УДК 351.862.4:342.951:351.85:340.134
DOI https://doi.org/10.32782/2663-5941/2023.1/22

Чумаченко С.М.
Національний університет харчових технологій

Кутовий О.П.
Національний університет оборони України імені Івана Черняхівського

Попель В.А.
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації

Гуйда О.Г.
Таврійський національний університет імені В.І. Вернадського

Заїка Н.В.
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації

Мурасов Р.К.
Національний університет оборони України імені Івана Черняхівського

НАУКОВО-МЕТОДИЧНИЙ ПІДХІД ЩОДО ОЦІНЮВАННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ЇЇ ОБ'ЄКТІВ ВІД БПЛА І КРИЛАТИХ РАКЕТ

Аналіз відомих підходів до оцінювання рівнів безпеки об'єктів критичної інфраструктури і обробки ризиків, пов'язаних із застосуванням терористами та ворогом безпілотних літальних апаратів та крилатих ракет, в тому числі із застосуванням засобів сучасного зенітно-ракетного, зенітно-артилерійського озброєння, комплексів радіоелектронної боротьби показує, що оцінки таких ризиків не завжди мають необхідну точність. Проблеми вимірювання ризиків пов'язані, в тому числі, з особливостями застосованого озброєння, включаючи крилаті ракети і безпілотні літальні апарати.

До визначальних чинників, що призводить до похибок оцінки цих ризиків, що можливо визначити, як проблему ефективної роботи комплексів оборони та захисту критичної інфраструктури, є вирішення задачі своєчасного виявлення безпілотних літальних апаратів і крилатих ракет та їх якісного супроводження.

Проблеми виявлення та розпізнавання цілей обумовлені їх малими розмірами та масо-габаритними характеристиками, що ускладнює їх виявлення навіть на малих відстанях. Це стосується як радіолокаційних засобів розвідки, так і оптико-електронних. Крім того сам процес виявлення цілей залежить від ступеня його автоматизації. Процес ураження цілей залежить від точності наданих координат розвідки засобам ураження, точності прицілювання цих засобів та їх тактико-технічних характеристик.

Таким чином, існує проблема створення таких засобів боротьби з безпілотними літальними апаратами, які взаємодіють та якісно працюють на всіх етапах – від виявлення цілей до їх ураження.

З метою досягнення необхідних результатів оборони (що в ризик-моделі відповідає точності обробки ризиків), доцільно розділити систему оборони на складові та провести аналіз впливу кожної складової, що входять до системи з числа засобів боротьби з безпілотними літальними апаратами.

Пропонується розглянути чотири основні підсистеми, такі як інформаційну, керуючу, виконавчу підсистеми та підсистему забезпечення. Кожна з підсистем визначається сукупністю показників і критеріїв оцінювання. Вклад кожної з підсистем дозволяє провести оцінку ефективності роботи всього комплексу засобів захисту критичної інфраструктури в цілому.

Пропонується розглянути модель оцінки ефективності комплексу засобів захисту об'єктів критичної інфраструктури і боротьби з безпілотними літальними апаратами та крилатими ракетами, у якій оцінюється ефективність роботи основних складових комплексу засобів. Пропонується проведення оцінки за критерієм ефективність-вартість, що допоможе приймати обґрунтовані рішення щодо побудови оптимальних схем захисту критичної інфраструктури і боротьби з безпілотними літальними апаратами і крилатими ракетами на основі наявних сил та засобів.

Ключові слова: *критична інфраструктура, ефективність, рівень ефективності, безпілотний літальний апарат, крилата ракета, зенітно-ракетний комплекс, зенітно-артилерійський комплекс, радіолокаційна станція, радіоелектронна боротьба, критерій, ваговий коефіцієнт.*

Постановка проблеми. Безпілотні літальні апарати (БПЛА, або дрони) та крилаті ракети (КР) є досить новими видами озброєнь на полі бою, з 1990-х років їх активно використовують збройні сили провідних країн світу і вже з'явилися результати їх ефективного застосування в останніх воєнних конфліктах.

Бурний розвиток БПЛА призвів до появи багатьох їх різновидів, від розвідників до ударних «камікадзе», дуже різних за розмірім та цільовим навантаженням. Особливо небезпечними стають саме ударні БПЛА – носії зброї та БПЛА «камікадзе» (або баражуючи боєприпаси). БПЛА «камікадзе» віднесені до різновиду ударних БПЛА, тільки вони знищують цілі атакуючи зверху. Так, під час воєнних конфліктів воюючі сторони демонструють ефектні відеокадри, які передають дрони-розвідники, відео з камер ударних безпілотників або записи виявлення цілей та самонаведення на цілі, які передали «дрони-камікадзе».

Всі провідні країни світу активно розвивають цей новий вид озброєння який має дуже великий потенціал розвитку та застосування в сучасних і майбутніх війнах. США, Ізраїль, Туреччина, Китай, Канада, Франція, Німеччина, Іран, Росія та інші країни проводять масове виробництво та активне застосування БПЛА в останніх воєнних конфліктах і в Україні, поступово покращуючи їх технічні характеристики та принципи застосування.

Ізраїль вважається лідером технологічних розробок в галузі БПЛА. За Ізраїлем йдуть США, Китай, Канада, Туреччина, Іран, Росія.

З розвитком принципів застосування БПЛА і КР по об'єктам критичної інфраструктури (КІ) відповідно відбувається розвиток систем озброєння, яке спроможне протидіяти цьому досить новому виду зброї. Традиційно до вирішення цієї задачі залучаються зенітні комплексі різних типів, які за своїми характеристиками спроможні виявляти та вражати БПЛА і КР. Але використання більшої частини зенітних комплексів неприйнятне за критерієм «ефективність-вартість». Враховуючи такий стан справ відбувається пошук прийнятних засобів боротьби з БПЛА і КР для захисту КІ. Такі роботи спрямовані на використання і засобів радіоелектронної та оптико-електронної боротьби, і засобів маскування та макетів техніки, і різних перешкод у повітрі (аеростати, сітки та інше), а також на можливу модернізацію зенітних комплексів, характеристики яких потенційно можуть бути покращені для ведення ефективної боротьби з БПЛА і КР. Виконання наведених напрямів робіт передбачає проведення попередньої оцінки їх ефективності, як за окремими рішеннями, так і за сукупністю рішень.

Актуальним стає завдання обґрунтування та оцінки таких засобів захисту КІ, протидії та боротьби з засобами повітряного нападу, що позбавлені недоліків притаманних сучасним зенітним комплексам, які спроможні ефективно захищати КІ, виявляти та вражати ударні БПЛА і КР, виконувати завдання боротьби або самостійно, або у складі існуючих зенітних комплексів, безпосередньо у складі бойової техніки.

Аналіз останніх досліджень і публікацій. Аналіз публікацій за напрямом протидії БПЛА і КР, показує, що наукових статей з даної тематики досить багато. У переважній більшості робіт в цій області переважають надмірно оптимістичні висновки щодо успішності ураження всіх видів БПЛА існуючими російськими засобами ППО та РЕБ. Ситуація нагадує роки початку розвитку авіації та наземних засобів протидії їх застосуванню – засобів протиповітряної оборони. Причому склалося так, що розвиток авіації завжди випереджав розвиток наземних засобів протиповітряної оборони. З авіацією добре боролась саме авіація. Але і у цьому випадку постійно йшла напружена конкурента боротьба технологій.

Разом з тим, різке та різноманітне вторгнення БПЛА в сучасні бойові дії, їх стрімкий технологічний розвиток виявили проблему ефективної боротьби з ними, особливо з малими БПЛА, яка на даний час залишається надзвичайно складною, системною, і до цих пір ефективно не вирішеною. Тільки одиниці держав світу мають частково в наявності та розвивають засоби, які спроможні достатньо ефективно протидіяти застосуванню сучасних БПЛА.

В існуючих публікаціях пропонуються певні технічні рішення щодо боротьби з БПЛА та теоретичні підходи до оцінки їх ефективності, які, як правило, носять оптимістичний характер [2-9, 12-17], з досить поверхневим теоретичним обґрунтуванням та наявності належних практичних результатів і не зовсім підходять для синтезу засобів протидії БПЛА та КР в умовах ведення сучасних інтенсивних бойових дій, в різних умовах бойової обстановки та погодно-кліматичних умов.

Крім того, у цих роботах, як правило, не обговорюється воєнно-технічний аспект оцінки технічних рішень за критерієм ефективність-вартість. Вважається, що «ефективність» є спроможність системи утворювати системний ефект, але така спроможність має кількісну міру. Таким

чином, об'єктивно існує безпосередній зв'язок між рівнем системного ефекту *VS* і витратами *RS* потенціалу здатності сил на його утворення (які дорівнюють «трудовитратам» сил *NS* за час їх застосування *TS* за дією управління використанням інформаційного ресурсу *IS*) [18].

Встає питання у об'єктивному порівнянні ефективності технічних рішень захисту критичної інфраструктури і боротьби з сучасними та перспективними БПЛА і КР з обґрунтуванням їх вартості.

Так, у роботах [5-7] виконаний тільки аналітичний огляд особливостей способів протидії БПЛА без їх порівняння між собою. У роботі [3] наведений алгоритм оцінки ефективності комплексних заходів протидії, деякі тактичні і технічні характеристики БПЛА але він не враховує можливі умови бойової обстановки та погодно-кліматичні умови. У роботі [4] запропонована якісна оцінка способів протидії БПЛА без кількісних оцінок. У [17] запропонована система критеріїв для оцінки ефективності способів протидії БПЛА з їх кількісною оцінкою, але систематизація способів протидії носить дуже суб'єктивний характер, без врахування особливостей об'єктів КІ, вартісних показників та особливостей складу систем захисту об'єктів КІ (ОКІ).

Поява нового виду озброєння – БПЛА та їх застосування в останніх воєнних конфліктах виявили суттєві недоліки зенітних комплексів, що стоять на озброєнні в різних країнах. Сталося так, що незалежна Україна отримала у спадок від Радянського Союзу разом із зенітним озброєнням і всі їх технічні недоліки щодо можливості ведення ефективної боротьби з сучасними БПЛА, особливо малорозмірними. Робіт щодо модернізації цих комплексів та спрямованих на усунення цього недоліку проводилось недостатньо. Аналіз характеристик зенітних комплексів протиповітряної оборони провідних країн світу показує, що багато різноманітних заявлених комплексів протиповітряної оборони нібито здатні вражати як БПЛА, так і крилаті ракети «повітря-земля», літаки, вертольоти. Однак, треба усвідомлювати, що боротьба з БПЛА різних класів суттєво відрізняється. Так, дійсно БПЛА великих та середніх розмірів (типу Predator и Reaper от General Atomics) виявляються, супроводжуються та вражаються з досить високою ефективністю, а з БПЛА малих розмірів виникають суттєві проблеми.

Концептуальні підходи до вирішення проблеми боротьби з БПЛА, що зустрічаються у більшості публікацій, можна звести до наступного:

формування багато-ешелонованого угруповання з різних типів зенітних комплексів, таких як зенітні ракетні комплекси (ЗРК), зенітні артилерійські комплекси (ЗАК), зенітні гарматно-ракетні комплекси (ЗГРК), переносні зенітні ракетні комплекси (ПЗРК), що мають досить високі розвідувальні та вогневі можливості щодо виявлення та вогневого ураження саме малорозмірних БПЛА;

розробка та застосування у складі існуючих ЗРК, ЗАК, ЗГРК додаткових каналів виявлення та супроводження цілей з метою ведення ефективної боротьби саме з малорозмірними БПЛА;

розробка перспективних зразків ЗРК, ЗАК, ЗГРК спроможних вести боротьбу з широким колом цілей, як з літаками (звичайними і за технологією «Стелс») так і малорозмірними БПЛА;

розробка спеціалізованих автоматизованих засобів захисту бойової техніки Сухопутних Військ від бойових БПЛА типу «камікадзе»;

застосування комплексу засобів що до радіоелектронного придушення каналів управління, розвідки, та бойового застосування БПЛА;

розробка спеціалізованих засобів та комплексів боротьби з малорозмірними БПЛА, які застосовують нетрадиційні принципи боротьби.

Сучасні комплекси і системи ППО і ПРО та їх можливі зони прикриття ОКІ наведено на рис. 1.

В [2] відмічається, що для виявлення малорозмірних БПЛА необхідно визначати спеціалізовані засоби розвідки, які мають кращі розвідувальні можливості виявлення та супроводження малорозмірних БПЛА, створювати спеціалізовані канали першочергової передачі розвідувальної інформації про дії малорозмірних БПЛА. Для досягнення високої ефективності системи розвідки повітряних цілей вважають, що немаловажним є виконання комплексу організаційно-тактичних заходів, а саме:

частіша зміна позицій радіолокаційних станцій (РЛС) і засобів зв'язку;

розгортання системи помилкових позицій з імітацією роботи радіоелектронних засобів;

проведення якісного інженерного обладнання позицій РЛС розвідки та зенітних комплексів;

інтенсивне застосування пасивних відбивачів-пасток, імітаторів теплового випромінювання;

розгортання біля позицій РЛС розвідки вогневих засобів протиповітряної оборони (ППО);

організація захисту засобів розвідки від дій диверсійних груп та інші.

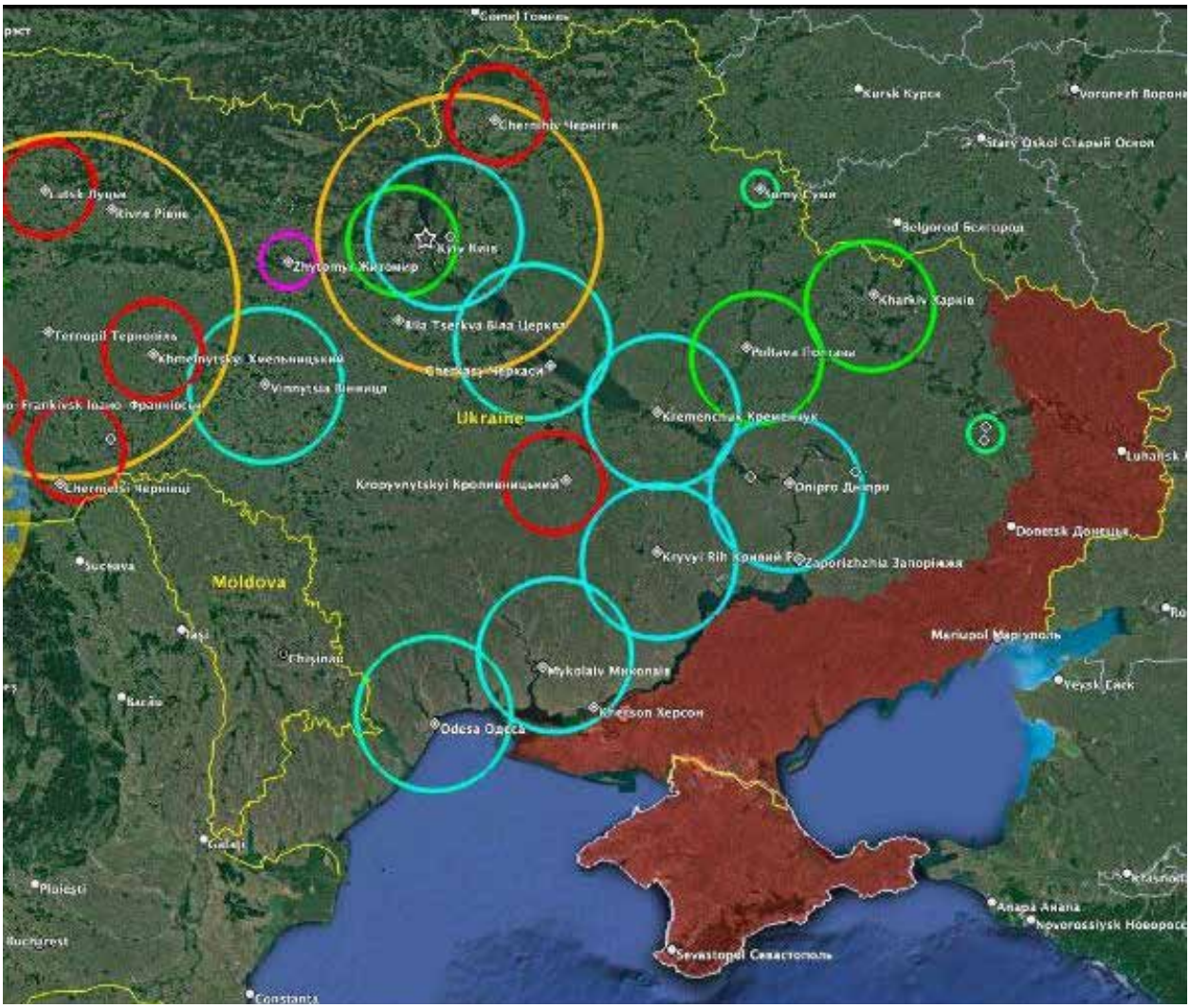

Рис. 1. Зони прикриття прийнятих на озброєння зенітно-ракетних систем і комплексів західного зразка для прикриття повітряного простору в зоні розташування ОКІ [19]:

8 NASAMS
6 NAWK
4 IRIS-T
1 Patriot и 1 SAMP/T
TOP

Як показали результати останніх бойових дій в Україні та у Нагорному Карабахі, – ці заходи залишаються малоефективними. Знаходження малорозмірного БПЛА у мертвій воронці зенітних засобів, безпосередньо над наземними цілями призводить до безкарних дій БПЛА по ураженню цих цілей.

Слід відзначити, що ефективна боротьба з малорозмірними БПЛА (що мають ефективну поверхню розсіяння (ЕПР) не менше 0,01 м^2) існуючими зенітними комплексами можлива лише з великими обмеженнями щодо їх своєчасного виявлення та обстрілу. Ефективна боротьба з БПЛА що мають ЕПР меншу ніж 0,01 м^2 сучасними зенітними комплексами практично неможлива.

Мета статті – дослідження методичного апарату для захисту ОКІ та техніко-економічного аналізу запропонованих технічних рішень ведення боротьби з БПЛА і КР за критерієм ефективність-вартість.

Викладення основного матеріалу. Кожна технічна система (комплекс) захисту ОКІ й боротьби з БПЛА і КР, як складна система, – повинна мати у своєму складі ряд технічних складових (підсистем), об'єднаних у єдине ціле. Розглянемо тезаурус такої складної системи.

Система безпеки ОКІ, як «ергатична система», має такі загальносистемні характеристики:

системна могутність – темп приросту у часі системного ефекту в процесі її застосування;

запас здатності – певний час для наявних умов застосування, на протязі якого система здатна власними «силами» утворювати ефект із потрібною могутністю наявним ресурсом «засобів» (тому ресурсний склад – матеріальна основа здатності);

системний потенціал – максимальний системний ефект застосування, який може бути досягнутий її «силами» при вичерпанні запасу здатності;

ефективність – міра «доцільності» (досконалості) системи як продуктивність витрат запасу здатності («трудовитрат» сил) щодо створення системного ефекту потрібного рівня (рівня «безпеки» ОКІ) в акті застосування.

Оскільки метою наукового дослідження взагалі є вдосконалення «об'єкту» наукового дослідження (тобто підвищення його ефективності), тому предметом дослідження обрано управління об'єктом «система безпеки ОКІ», як найбільш значущий (пріоритетний) чинник, що впливає на ефективність об'єкту. Пріоритетність управління обґрунтована таким чином. Основні принципи системного підходу випливають із загальної концепції застосування об'єкта «складна система» для досягнення мети. Основою загальної концепції функціонування складної системи є кероване (згідно завданню – стимулу) перетворення ресурсного потенціалу системи у системний ефект (реакцію) для досягнення системної мети [18], що й визначає зміст системних ознак, властивостей і характеристик, як то показане на рис. 2.

Кожна складна система складається з підсистем, які мають своє цільове призначення. Умовно у складі складних технічних систем виділяють за призначенням інформаційну, керуючу, виконавчу підсистеми та підсистему забезпечення. Їх спільна робота і повинна забезпечити ефективну роботу всієї системи захисту ОКІ і боротьби з БПЛА і КР.

Розглянемо головні функції, які повинні вирішувати підсистеми у складі системи захисту ОКІ і боротьби з БПЛА і КР.

Функцією інформаційної підсистеми є пошук, виявлення та розпізнавання БПЛА і КР, що знаходяться у верхній (особливо небезпечній) півсфері.

У якості інформаційної підсистеми можуть буди використані радіолокаційні, оптичні, інфрачервоні та інші типи датчиків (сенсорів) з відповідною апаратурою обробки інформації та прийняття рішення по виявленню та ураженню БПЛА і КР. Відстані роботи цих датчиків різні, по різному залежать від зовнішніх умов та перешкод. Тому ефективність роботи інформаційної підсистеми з одним з наведених датчиків крім їх технічних характеристик буде залежати від ступеня впливу зовнішніх умов та перешкод.

Функціями керуючої підсистеми є управління роботою всіх підсистем системи захисту ОКІ і боротьби з БПЛА і КР на підставі розпізнавання та класифікації БПЛА і КР.

Функцією виконавчої підсистеми є безпосереднє ураження або протидія БПЛА і КР.

Функцією підсистеми забезпечення є забезпечення всіх підсистем енергоживленням, контролем функціонування, обслуговування та ремонтом.

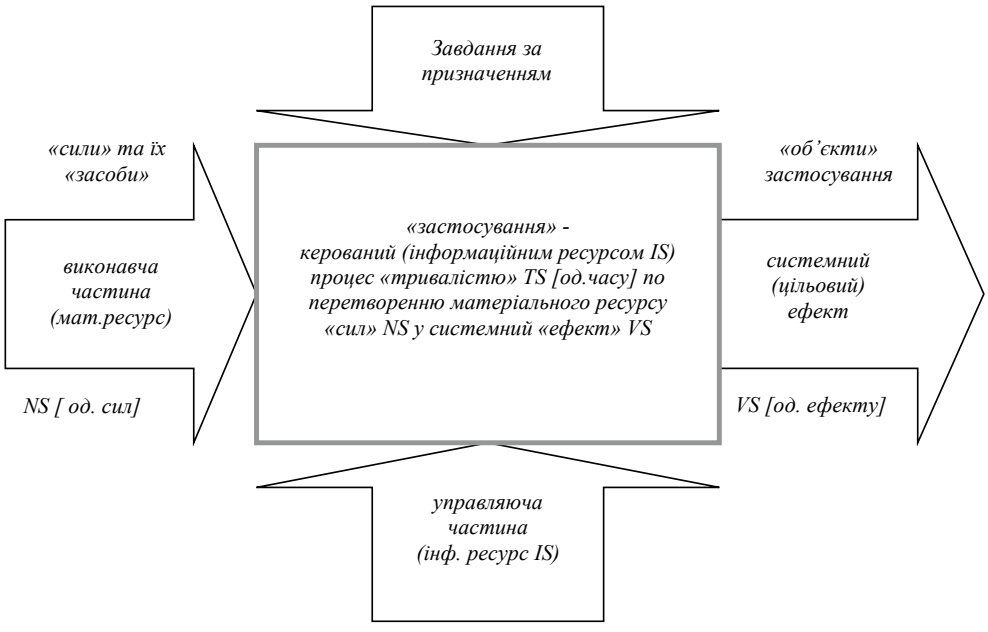

Рис. 2. Концептуальна модель «функції складної системи»

В різних варіантах системи боротьби з БПЛА і КР функції перелічених підсистем можуть бути обмежені або частково відсутні.

Зрозуміло, що кожна з наведених підсистем повинна працювати належним чином, з відповідною ефективністю. Їх розробка та виготовлення потребують певного фінансування та визначають кінцеву вартість всієї складної системи. Таким чином, виникає потреба оцінки ефективності складної системи захисту ОКІ і боротьби з БПЛА і КР, шляхом оцінки ефективності роботи складових підсистем з оцінкою їх вартісних показників.

У таблиці 1 запропоновані критерії оцінки ефективності роботи наведених підсистем у системі захисту ОКІ і боротьби з БПЛА і КР (варіант).

Таблиця 1

Цільові (часткові) критерії оцінки ефективності роботи наведених підсистем у системі захисту ОКІ і боротьби з БПЛА і КР

Інформаційна підсистема	
Критерії оцінки	**Рівень оцінки**
1. Просторово-часові характеристики:	
1.1. Ефективна дальність виявлення. 1.2. Час виявлення. 1.3.Кут огляду по координаті X. 1.4. Кут огляду по координаті Y. 1.5.Час огляду по координаті X. 1.6. Час огляду по координаті Y.	1.1: 0 – дальність менше 100 м; 1 – дальність більше 100 м. 1.2: 0 – час більше 3 сек.; 1 – час менше 3 сек. 1.3: 0 – кут менше 90^0 1 – кут більше 90^0 1.4: 0 – кут менше 90^0 1 – кут більше 90^0 1.5: 0 – час огляду більше 1 сек. 1 – час огляду менше 1 сек. 1.6: 0 – час огляду більше 1 сек. 1 – час огляду менше 1 сек.
2. Електромагнітна сумісність (ЕМС)	
–	0 – несумісність в зоні бойових дій; 0,5 – несумісність у зоні до 50 м; 1,0 – повна сумісність.
3. Універсальність використання:	
3.1.Діапазон зовнішніх чинників, що впливають, при яких забезпечується стійка робота: 3.1.1. вітер 3.1.2. температура 3.1.3. вологість 3.1.4. Складна фонова та цільова обстановка 3.2.Можливість використання для протидії БПЛА І КР іншого виду базування (наземного, морського).	3.1: 3.1.1 – 3.1.3: 0 – мінімальне значення; 1,0 – максимальне значення. 3.1.4: 0 – відсутність селекції на складному фоні; 0,9 – здатність розрізняти бойові БПЛА І КР на складному фоні; 1,0 – здатність розрізняти БПЛА І КР типу «камікадзе» на складному фоні. 3.2: 0 – неможливо; 0,5 – із середнім за технічною складністю і вартістю доопрацювання; 1,0 – можливо без доопрацювання.
4. Наявність функції розпізнавання типу БПЛА і КР:	
4.1. Селекція на фоні птахів. 4.2. Ефективна площа розсіювання БПЛА І КР, що виявляється у автоматичному або автоматизованому режимі. 4.3. Розпізнавання типу БПЛА І КР (важкий, середній, легкий, міні, мікро, або за іншою ознакою).	4.1: 0 – відсутність селекції; 1,0 селекція є. 4,2., 4,3: 0 – більше 1,0 $м^2$ 0,1 – більше 0,1 $м^2$ 0,3 – більше 0,01 $м^2$ 0,5 – більше 0,005 $м^2$ 1,0 – більше 0,001 $м^2$

Продовження таблиці 1

Інформаційна підсистема	
Критерії оцінки	**Рівень оцінки**
Керуюча підсистема	
5. Ступінь автоматизації роботи:	
5.1. Необхідна кількість операторів для протидії БПЛА І КР (від 0 до 1).	5.1: 0 – потрібен оператор; 0,2 – автоматизація роботи в одному з режимів; 0,4 – автоматизація в режимі виявлення і супроводу; 0,6 – автоматизація в режимі виявлення і супровадження; 0,8 – автоматизація у режимах виявлення, супроводу і ураження під контролем операторів; 1,0 – повністю автоматична робота.
5.2. Наявність розпізнавання і класифікації цілей (від 0 до 1).	5.2: 0,8 – глибока автоматизація розпізнавання та класифікації у всій зоні виявлення; 1,0 – автоматичне розпізнавання і класифікація у всій зоні виявлення.
Виконавча підсистема	
6. Зниження ефективності виконання цільового завдання БПЛА і КР від засобів ураження та протидії:	
6.1. Артилерійський канал. 6.2 Ракетний канал. 6.3 Спеціальний БПЛА І КР. 6.4 Оптичні пастки. 6.5 РЕБ , ОЕП з порушення управління. 6.6 Макети об'єкту прикриття. 6.7 Засоби маскування. 6.8 Перехоплення управління.	0 – гарантоване виконання цільового завдання; 1,0 – спосіб самозахисту неефективний.
Підсистема забезпечення	
Наявність автономного електрозабезпечення. Наявність самодіагностики (функціонального контролю). Наявність ремкомплекту. Наявність технічного обслуговування.	0 – нема у наявності; 1,0 – є в наявності. .

Кожен цільовий критерій, що наведений у таблиці, нормований та знаходиться в межах від 0 до 1.

Ефективність кожної з наведених j-тих (в даному випадку j-1,4) підсистем $E_j(i)$ можна оцінити шляхом згортки всіх їх цільових (часткових) і-тих критеріїв:

$$E_j(i) = \prod_{i=1}^{M} k_i^{c_i} = k_1^{c_1} \times k_2^{c_2} \times \ldots \times k_M^{c_M}, \qquad (1)$$

де $k_1, \ldots, k_M$ – цільові (часткові) критерії ефективності виконання своїх функцій кожної з підсистем;

$C_1, \ldots, C_M$ – вагові коефіцієнти цільових (часткових) критеріїв ефективності, $\sum_{i=1}^{M} C_i = 1$;

M – кількість часткових показників ефективності.

Послідовність (етапи) вибору функції згортки наступна:

1. Обґрунтування допустимості згортки – критерії, що згортаємо, повинні бути однорідними.

2. Нормалізація критеріїв – критерії, що згортаємо, повинні бути нормалізовані. У задачах, де локальні критерії мають різні одиниці вимірювання, необхідно привести критерії до єдиного, бажано безрозмірного, масштабу вимірювання.

3. Врахування пріоритетів критеріїв – формування вагових коефіцієнтів, які відображають важливість критерія.

4. Побудова функції згортки.

Для згортання критеріїв використовують такі функції:

адитивна згортка;

мультиплікативна згортка;

агрегування та інші операції.

Вагові коефіцієнти C_i цільових (часткових) критеріїв ефективності зазвичай визначаються методом експертних оцінок (і тільки при неможливості проведення експертного опитування, ваги усіх часткових критеріїв приймаються рівноваговими $C_i = 1 / M$).

Визначимо суперкритерій ефективність-вартість оцінки всієї системи захисту ОКІ і боротьби з БПЛА і КР.

Вважається, що «ефективністю» є спроможність системи утворювати системний ефект, але така спроможність має кількісну міру. Таким чином,

об'єктивно існує безпосередній зв'язок між рівнем системного ефекту *VS* і витратами *RS* потенціалу здатності сил на його утворення (які дорівнюють «трудовитратам» сил *NS* за час їх застосування *TS* за дією управління використанням інформаційного ресурсу *IS*). Очевидний характер такого зв'язку в системах матеріальної природи – це «пряма» залежність ефекту від витрат, тому вважаємо, що аксіоматично справедливо –

$$VS(IS) = ES \times RS(IS) = ES \times \{NS(IS) \times TS(IS)\}. \quad (2)$$

Тому коефіцієнт «перетворення» *ES*, який має фізичний зміст продуктивності витрат потенціалу здатності (ресурсів) по створенню ефекту, є загальною мірою «досконалості» системи (тобто її «доцільності» як пристосованості до використання за призначенням) і служить об'єктивною оцінкою ефективності системи в акті застосування; він дорівнює, як то витікає із (2) –

$$ES = \frac{VS(IS)}{RS(IS)} = \frac{VS(IS)}{\{NS(IS) \times TS(IS)\}}. \quad (3)$$

Підкреслимо, що загальносистемна характеристика «ефективність» є фундаментальною для «складної» системи, оскільки визначається загально-системними «зовнішніми» показниками (системним ефектом *VS,* складом сил *NS,* часом застосування *TS)*, що пов'язані з кінцевим результатом акту застосування системи і тому залежать від усіх «внутрішніх» факторів – системних ознак.

Інформаційний ресурс СС, що містить дані про стан матеріальних ресурсів та умови акту застосування системи, інформаційні технології та засоби інформатизації управління, дозволяє сформувати план *X* розподілу «засобів» по об'єктах застосування, план розподілу сил по заходах процесу застосування та план (сценарій) дій *D* «сил» по реалізації планів *X,Y* розподілу, які складають зміст «організаційного управління» і саме якість котрих визначає ефективність системи.

Для кількісної оцінки системної ефективності *ES* потрібне обчислення значення функціонала –

$$ES(VS, NS, TS) = \frac{VS\{BS(X)\}}{NS(Y,D) \times TS(Y,D)}, \quad (4)$$

де $\boldsymbol{X}$ – «план» розподілу засобів ***BS*** по об'єктах застосування;

$\boldsymbol{Y}$ – «план» розподілу сил ***NS*** по завданнях процесу застосування для реалізації плану розподілу засобів ***X*;**

$\boldsymbol{D}$ – «план» (сценарій) дій сил у часі ***T*S** по виконанню завдань щодо застосування засобів.

Принцип «максимуму системної ефективності» системного підходу, безумовно, є фундаментальним критерієм оптимальності «рішень» щодо створення, застосування і розвитку СС.

Будемо вважати, що ефективність технічної системи (*ТС*) безпеки ОКІ і ведення боротьби з БПЛА І КР $E_{ТС}^{захисту}$ повинна бути не гірше припустимої $E_{ТС\ прип.}^{захисту}$, значення якої забезпечує збереження функціональності об'єкта захисту – ОКІ, при мінімумі витрат ресурсів:

$$E_{ТС}^{захисту} \geq E_{ТС\ прип.}^{захисту},\ при\quad C_{ТС}^{захисту} \to C_{ТС\ min}^{захисту} \quad (5)$$

де $C_{ТС}^{захист}$ – ціна технічного рішення захисту;

$C_{ТС\ min}^{захисту}$ – припустима ціна технічного рішення захисту.

З'ясування припустимого рівня ефективності технічних рішень захисту ОКІ і ведення боротьби з БПЛА і КР залежить від ступеня збереження функціональності об'єкта КІ. Зрозуміло, що можливі пошкодження об'єкта КІ повинні бути мінімальними або зовсім відсутніми. Звідси є логічним при відсутності будь-яких пошкоджень об'єкта КІ прийняти рівень ефективності технічних рішень біля одиниці. Але зрозуміло, що такий варіант передбачає реалізацію дуже вартісного технічного рішення, реалізація якого вкрай складна і недоцільна. Тому доцільно у якості припустимого рівня ефективності технічних рішень вибрати рівень по методу Фібоначчі або золотого перетину – 0,62. Такий рівень забезпечує виживання об'єкту КІ, можливість до подальшого виконання задач за призначенням та прийнятну вартість системи безпеки КІ і захисту від БПЛА і КР.

Ефективність технічної системи безпеки ОКІ і боротьби з БПЛА і КР $E_{ТС}^{захисту}$ є результатом згортки часткових критеріїв **ефективності** виконання своїх функцій складовими *j* підсистемами.

Всі вище наведені критерії підсистем є взаємопов'язаними, однорідними, лінійними, нормалізованими, позитивними, потенційно мають різні пріоритети, та відносяться до групи результативних. Тому для формування загального критерію (суперкритерію) може бути застосована за аналогією мультиплікативна згортка у вигляді критерію ефективності (1).

Виходячи з цього, ефективність технічної системи безпеки ОКІ і боротьби з БПЛА І КР (протидії) можна оцінити як результат (або рівень) функціонування всіх чотирьох підсистем, який прагне до максимального значення, за формулою:

$$E_{ТС}^{захисту} = E_j(i) = E_1^{B1} \times E_2^{B2} \times E_3^{B3} \times E_4^{B4} \to max, \quad (6)$$

де $E_1^{B1}, E_2^{B2}, E_3^{B3}, E_4^{B4}$ – відповідно, ефективності інформаційної, керуючої, виконавчої підсистем та підсистеми ресурсного забезпечення;

$B_1, .., B_4$ – вагові коефіцієнти критеріїв ефективності інформаційної, керуючої, виконавчої підсистем та підсистеми ресурсного забезпечення,

$$\sum_{j=1}^{4} B_j = 1.$$

Вагові коефіцієнти B_j цільових (часткових) критеріїв ефективності наведених підсистем зазвичай визначаються методом експертних оцінок (і тільки при неможливості проведення експертного опитування, ваги усіх часткових критеріїв приймаються рівновагими $B_j = 1 / 4$).

Таким чином, кожна з чотирьох підсистем, що входять до складу технічної системи безпеки ОКІ і боротьби з БПЛА і КР, вносить свій внесок у ефективність цієї системи. Як слідує з аналізу виразу (6) критерії ефективності кожної з підсистем повинні бути досить високими. Інакше ефективність функціонування системи буде низькою.

За результатами оцінки ефективності способів протидії БПЛА і КР доцільно подальше порівняння способів за критерієм «ефективність – вартість».

Авторами запропонована шкала оцінки ефективності системи безпеки ОКІ і боротьби з БПЛА і КР, що наведена у таблиці 1.

Встановивши припустимі рівні ефективності системи безпеки ОКІ і протидії БПЛА і КР можна визначити оптимальні критерії прийняття рішень вибору способів протидії БПЛА і КР (2): ефективність системи безпеки ОКІ і боротьби з БПЛА і КР (протидії) повинна бути більшою за припустиму, при мінімумі витрат ресурсів.

Оцінка ефективності існуючих та перспективних систем безпеки ОКІ і боротьби з БПЛА і КР та її результати виходять за рамки цієї публікації та будуть наведені у наступній публікації.

Висновки. Засоби боротьби та протидії з БПЛА і КР доцільно розглядати з системних позицій. В роботі розроблена модель оцінювання безпеки критичної інфраструктури на основі комплексу засобів захисту її об'єктів від БПЛА і крилатих ракет.

Таблиця 2

Шкала оцінки ефективності системи боротьби з БПЛА і КР

Рівень ефективності	Значення показника
Дуже ефективна	$E_{ТС}^{захисту} \geq 0,8$
Ефективна	$0,8 > E_{ТС}^{захисту} \geq 0,6$
Недостатньо ефективна	$0,6 > E_{ТС}^{захисту} \geq 0,4$
Неефективна	$0,4 > E_{ТС}^{захисту} \geq 0,2$
Дуже неефективна	$E_{ТС}^{захисту} < 0,2$

1. Запропонована в моделі система критеріїв дозволяє:

детально дослідити ефективність роботи основних підсистем системи безпеки ОКІ і боротьби з БПЛА і КР;

проводити кількісну оцінку ефективності способів боротьби та протидії БПЛА і КР на рівні підсистем та складної системи в цілому;

виконувати порівняння між собою різних реалізацій одного або декількох способів боротьби з БПЛА і КР;

виявляти найбільш ефективні способи боротьби та протидії в різних умовах обстановки та кліматичних умовах.

2. Оцінка використання декількох способів протидії зводиться до формування єдиного критерія шляхом згортки цільових критеріїв кожної з підсистем.

3. Результати оцінки ефективності існуючих та перспективних систем безпеки ОКІ і боротьби з БПЛА і КР будуть наведені у наступній публікації.

Список літератури:

1. Ерёмин Г. В., Гаврилов А. Д., Назарчук И. И., Организация системы борьбы с малоразмерными БПЛА «Арсенал Отечества» № 6(14) за 2014 г. [Електронний ресурс]. – Доступний https://arsenal-otechestva.ru/article/389-antidrone

2. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 1. Беспилотный летательный апарат как объект обнаружения и поражения. Системы управления, связи и безопасности, № 1, 2020. С. 109–145. [Електронний ресурс]. – Доступний http://sccs.intelgr.com/archive/2020-01/05-Makarenko.pdf

3. Слободян М.Г., Можаева Е.И., Подстригаев А.С. Способы и средства противодействия беспилотным летательным аппаратам // Современные проблемы радиоэлектроники: сборник научных трудов. – Красноярск: Сибирский федеральный университет, 2018. С. 46–50.

4. Семенец В.О., Трухин М.П. Способы противодействия беспилотным летательным аппаратам // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 3. С. 4–12.

5. Теодорович Н.Н., Строганова С.М., Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет журнал «Науковедение». 2017. Т. 9. № 1. URL: http://naukovedenie.ru/PDF/13TVN117.pdf

6. Cang Liang, Ning Cao, Xiaokai Lu, Youjie Ye. UAV Detection Using Continuous Wave Radar // 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), 28-30 Sept. 2018, Singapore. DOI:10.1109/ICICSP.2018.8549736

7. Sineglazov V.M. Complex structure of UAVs detection and identification // Electronics and Control Systems, 2015, no. 3 (45), C. 28–32.

8. Igor Korobiichuk, Yuriy Danik, Oleksyj Samchyshyn The estimation algorithm of operative capabilities of complex countermeasures to resist UAVs // Simulation: Transactions of the Society for Modeling and Simulation Innternational, 7 August 2018, vol. 95, pp. 569–573. DOI: 10.1177/0037549718791264.

9. Ергунов В.О., Ильин В.О., Некрасов М.И., Сосунов В.Г. Анализ способов противодействия беспилотным летательным аппаратам для обеспечения безопасности защищаемых объектов // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 1-2 (115-116). С. 51–58.

10. Todd Humphreys. Statement on the security threat posed by unmanned aerial systems and possible countermeasures, Radionavigation Laboratory, The University of Texas at Austin, 2015. URL: https://radionavlab.ae.utexas.edu/images/stories/files/papers/statement-humphreys-20150318.pdf

11. Теодорович Н.Н., Строганова С.М., Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет журнал «Науковедение». 2017. Т. 9. № 1. URL: http://naukovedenie.ru/PDF/13TVN117.pdf

12. Dinesh Sathyamoorthy. A review of security threats of unmanned aerial vehicles and mitigation steps // ResearchGate, 2015, available at: https://www.researchgate.net/publication/282443666_A_Review_of_Security_Threats_of_Unmanned_Aerial_Vehicles_and_Mitigation_Steps.

13. Кузнецов В.Е., Волков Ю.А. Анализ методов противодействия малоразмерным беспилотным летательным аппаратам // Вопросы радиоэлектроники. 2016. № 12. С. 81–87.

14. Корченко А.Г., Ильяш О.С. Обобщенная классификация беспилотных летательных аппаратов // Збірник наукових праць Харківського національного університету Повітряних Сил. 2012. № 4(33). С. 27–36.

15. Каримов А.Х. Цели и задачи, решаемые беспилотными авиационными комплексами нового поколения // Труды МАИ. 2011. № 47. URL: http://trudymai.ru/published.php?ID=26767

16. Nickolay L. Georgiev, Venstislav I. Pehlivanski, Ognyan G. Todorov. Indicators on the Effectiveness of Radio-Electronic Counteraction against Unmanned Aerial Vehicles // NDT Days, 2018, vol. 1, issue.1, pp. 126–131.

17. Подстригаев А.С.1, Слободян М.Г., Можаева Е.И. Система критериев для оценки эффективности способов противодействия беспилотным летательным аппаратам http://trudymai.ru/upload/iblock/d1b/Podstrigaev_Slobodyan_Mozhaeva_rus.pdf

18. Педченко Г.М., Невольніченко А.І., Шарий В.І. Воєнно-наукове забезпечення операцій військ (сил). Монографія. МО України. Видання ВІ КНУ ім.. Тараса Шевченка, 2011.

19. Так виглядає покриття України системами ППО NASAMS 2 та IRIS-T SLM. ITnews. URL: http://itnews.com.ua/news/96246-tak-viglyadaye-pokrittya-ukrayini-sistemami-ppo-nasams-2-ta-iris-t-slm (дата звернення: 18.01.2023).

Chumachenko S.M., Kutovoi O.P., Popel V.A., Guida O.G., Zaika N.V., Murasov R.K.

SCIENTIFIC-METHODICAL APPROACH REGARDING CRITICAL INFRASTRUCTURE SECURITY ASSESSMENT ON THE BASIS OF THE COMPLEX OF TOOLS FOR THE PROTECTION OF ITS FACILITIES FROM UNMANNED AERIAL VEHICLES AND CRUISE MISSILES

Analysis of known approaches to assessing the assurance levels of critical infrastructure objects and processing risks, associated with the use of unmanned aerial vehicles and cruise missiles by terrorists and the enemy, including the use of modern anti-aircraft missile and anti-aircraft artillery weapons, electronic warfare systems shows that assessments of such risks do not always have the required accuracy. Risk measurement problems are related among other things, to the specifics of the weapons used, including cruise missiles and drones.

Among the determining factors that lead to errors in the assessment of these risks, which can be identified as a problem of the effective operation of defense complexes and the protection of critical infrastructure, is the solution to the problem of timely detection of drones and cruise missiles and their quality escorting.

The problems of detecting and recognizing targets are caused by their small size and mass-dimensional characteristics, which makes it difficult to detect them even at short distances. This applies to both radar and optical-electronic means of reconnaissance. In addition, the target detection process itself depends on the degree of its automation. The process of defeating targets depends on the accuracy of the intelligence coordinates provided to the means of destruction, the accuracy of aiming of these means and their tactical and technical characteristics.

Thus, there is a problem of creating such means of combating unmanned aerial vehicles that interact and work well at all stages - from identifying targets to their destruction.

In order to achieve the necessary defense results (which in the risk model corresponds to the accuracy of risk processing), it is advisable to divide the defense system into components and conduct an analysis of the impact of each component included in the system from the means of combating unmanned aerial vehicles.

It is proposed to consider four main subsystems, such as informational, control, executive subsystem and support subsystem. Each of the subsystems is determined by a set of indicators and evaluation criteria. The contribution of each of the subsystems makes it possible to evaluate the effectiveness of the entire complex of means of protection of critical infrastructure as a whole.

It is proposed to consider a model for evaluating the effectiveness of the complex of means of protecting critical infrastructure objects and combating drones and cruise missiles, which evaluates the effectiveness of the main components of the complex of means. It is proposed to carry out an assessment based on the efficiency-cost criterion, which will help to make informed decisions regarding the construction of optimal schemes for the protection of critical infrastructure and the fight against drones and cruise missiles based on the available forces and means.

Key words: *critical infrastructure, efficiency, level of efficiency, unmanned aerial vehicle, cruise missile, anti-aircraft missile complex, anti-aircraft artillery complex, radar station, electronic warfare, criterion, weighting factor.*