспільство; інформаційно-комунікаційні системи; оцінювання спроможностей; кіберзагрози; кібербезпека; кіберпростір.*

Вступ

Постановка проблеми. Оцінювання спроможностей – це процес, який є складовою частиною планування на основі спроможностей. Планування на основі спроможностей – процес, який здійснюється періодично під час оборонного огляду та циклів середньострокового планування і зосереджується на визначенні перспективних спроможностей, структури і складу Збройних Сил України (далі – ЗС України) на довгострокову перспективу з урахуванням майбутнього безпекового та оперативного середовища і встановлених ресурсних обмежень.

Доволі часто, в ході здійснення планування на основі спроможностей низка органів військового управління (далі – ОВУ) проводить формальне відпрацювання зазначеного заходу. Мають місце: не узгоджені із завданнями пропозиції, що визначені Указом Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021 і Наказом Міністерства оборони України «Про затвердження Основних напрямів підготовки до відбиття воєнної агресії у кіберпросторі (підготовки та ведення кібероборони) у системі Міністерства оборони України» від 01.04.2019 р. № 10/ДСК; неузгодженість пропозицій відповідно до

положень Єдиного переліку (каталогу) спроможностей Міністерства оборони України та ЗС України. При цьому виконавцями зазначених пропозицій не розкривається, а нерідко і не включається інформація про критерії оцінювання та їх результати, власне, очікувані результати у процесі життєвого циклу, джерела та обсяг фінансування (виділення інших ресурсів) взагалі не обґрунтовується.

Враховуючи зазначене, постає доволі серйозна проблематика щодо визначення складових елементів самих спроможностей Військ зв'язку та кібербезпеки ЗС України, в частині виконання завдань з кібербезпеки і, як похідна, розроблення методик їх оцінювання під час виконання завдань з відбиття воєнної агресії в кіберпросторі (далі – КП).

Аналіз останніх досліджень і публікацій. В умовах глобалізації світу окрема держава практично не може протистояти можливим кіберзагрозам (далі – КЗаг) сучасності без інформаційного обміну з іншими. Нормативно-правовою базою (далі – НПБ) України [1; 2; 3; 4] значна увага надається співпраці з ЄС, НАТО та іншими міжнародними суб'єктами із забезпечення безпеки КП та спільного захисту від КЗаг, в тому числі, у військовій та оборонній сферах. Дуже важливим індикатором готовності систем кібербезпеки (далі – КБ) та кібероборони (далі – КО) держав-партнерів є досягнення визначеного рівня їх інтероперабельності. Але, в ході проведення чисельних консультацій, практичних навчань, науково-практичних конференцій, семінарів і тренінгів, що займають значне місце серед різноманітних заходів програм взаємодії між Україною – НАТО та США у сфері КБ, були виявлені суперечності базового термінологічного апарату, що, як мінімум, знижує ефективність заходів та не дозволить в майбутньому ефективно виконувати завдання передбачені [2; 5; 6] та рядом інших домовленостей. Аналіз існуючих законів України та інших нормативно-правових актів України [2; 5; 6], ЄС, НАТО, провідних країн світу, зокрема США, свідчить про дефініційну, термінологічну та нормативно-правову невизначеність або/та розбіжність об'єктно-предметної області декількох десятків понять, що складають базовий термінологічний набір терміносистеми сфери КБ та КО, зокрема таких як «кібербезпека», «кіберзахист», «кіберзброя», «кібероборона», «кібертероризм», «кіберпростір» тощо [7]. Так, США, Міжнародна спілка з телекомунікацій (ITU), Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) розглядають КП як сферу діяльності складних технічних систем, а в Україні – складних соціотехнічних систем [8; 9; 10; 11].

В цілому, розвиток та широке впровадження систем і комплексів зв'язку з використанням інноваційних інформаційних та комунікаційних технологій в системах військового призначення відбувається у відповідності до міжнародних правил ведення кібервійн на зразок Женевської конвенції. Водночас, основні принципи формування систем КБ та КО провідних країн світу науково обґрунтовані законодавчо, врегульовані НПБ та дефініційно-термінологічно визначені на державному рівні. За таких умов трансформування НПБ відбувається під впливом постійної мілітарізації національних сегментів КП з урахуванням критеріїв (індикаторів) загроз у сфері КБ та КО провідних держав, рівня готовності систем та набуття відповідних спроможностей тощо.

Сьогодні, для організації та проведення оцінювання спроможностей, в ЗС України використовуються чинні національні стандарти, методики та керівництва, також – міжнародні практики, описані відповідними стандартами і публікаціями НАТО. Зокрема, для проведення оцінювання спроможностей організаційно-штатними структурами (далі – ОШС) використовуються такі документи:

Рекомендації з оборонного планування на основі спроможностей в Міністерстві оборони України (далі – МО України) та ЗС України, затверджені Міністром оборони України 12.06.2017 р.;

Військовий стандарт ВСТ 01.004.005-2017(01) «Воєнна політика, безпека та стратегічне планування. Стратегічне планування розвитку спроможностей Збройних Сил України. Абревіатури»;

Військовий стандарт ВСТ 01.004.006-2017(01) «Воєнна політика, безпека та стратегічне планування. Стратегічне планування розвитку спроможностей ЗС України. Терміни та визначення»;

Стандарт НАТО (Allied Forces Standard) AFS Vol. I (General force standards) – загальні вимоги до спроможностей військ (сил);

Стандарт НАТО AFS Vol. II (Standards for Land Forces) – вимоги до спроможностей сухопутних військ;

Стандарт НАТО AFS Vol. III (Standards for Air Forces) – вимоги до спроможностей повітряних сил;

Стандарт НАТО AFS Vol. IV (Standards for Maritime Forces) – вимоги до спроможностей військово-морських сил;

Стандарт НАТО AFS Vol. V (Joint Headquarters) – вимоги до спроможностей об'єднаних штабів;

Стандарт НАТО AFS Vol. X (Standards for Special Operations Forces) – вимоги до спроможностей спеціальних операцій.

Метою статті є визначення показників оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України із виконання завдань із відбиття воєнної агресії в КП для формування методики оцінювання спроможностей військ

зв'язку та кібербезпеки ЗС України в ході їх підготовки та застосування.

Виклад основного матеріалу дослідження

Нормативно-правові акти МО України та ЗС України, більшість з яких має обмеження доступу, видаються відповідно до вимог законів України, підзаконних актів державних органів, уповноважених у сферах комунікації (телекомунікації), інформатизації, захисту інформації тощо [12; 13; 14]. Разом із тим, спираючись на [13; 14], є можливим й доцільним цитування в частині КЗ інформаційно-комунікаційних систем (далі – ІКС) військового призначення, окремих положень та завдань з нормативно-правових актів МО України і ЗС України, які не є інформацією з обмеженим доступом. Так, визначено, що функціональна складова КЗ включає системи на:

запобігання (англійською мовою – «Prevention») – заходи щодо завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) КЗаг чи кібератак, припинення підготовки до них;

захисту (англійською мовою – «Protection») – заходи щодо забезпечення випереджувального захисту від можливих кібератак (кібервпливу) противника, в першу чергу, в інтересах всебічного та сталого забезпечення у КП процесів управління власними військами;

попередження (англійською мовою – «Mitigation») – заходи щодо безпосереднього виявлення, відвернення загрози, зменшення можливих втрат (збитків, пошкоджень) у разі безпосередньої загрози проведення кібератак;

реагування (англійською мовою «Response») – заходи комплексного реагування на вплив противника, у тому числі заходи захисту власної інфраструктури, особового складу, активів та ресурсів, тощо;

відновлення (англійською мовою – «Recovery») – заходи, спрямовані на відновлення інформаційної та іншої інфраструктури, що стала об'єктом кібератак противника, стабілізацію ситуації та ліквідації інших негативних наслідків.

Відповідним ОВУ, що здійснює управління військовими ОШС, які уповноважені на виконання вищезазначених функцій, визначені завдання щодо:

співпраці (реалізації спільних проектів та заходів, підтримання взаємодії) у межах повноважень з суб'єктами забезпечення воєнної безпеки та КБ держави, а також з НАТО, Європейським Союзом, державами-партнерами в частині спільного виконання завдань КО;

реагування (практичного виконання необхідних заходів) на поточні загрози КБ у воєнній сфері шляхом їх попередження, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу;

здійснення КЗ власної інформаційної інфраструктури (далі – ВІІ) (засобів рухомого зв'язку, як апаратної, так і контентної складових, додатків та сервісів зв'язку, інших ІКС та об'єктів інформаційної діяльності суб'єктів оборони держави) від кібератак та кібервпливу противника, що забезпечує необхідний рівень інформаційного забезпечення управління військами та зброєю, інші дії в КП тощо.

У 2016 р. введена в дію Стратегія кібербезпеки України [1], яка системно базувалася на положеннях Конвенції про кіберзлочинність, законодавство України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої була встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України [15] та стала першим офіційним документом, який визначив дефініцію КБ, як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в КП, що досягається комплексним застосуванням сукупності правових, організаційних та інформаційних заходів. Стратегія [1] визначила МО України та ГШ ЗС України завдання, щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у КП (КО) та КЗ ВІІ. Вона передбачала гармонізацію нормативних документів України у сфері КБ відповідно до міжнародних стандартів і стандартів ЄС та НАТО. За результатами експертних оцінок, стан реалізації Стратегії за визначеними показниками не перевищує 40 %, а саме:

не розроблені індикатори виконання Стратегії кібербезпеки України;

не вирішені питання оперативного обміну інформацією про КЗаг;

недостатніми є організація і проведення наукових досліджень у сфері КБ;

не створена ефективна система підготовки кадрів;

не створено дієву модель державно-приватного партнерства.

При цьому, Національна система КБ включає в тому числі й оборонні заходи, також визначено МО України та ГШ ЗС України завдання щодо підготовки держави до відбиття воєнної агресії у КП (КО); передбачено військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки КП та спільного захисту від КЗаг.

Проаналізувавши існуючу НПБ щодо завдань визначених перед МО України та ЗС України з відбиття воєнної агресії в КП є необхідним наголосити, що у 2021 р. було прийнято низку логічно взаємопов'язаних (рис. 1) документів оборонного та довгострокового планування.

Відкритими документами оборонного та довгострокового планування передбачено:

здійснення заходів із підготовки держави до

відбиття воєнної агресії у КП (КО), координація діяльності державних органів та органів місцевого самоврядування щодо підготовки та ведення КО;

отримання та узагальнення від основних суб'єктів забезпечення КБ інформації щодо об'єктів критичної ВІІ воєнної сфери та сфери оборони держави;

проведення інформаційно-аналітичної діяльності та прогнозування розвитку обстановки у воєнній сфері, пов'язаної з КЗаг та КП;

підтримання сил та засобів для дій в КП в готовності до виконання завдань за призначенням, здійснення адекватного нарощування їх готовності залежно від рівня загроз та ступенів реагування на них;

забезпечення несення бойового чергування визначених сил та засобів в інтересах підготовки та ведення КО;

здійснення підготовки та застосування ЗС України в КП щодо виконання ними завдань за призначенням та безпечного використання ними КП;

здійснення розвитку необхідних спроможностей МО України, ЗС України для дій в КП, підготовки та ведення КО, створення та розвиток відповідних ОШС, їх комплектування, підготовку та всебічне забезпечення [16];

здійснення військової співпраці з НАТО, пов'язаної з безпекою КП та спільним захистом від КЗаг, в тому числі й з військовими CERT країн-членів НАТО;

формування дієвої єдиної мережі ситуаційних центрів. Розгортання ситуаційних центрів МО України та ЗС України на одній ІТ – платформі в режимі реального часу у тісній взаємодії із ситуаційними центрами органів державної влади (резервними, на рухомій базі);

використання національного спеціального програмного забезпечення, яке дозволить здійснити інформаційне-аналітичне супроводження, моніторинг, прогнозування, прийняття рішень, проведення аудиту та безпеки. Зазначені процеси повинні відбуватись в одному цифровому середовищі, надійно захищеному від зовнішнього несанкціонованого втручання та кібератак;

реалізацію сталої технічної підтримки функціонування програмно-апаратного комплексу (платформи).

Виходячи із зазначеної НПБ держави, одним із головних безпекових аспектів у воєнній сфері на національному рівні, сфері оборони і військового будівництва визначено підтримання, нарощування (розвиток) та координація із забезпечення КБ, КЗ та КО під час підготовки та ведення всеохоплюючої оборони України [17].

Нинішні спроможності військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в КП складаються з сукупності показників спроможностей, а саме з:

прогнозування, виявлення та оцінки загроз національній безпеці держави в КП та через КП (кіберрозвідки);

активного КЗ (кібервпливу);

кіберзахисту.

Рис. 1. Модель формування нормативно правової бази України, МО України та ЗС України сфери КБ та КО

Зазначені показники спроможностей, в свою чергу, складаються з окремих показників виконання завдань, а саме:

1. Прогнозування, виявлення та оцінки загроз національній безпеці держави в КП та через КП (кіберрозвідка):

прогнозування та оцінка загроз національній безпеці держави в КП та через КП;

моніторинг КП, у тому числі щодо виявлення загроз в ІКС ЗС України;

здійснення розвідувальної діяльності щодо загроз національній безпеці держави у КП, інших подій і обставин, що стосується сфери КБ;

заходів, щодо виявлення уразливостей об'єктів КО, у тому числі шляхом моделювання, тестування на уразливість від КЗаг (кібератак), тощо;

оперативного інформаційного обміну між суб'єктами забезпечення КБ держави, щодо реалізованих та потенційних КЗаг;

інфомаційно-аналітичної діяльності та прогнозування розвитку обстановки у воєнній сфері, пов'язаній з КЗаг та КП.

2. Активного КЗ (кібервплив):

підготовки і проведення скоординованих заходів у КП суб'єктами КО (у тому числі щодо підготовки ВІІ) з метою запобігання виникнення воєнних конфліктів, стримування та відсічі воєнної агресії;

здатності зі створення сприятливих умов у КП для застосування ЗС України, інших військових формувань та правоохоронних органів, їх ефективних дій в КП, сприяння забезпеченню інформаційної безпеки держави у воєнній сфері;

реагування на поточні загрози КБ у воєнній сфері шляхом їх запобігання, завчасного виявлення, стримування та випереджувального реагування на них, усунення (мінімізації,

ліквідації) її наслідків;

порушення функціонування ВІІ противника, систем (процесів) прийняття ним рішень та здійснення управління військами (силами) під час одночасного захисту власного КП;

спроможності щодо проведення розвідувальним органом МО України відповідно до компетенції заходів протидії зовнішнім загрозам національній безпеці України у КП;

випереджувального та/або оперативного реагування на проведення противником заходів у КП та через КП, мінімізація результатів їх впливу;

з отримання доступу (у тому числі фізичного) до ВІІ противника, у тому числі на контрольованій ним території;

проведення заходів фізичного впливу в інтересах та під час ведення КО, у тому числі шляхом виведення з ладу особового складу, озброєння, технічних засобів, комунікацій противника, а також проведення спеціальних дій (диверсій), вогневого ураження, інших форм кінетичного та іншого впливу, що призводить до припинення функціонування, механічного руйнування, пошкодження конструкції, виведення з ладу або знищення фізичного об'єкта ВІІ (його інформаційних ресурсів) та суб'єктів інформаційної діяльності, сил і засобів інформаційних (кібер) операцій;

проведення правових, організаційних, технічних заходів припинення функціонування (блокування) об'єктів ВІІ в інтересах підготовки та ведення КО;

створення електромагнітних перешкод, радіоелектронного придушення роботи телекомунікаційних та інших засобів в інтересах КО;

спроможності щодо спеціальних дій підрозділів спеціального призначення та інформаційно-психологічних операцій в інтересах КО.

3. Кіберзахист:

КЗ ІКС ЗС України (статистичний та мобільний КЗ);

КЗ систем управління озброєнням та військовою технікою;

КЗ (участь у заходах КЗ) об'єктів критичної ІІ держави в умовах правового режиму надзвичайного та воєнного стану;

КЗ об'єктів інфраструктури МО України, ЗС України, Державної спеціальної служби транспорту (арсеналів, баз, складів, позицій чергування засобів ППО, місць базування авіації та ВМС, спеціальних споруд тощо).

Модель методики оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в КП можна навести такою логіко-структурною схемою (рис. 2).

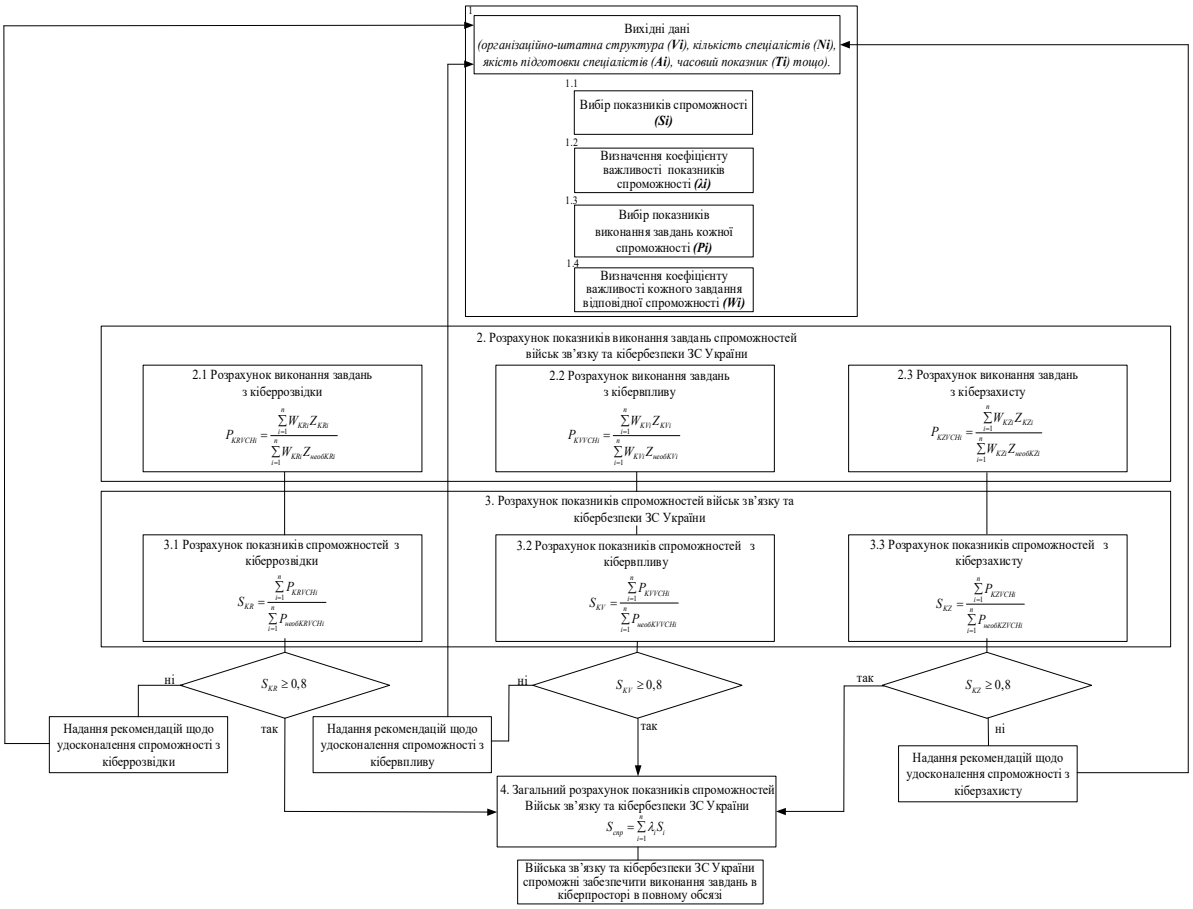

Рис. 2. Логіко-структурна схема моделі методики оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в кіберпросторі

Запропонована модель методики дає можливість послідовно крок, за кроком проводити розрахунок спроможностей військ зв'язку та кібербезпеки ЗС України із виконання завдань з відбиття воєнної агресії в КП. По даній методиці розрахунок спроможностей військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в КП займає дуже багато часу та сил, але затрачені зусилля на проведення розрахунків спроможностей компенсуються отриманим, об'єктивним результатом. Зазначене, дає змогу найбільш ефективно застосовувати війська зв'язку та кібербезпеки ЗС України для виконання бойових задач із КБ та активних дій, від характеру виконання загальних дій яких залежить якість, ефективність, мобільність, оперативність управління військами (силами) в операціях. При цьому пропорційно збільшуються показники з бойового потенціалу військ зв'язку та кібербезпеки ЗС України в ході планування на їх бойове застосування.

Для оцінки спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з відбиття воєнної агресії в КП в цілому необхідно оцінити виконання окремих завдань кожної спроможності, а саме:

1. Прогнозування, виявлення та оцінка загроз національній безпеці держави в КП та через КП (здійснення кіберрозвідки) (табл. 1).

Таблиця 1

Оцінювання спроможностей військ зв'язку та кібербезпеки в частині виконання завдань із кіберрозвідки

Показник $KRVCHi$	Розрахунок показника P_{KRVCHi}
Головний об'єднаний ЦЗІ та КБ ЗС України, у складі:	P_{KRVCHi}
ЦЗІ та КБ	P_{KRVCHi}
…	…
ЦЗІ та КБ	P_{KRVCHi}
…	$P_{KRVCHi} = \frac{\sum_{i=1}^{n} W_{KRi} Z_{KRVCHi}}{\sum_{i=1}^{n} W_{KRi} Z_{max KRVCHi}}$
S_{KR} – показник спроможності військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з кіберрозвідки загалом	$S_{KR} = \frac{\sum_{i=1}^{n} P_{KRVCHi}}{\sum_{i=1}^{n} P_{max KRVCHi}}$

де P_{KRVCHi} – загальний показник оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань із кіберрозвідки;

Z_{KRVCHi} – показник оцінювання окремого завдання з кіберрозвідки за кожну визначену військову частину військ зв'язку та кібербезпеки ЗС України;

W_{KRi} – коефіцієнт важливості виконання кожного окремого завдання з кіберрозвідки.

Показник спроможності військ зв'язку та кібербезпеки ЗС України з кіберрозвідки загалом розраховується, як зважена та нормована оцінка показників здатності виконання завдань з кіберрозвідки.

2. Активного КЗ (здійснення кібервпливу). (табл. 2).

Таблиця 2

Оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з кібервпливу

Показник $KVVCHi$	Розрахунок показника P_{KVVCHi}
Головний об'єднаний ЦЗІ та КБ ЗС України, у складі:	P_{KVVCHi}
ЦЗІ та КБ	P_{KVVCHi}
…	…
ЦЗІ та КБ	P_{KVVCHi}
…	$P_{KVVCHi} = \frac{\sum_{i=1}^{n} W_{KVi} Z_{KVVCHi}}{\sum_{i=1}^{n} W_{KVi} Z_{max KVVCHi}}$
S_{KV} – показник спроможності військ зв'язку та кібербезпеки ЗС України виконання завдань з кібервпливу загалом	$S_{KV} = \frac{\sum_{i=1}^{n} P_{KVVCHi}}{\sum_{i=1}^{n} P_{max KVVCHi}}$

де P_{KVVCHi} – загальний показник оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з кібервпливу;

Z_{KVVCHi} – показник оцінювання окремого завдання з кібервпливу за кожну визначену військову частину військ зв'язку та кібербезпеки ЗС України;

W_{KVi} – коефіцієнт важливості виконання кожного окремого завдання з кібервпливу.

Показник спроможності військ зв'язку та кібербезпеки ЗС України з кібервпливу загалом розраховується, як зважена та нормована оцінка показників здатності виконання завдань з кібервпливу.

3. Кіберзахист (здійснення КЗ) (табл. 3).

Таблиця 3

Оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з кіберзахисту

Показник $KZVCHi$	Розрахунок показника P_{KZVCHi}
Головний об'єднаний ЦЗІ та КБ ЗС України, у складі:	P_{KZVCHi}
ЦЗІ та КБ	P_{KZVCHi}
…	…
ЦЗІ та КБ	P_{KZVCHi}
…	$P_{KZVCHi} = \frac{\sum_{i=1}^{n} W_{KZi} Z_{KZVCHi}}{\sum_{i=1}^{n} W_{KZi} Z_{max KZVCHi}}$
S_{KZ} – показник спроможності військ зв'язку та кібербезпеки ЗС України виконання завдань з кіберзахисту загалом	$S_{KZ} = \frac{\sum_{i=1}^{n} P_{KZVCHi}}{\sum_{i=1}^{n} P_{max KZVCHi}}$

де P_{KZVCHi} – загальний показник оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з кіберзахисту;

Z_{KZVCHi} – показник оцінювання окремого завдання з кіберзахисту за кожну визначену військову частину військ зв'язку та кібербезпеки

ЗС України;

W_{KZi} – коефіцієнт важливості виконання кожного окремого завдання з кіберзахисту.

Показник спроможності військ зв'язку та кібербезпеки ЗС України з кіберзахисту загалом розраховується, як зважена та нормована оцінка показників здатності виконання завдань з кіберзахисту.

Якщо показники $S_{KR} \geq 0{,}8, S_{KV} \geq 0{,}8, S_{KZ} \geq 0{,}8$, то для оцінки спроможності військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в КП в цілому розраховуємо загальний коефіцієнт виконання спроможностей:

$$S_{спр} = \sum_{i=1}^{n} \lambda_i S_i,$$

де $S_i - S_{KR}, S_{KV}, S_{KZ}$ – спроможність військ зв'язку та кібербезпеки ЗС України до виконання завдань з кіберрозвідки, кібервпливу та кіберзахисту загалом;

λ_i – коефіцієнт важливості показника кожної спроможності.

$S_{спр}$ – спроможність військ зв'язку та кібербезпеки ЗС України виконувати завдання з відбиття воєнної агресії в кіберпросторі в повному обсязі.

Водночас, слід пам'ятати, що проведення аналізу відповідності окремих спроможностей, груп спроможностей, функціональних груп спроможностей, чи органів військового управління (військ зв'язку та кібербезпеки ЗС України) та здійснення їх оцінювання проводиться відповідно до сценаріїв оборонного планування. Результатом зазначеного аналізу є вироблення обґрунтованих рекомендацій для формування узгоджених, реалістичних та прийнятних рішень (матеріальних і нематеріальних) з розвитку відповідних спроможностей.

Типовими проблемами під час виконання процесу оцінювання спроможностей можуть бути:

неможливість досягти визначених, в ході оборонного огляду спроможностей, в реальних умовах (потребує матеріальних рішень);

недостатні кількісні та якісні показники спроможності (потребує матеріальних і нематеріальних рішень);

закінчення життєвого циклу носіїв спроможності (потребує матеріальних рішень);

політичні обмеження, які унеможливлюють досягнення окремих спроможностей (необхідні нематеріальні рішення).

Отже, загалом, процедура оцінювання спроможностей передбачає: порівняння наявних спроможностей з тими, які будуть потрібні у майбутньому; виявлення недоліків у вимогах до спроможностей; встановлення нових чи оновлення існуючих вимог. Водночас, у ході оцінювання спроможностей розробляються рекомендації щодо проведення відповідних змін одночасно у всіх споріднених організаційних структурах та носіях відповідних спроможностей.

Висновки й перспективи подальших досліджень

Отже, в межах розгляду шляхів розбудови національної системи КБ, на основі досвіду провідних країн світу з протистояння в КП, встановлено, що провідні держави світу дедалі більше уваги надають розвитку й захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення КБ держави.

Водночас залишаються невирішеними питання в міжнародному нормативно-правовому полі, які унеможливлюють формалізацію безпекової політики в КП. Відсутній консенсус щодо правил поведінки в КП, не визначені загальноприйняті методології оцінки наслідків кіберзлочинів та їх розгляд як об'єкта міжнародних норм і правил (зокрема, щодо визнання кібератаки як акту війни).

Сьогодні, для організації та проведення оцінювання спроможностей в ЗС України використовуються існуючі національні стандарти, методики та керівництва, також використовуються міжнародні практики, описані відповідними стандартами і публікаціями НАТО.

В цілому, з огляду на зазначене, в статті визначено показники оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України із виконання завдань з відбиття воєнної агресії в КП, сформовано методику оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в ході їх підготовки та застосування.

Література

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 23.12.2022). **2. Закон України** «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 23.12.2022). **3. Закон України** «Про оборону України» від 06.12.1991 р. № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 23.12.2022). **4. Закон України** «Про Збройні Сили України» від 6 грудня 1991 р. № 1934-XII. URL: https://zakon.rada.gov.ua/laws/show/1934-12#Text (дата звернення: 23.12.2022). **5. Ertan A.** (Eds.) Cyber Threats and NATO 2030: Horizon Scanning and Analysis: URL://https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf (дата звернення: 23.12.2022). **6. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021 URL:

https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 23.12.2022). **7. Указ Президента України** «Про Концепцію боротьби з тероризмом в Україні» від 05.03.2019 р. № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text (дата звернення: 23.12.2022). **8. Вдовенко С., Даник Ю., Фараон С.** Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *Комп'ютерні науки та кібербезпека*. 2019. № 1(12). URL: https://periodicals.karazin.ua/cscs/article/view/13080 (дата звернення: 23.12.2022). **9. Звіт про науково-дослідну роботу** удосконалення понятійно-категорійного апарату у сфері кібероборони шифр «Дефініція» (заключний) № держреєстрації 0120U103696 8.06.5.035. Київ, 2020. 203 с. **10. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В.** Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ : ДУТ, 2015. 288 с. **11. Трофименко О.** Аналіз дефініцій різновидів інформаційних війн. URL: http://conf.inf.od.ua/doklady-konferentsii/150-trofimenko (дата звернення: 23.12.2022). **12. Закон України** «Про державну таємницю» від 21.01.1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 23.12.2022). **13. Закон України** «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 23.12.2022). **14. Закон України** «Про інформацію» № 2938-VI. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text. **5. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 06 травня 2015 року "Про Стратегію національної безпеки України"» від 26.05.2015 р. № 287 URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення: 23.12.2022). **16. Живило Є.** Об'єднана підготовка персоналу складових Сил оборони сфери кібербезпеки в умовах тотальної оборони держави. URL: https://tp.kh.ua/index.php/tpdu/article/view/295/273, DOI: 10.34213/tp.21.02.16. **17. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 16 лютого 2017 року "Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури" від 16 лютого 2017 року» від 16.02.2017 р. № 37/2017. URL: https://zakon.rada.gov.ua/laws/show/n0001525-17#Text. (дата звернення: 23.12.2022).

MODEL OF ASSESSMENT OF MILITARY COMMUNICATION AND CYBER SECURITY CAPABILITIES OF THE ARMED FORCES OF UKRAINE FOR PERFORMING TASKS OF REFLECTING MILITARY AGGRESSION IN CYBER SPACE

Yevgen Zhyvylo (Candidate of sciences in public administration) [1]
Valentyn Dokil [2]

[1] ***Kruty Heroes Military Institute of Telecommunications and and Information Technologies***
[2] ***National Defence University of Ukraine named after Ivan Cherniakhovskyi***

Innovation has driven military strategy since the dawn of mankind. The invention of gunpowder, the organ cannon, and the internal combustion engine had a huge impact not only on the trends in the development of military strategy, but also on the entire chronology of world history. The 20th century was no exception. The evolving Internet continues to expand the possibilities of information technology. But, like other great inventions, its capabilities are often used to achieve negative goals and results.

Today, in the course of the full-scale Russian invasion of Ukraine, our society and state faced a new threat that has enormous military and geopolitical potential. In a short period of time, the vulnerabilities of unified electronic communications systems, technological process management systems have turned into an effective and probable set of real and potential threats to Ukraine's national security in cyberspace. These threats are capable of disrupting the normal functioning of communication systems of special users, including disruption and/or blocking of system operation, and/or unauthorized management of its resources.

At the same time, the communication and cyber security forces of the Armed Forces of Ukraine play a key role in supporting the stable functioning of such systems as part of the Security and Defense Forces of Ukraine. Thus, the procedure for organizing the assessment of capabilities in the Armed Forces of Ukraine as an element of capability-based planning is carried out taking into account the approaches adopted by NATO member states.The specified field of application covers the issue of the methodology of the process of organizing the assessment of capabilities, determining the participants of this process, the procedure and order of its implementation, the relationship with other processes, and the use of the results of this activity.

At the same time, due to the absence of the Law of Ukraine "On the National Security of Ukraine" (revision is underway), which will regulate the issues of assessment of capabilities, it will be premature to approve any legal framework that would regulate this area of activity. Under these conditions, representatives of the Ministry of Defense and the Armed Forces of Ukraine unanimously emphasize the need to develop appropriate methods for forecasting, identifying and assessing threats to the state's national security in cyberspace and through cyberspace. Separately, it should be emphasized the need to determine the order of organization of the assessment of capabilities, the development of a methodology for assessing the capabilities of the communications and cyber security forces of the Armed Forces of Ukraine for the performance of tasks to repel military aggression in cyberspace.

Keywords: *digital society; information and communication systems; assessment of abilities; cyber threats; cyber security; cyberspace.*

References

1. Hrytsiuk, Yu. I. (2016). Cyber Intervention and Cybersecurity in Ukraine: Problems and Prospects for Overcoming Them. Naukovyi visnyk, 26, 8. **2. Hryshchuk, R. V., Danyk, Yu. H.** (2016). Basics of cyber security: monohrafiia. Zhytomyr : ZhNAEU, 636. **3. Dubov, D. V., Ozhevan, M. A.** (2011). Cybersecurity: global trends and challenges for Ukraine. Kyiv: Vyd-vo NISD, 30. **4. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V.** (2015). Information and cybersecurity: the socio-technical aspect: pidruchnyk. Kyiv : DUT, 288. **5. Kyryliuk, R., Shelest, Ye.** (2021). Cyber Forces as a Component of the National Security System Transformation. Oboronnyi visnyk : Tsentr voiennoi polityky ta polityky bezpeky, 9, 4–10. **6. Klymchyk, O. O.** (2010). Criminal Legal Qualification of the Use of Computer Technologies for Committing Terrorist Acts. Informatsiina bezpeka liudyny, suspilstva, derzhavy, 1(3), 26–30. **7. Lipkan, V. A., Lipkan, O. S.** (2008). National and international security in definitions and concepts. Kyiv : Tekst, 400. **8. Melnyk, S. V., Kashchuk, V. I.** (2013). Current Areas of Prevention of Offenses in Cyberspace as a Component of the State's Cyber Security Strategy: zb. materialiv nauk.-prakt. konf. 5 kvitnia 2013 r., m. Kyiv. Kyiv : Nauk.-vyd. tsentr NA SB Ukrainy, 416. **9. Shelomentsev, V. P.** (2012). Legal support of the cyber security system of Ukraine and the main directions of its improvement. Fighting organized crime and corruption (theory and practice), 1, 312–320. **10. Strategy of the NATO** Defence Education Enhancement Program (DEEP) in terms of distance learning. (2021). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230208-deep-strategy-for-distance-learni-1.pdf (data zvernennia: 05.12.2022). **11. Didyk, V. O., Honcharuk, A. A., Simonenkova, I. V.** (2017). Cybersecurity in the Armed Forces of Ukraine to counter possible variants of cybercrime. Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: mater. Vseukr. nauk.-prakt. konf. (m. Odesa, 17 lystopada 2017 r.). Odesa: Odes. derzh. un-t vnutr. spr., 94–95. **12. Voitsikhovskyi, A. V.** (2018). Cybersecurity as a direction of Ukraine's Euro-Atlantic integration. Pravo i bezpeka u konteksti yevropeiskoi ta yevroatlantychnoi intehratsii: zbirnyk statei ta tez naukovykh povidomlen za materialamy dyskusiinoi paneli II Kharkivskoho mizhnarodnoho yurydychnoho forumu, m. Kharkiv, 28 veresnia 2018 r. / redkol: Yu. H., Barabash, T. M., Anakina, D. V., Abbakumova. Kharkiv : Pravo, 42–48. **13. Law of Ukraine** «On the Basic Principles of Ensuring Cybersecurity of Ukraine», 05.10.2017, 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennia: 05.12.2022). **14. Law of Ukraine** «On Defense of Ukraine», 06.12.1991, 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (data zvernennia: 05.12.2022). **15. Decree of the President of Ukraine** «On the Regulation on the General Staff of the Armed Forces of Ukraine», 30.01.2019, 23/2019. URL: https://zakon.rada.gov.ua/laws/show/23/2019#Text (data zvernennia: 05.12.2022). **16. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"», 26.08.2021, 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (data zvernennia: 05.12.2022). **17. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On Urgent Measures for the State's Cyber Defense"», 26.08.2021, 446/2021. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text (data zvernennia: 05.12.2022). **18. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine"», 17.09.2021, 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (data zvernennia: 05.12.2022).