УДК 351.862.4:342.951:351.85:340.134
DOI https://doi.org/10.32782/2663-5941/2023.2.1/41

Чумаченко С.М.
Національний університет харчових технологій

Кутовий О.П.
Центр воєнно-стратегічних досліджень
Національного університету оборони України імені Івана Черняхівського

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

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

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

КОМПЛЕКСНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ РІВНЯ БЕЗПЕКИ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ІНТЕГРАЛЬНОЇ СИСТЕМИ ЗАХИСТУ ЇЇ ОБ'ЄКТІВ ВІД БПЛА ТА КРИЛАТИХ І БАЛІСТИЧНИХ РАКЕТ

В роботі проведено аналіз відомих підходів експертного оцінювання рівнів безпеки, пов'язаних із застосуванням безпілотних літальних апаратів для розвідки, крилатих і балістичних ракет для ураження об'єктів критичної енергетичної інфраструктури пошкодження та віддаленої кібератаки по ним.

Безпека і захист критичної енергетичної інфраструктури займають сьогодні ключове місце в системі національної безпеки і оборони України у зв'язку з масованими атаками на неї російського агресора. В першу чергу, це пов'язане із ключовим значенням енергетики і її визначальним впливом на загальний рівень безпеки всієї критичної інфраструктури (КІ)

В умовах сучасної науково-технічної революції у військовій сфері, що активно продовжується з першої половини 3-го тисячоліття, все більшого значення набуває пошук ефективних засобів протиборства з більш оснащеним в технічному плані супротивником, який широко використовує новітні інформаційні технології для атак на об'єкти критичної енергетичної інфраструктури. Враховуючи досвід гібридних війн в Іраку, Югославії, Сирії і Україні, характерним є застосування засобів повітряного нападу із бомбардувальної авіації (стратегічної й фронтової), корабельних (надводних і підводних) та наземних систем базування, що знаходяться поза зоною можливого ураження.

До чинників, що призводить до похибок оцінки цих загроз, є вирішення задачі своєчасного виявлення повітряних засобів нападу та постановки їм перешкод. Проблеми виявлення та розпізнавання цілей обумовлені їх малими масо-габаритними характеристиками, що ускладнює їх виявлення навіть на невеликих відстанях. Це стосується як радіолокаційних так і оптико-електронних засобів розвідки. Крім того, сам процес виявлення цілей залежить від ступеню його автоматизації. Процес ураження цілей залежить від точності наданих координат засобам ураження та їх тактико-технічних характеристик щодо точності прицілювання.

Пропонується розглянути інформаційну модель оцінки ефективності комплексу засобів захисту об'єктів критичної інфраструктури за критерієм ефективність-вартість, що допоможе приймати обґрунтовані рішення щодо побудови оптимальних схем захисту критичної інфраструктури і боротьби з повітряними засобами ураження критичної енергетичної інфраструктури.

Ключові слова: *критична інфраструктура, ефективність, рівень ефективності, безпілотний літальний апарат, радіолокаційна станція, радіоелектронна боротьба, критерій, ваговий коефіцієнт.*

Постановка проблеми. Застосування крилатих і балістичних ракет призводить до різкого росту загрози безповоротного ураження об'єктів критичної енергетичної інфраструктури (ОКЕІ), основні елементи якої є критично важливими для забезпечення життєдіяльності населення та об'єктів оборонно-промислового комплексу в Україні (див. рис. 1).

Ще один із засобів ураження представляє собою безпілотні літальні апарати (БПЛА), або дрони, які є досить новими видами озброєнь на полі бою. Починаючи з 1980-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 дронів-«камікадзе», які відрізняються за розмірами та цільовим навантаженням. Відеокадри, що передають дрони-розвідники, і закладені у їх бортовий комп'ютер алгоритми маневрування та виявлення нових шляхів наближення до цілей, збільшують ризики проведення результативної атаки по ОКЕІ та їх ураження. Застосування групи дронів прикриття та ретрансляторів збільшує небезпечну зону віддаленої атаки.

Аналіз останніх досліджень і публікацій. Аналіз публікацій за напрямом протидії крилатим, балістичним ракетам і БПЛА показує, що наукових статей з даної тематики на сьогодні досить багато. У переважній більшості робіт в цій сфері переважають надмірно оптимістичні висновки щодо успішності ураження всіх їх видів сучасними засобами ППО та РЕБ [1-3]. Разом з тим, різке та різноманітне вторгнення цих засобів ураження КІ 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. Тільки одиниці держав світу мають частково в наявності та розвивають засоби, які спроможні достатньо ефективно протидіяти застосуванню сучасних БПЛА.

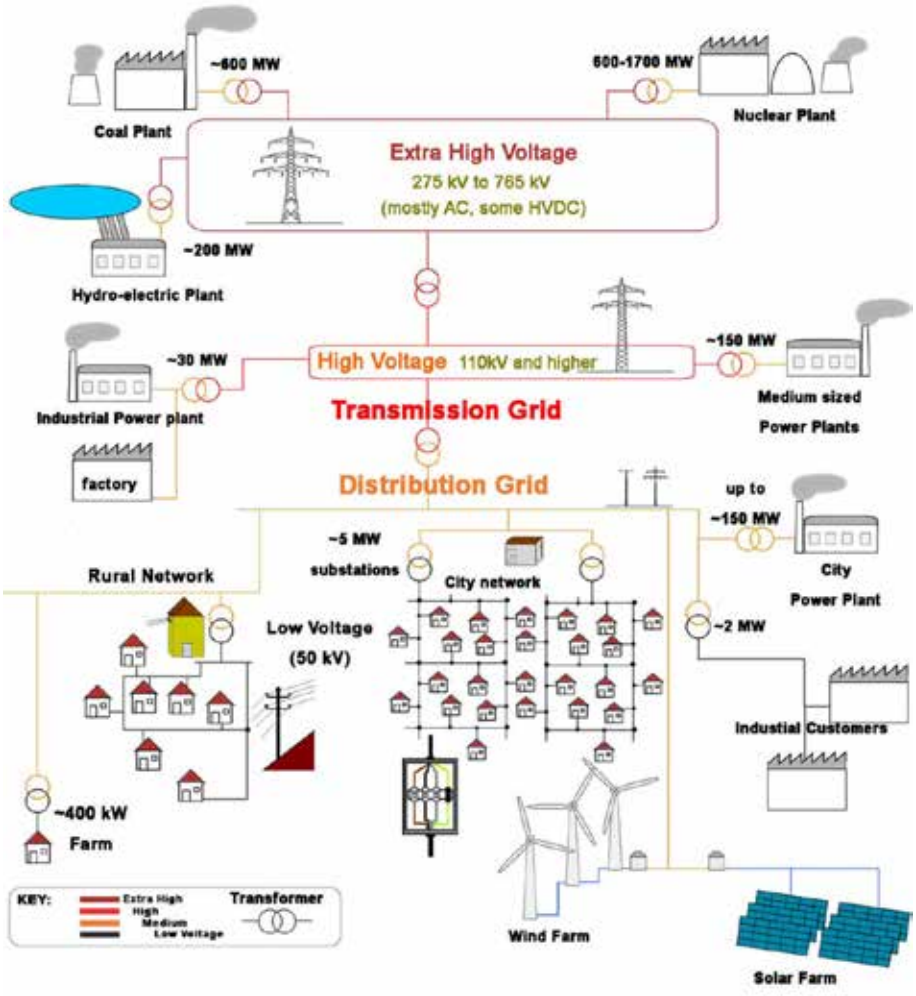

Рис. 1. Схема розподілення мережі та об'єднання об'єктів критичної енергетичної інфраструктури

Встає питання у об'єктивному порівнянні ефективності технічних рішень щодо захисту КІ і боротьби з сучасними та перспективними БПЛА, крилатими і балістичними ракетами з обґрунтуванням їх ефективності.

Поява нових видів ураження КІ, серед яких слід окремо виділити БПЛА та їх застосування в останніх воєнних конфліктах, виявили суттєві недоліки зенітно-ракетних комплексів (ЗРК), що стоять на озброєнні в різних країнах світу. Аналіз характеристик ЗРК протиповітряної оборони (ППО) провідних країн світу показує, що багато різноманітних заявлених комплексів ППО нібито здатні вражати як БПЛА, так і крилаті ракети «повітря-земля», балістичні ракети, літаки, вертольоти. Однак, треба усвідомлювати, що боротьба з БПЛА різних класів суттєво відрізняється. Так, дійсно БПЛА великих та середніх розмірів (типу Predator и Reaper від General Atomics) виявляються, супроводжуються та вражаються з досить високою ефективністю, а з БПЛА малих розмірів виникають суттєві проблеми. В [2] відмічається, що для виявлення малорозмірних БПЛА необхідно застосовувати спеціалізовані засоби розвідки, що мають кращі можливості виявлення та супроводження малорозмірних БПЛА, створювати спеціалізовані канали першочергової передачі розвідувальної інформації про їх дії.

Як правило, для протидії крилатим ракетам та дронам-камікадзе, перспективними є способи впливу на використання високотехнологічних інформаційних систем визначення навігаційних параметрів космічного базування і зокрема Глобальних Систем Позиціонування (ГСП) (GPS/GLONASS), супутникові угрупування яких були розгорнуті США і Росією.

Бойові дії в зоні Перської затоки спочатку показали високі експлуатаційні характеристики ГСП. Однак, у ході конфлікту в Іраку на території останнього було встановлено кілька достатньо потужних передавачів для постановки перешкод системі GPS. Внаслідок їх дії в перші три дні конфлікту за наявними даними коаліційні сили втратили значну кількість крилатих ракет. Після визначення причин зниження ефективності ураження обстріли було припинено. Розташування передавачів було встановлено, передавачі було знищено, що дозволило продовжувати бойові дії з високою ефективністю.

Принциповою особливістю ГСП є їхня слабкість до активних перешкод. Це чітко фізично обумовлено трьома чинниками [3]:

– великою дальністю передачі сигналів (~20 000 км);

– обмеженою потужністю радіосигналу супутника (10...50 Вт);

– малим коефіцієнтом посилення антени супутникового передавача (що зазвичай не перевищує 10–15 дБ) [5].

Мета статті – дослідження науково-методичного апарату для оцінювання ефективності системи захисту ОКІ від БПЛА та проведення техніко-економічного аналізу запропонованих технічних рішень ведення боротьби з ними за критерієм ефективність-вартість.

Викладення основного матеріалу. Кожна технічна система (комплекс) захисту ОКЕІ й боротьби з БПЛА, як складна система, повинна мати у своєму складі ряд технічних складових (підсистем), поєднаних у єдине ціле.

Кожна складна система складається з підсистем, що 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 ОКЕІ і боротьби з БПЛА.

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 ОКЕІ і боротьби з БПЛА шляхом оцінки ефективності роботи складових підсистем з оцінкою їх вартісних показників. Вважається, що «ефективністю» є спроможність системи утворювати системний ефект, але така спроможність має кількісну міру. Виходячи з цього, ефективність технічної системи безпеки ОКЕІ і боротьби з БПЛА (протидії) можна оцінити як результат (або рівень) функціонування всіх чотирьох підсистем, який прагне до максимального значення, за формулою:

$$E_{TC}^{захисту} = E_j(i) = E_1^{B1} \times E_2^{B2} \times E_3^{B3} \times E_4^{B4} \to max, \quad (1)$$

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 експертним шляхом

з використанням методу аналізу ієрархій Сааті або методу аналітичних мереж [6, 7] (і тільки при неможливості проведення експертного опитування, ваги усіх часткових критеріїв приймаються рівновагими $B_j = 1/4$).

За результатами оцінки ефективності способів протидії БПЛА доцільним є подальше порівняння способів за критерієм «ефективність – вартість». Оцінка використання декількох способів протидії зводиться до формування єдиного критерію шляхом згортки цільових критеріїв кожної з підсистем.

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

Таблиця 1

Шкала оцінки ефективності системи боротьби з БПЛА і КР

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

Оцінка необхідної потужності передавача перешкод

Приймальний пристрій GPS перекривається сигналом перешкоди в тому випадку, якщо відношення потужності перешкоди, що потрапляє на вхід приймача, до потужності корисного сигналу, що надходить від супутників не менше деякої величини, яка називається коефіцієнтом придушення (Кп), характерного для даної перешкоди та конкретного типу приймача GPS. Інакше висловлюючись, перешкода ефективна, якщо виконується умова

$$\frac{P_{п\,вх}}{P_{с\,вх}} \geq K_п \qquad (1)$$

де $P_{п\,вх}$, $P_{с\,вх}$ – потужність перешкоди та корисного сигналу на вході приймача GPS відповідно.

Коефіцієнт придушення залежить від виду перешкоди та технічних характеристик GPS приймача. Зазвичай для шумової перешкоди приймають $K_п = 0,5...1$. При формуванні хибних кодів для дезінформації роботи приймачів GPS рівень сигналів на вході приймачів повинен бути того ж порядку, що й рівні сигналів, що приймаються від супутників GPS.

Проведемо оцінку необхідної потужності передавача перешкод, що забезпечує виконання умови 1.

Нехай передавач перешкод потужністю $P_{Прд}$ із коефіцієнтом посилення його антени $G_{Прд}$ опромінює приймач з ефективною площею антени $S_{эф\,Прм}$, віддалений від нього на відстань R.

Щільність потужності випромінювання у приймача $П_R$ [Вт/м^2] визначається ставленням потужності $P_{Прд}$ до площі поверхні сфери радіусу, яке має бути збільшено в $G_{Прд}$ разів:

$$П_R = \left(П_{Прд}\,\eta / 4\pi R^2\right) G_{Прд},$$

де η – коефіцієнт втрат серед поширення.

Потужність сигналу перешкоди на вході приймача GPS дорівнюватиме :

$$P_{п\,вх} = П_R\, S_{эф\,Прм} = P_{Прд} G_{Прд} S_{эф\,Прм} \eta / (4\pi R^2). \qquad (2)$$

Використовуючи відоме співвідношення

$$S_{эф\,Прм} = G_{Прм} \lambda^2 / 4\pi$$

де λ – довжина хвилі), отримуємо:

$$P_{п\,вх} = P_{Прд} G_{Прд} G_{Прм} \lambda^2 \eta / (4\pi)^2 R^2. \qquad (3)$$

Враховуючи вирази 1 і 3 знаходимо необхідну потужність передавача перешкоди

$$P_{Прд} = (4\pi)^2 R^2 P_{Прм\ min} K_п / G_{Прд} G_{Прм}\, \theta(\beta,\varepsilon)\, \lambda^2 \eta, \qquad (4)$$

де $P_{Прм\ min}$ – реальна чутливість приймача GPS, $\theta(\beta,\varepsilon)$ – рівень пелюсток діаграми спрямованості антени приймача GPS за якими впливає перешкода.

Для оцінки необхідної потужності передавача перешкод, що забезпечує придушення приймача GPS, задамо значення параметрів, що входять у формулу 4:

$$R = 100 \text{ км}, P_{Прм\ min} = 10^{-12} \text{ Вт}, K_п = 1, G_{Прд} = 500, G_{Прм} = 5;$$

$$\lambda = 19 \text{ см}, 24 \text{ см};\ \eta = 1;\ \theta(\beta,\varepsilon) = 1.$$

Тоді, необхідна потужність передавача перешкод дорівнюватиме $\approx 0,01$ Вт. Даної потужності достатньо для придушення приймача GPS по головному пелюстку діаграми спрямованості ($\theta(\beta,\varepsilon)$=1). Таке придушення можливе у разі розміщення передавача перешкод на борту якогось літального апарату (наприклад БПЛА). У разі впливу на бічні пелюстки потрібна потужність передавача повинна бути збільшена з урахуванням реального рівня бічних пелюсток антени приймача GPS. Реальні значення рівнів бічних пелюсток антен приймачів GPS знаходяться в межах 10^{-2}….10^{-3}. Отже, необхідна потужність передавача перешкод для придушення приймача GPS на відстані до 100 км по бічних пелюстках антени не перевищує 10 Вт.

Для перевірки викладених припущень було реалізовано імітаційну модель автокомпенсатора перешкод, що знаходиться у складі приймача ГСП [4].

Потужність джерел перешкод в імітаційній моделі у 1000 разів перевищує потужність власних шумів автокомпенсатора приймачів ГСП, що

відповідає потужності, що приймається антенами приймачів ГСП від джерела перешкод потужністю 10 Вт і що знаходиться на дальності близько 100 км (коефіцієнт посилення антени передавача перешкод вважали рівним 10 дБ). Модуляція потужності передавача перешкод здійснювалася згідно із законом:

$$P_i(t) = P_o \cdot \left(1 + \cos\left(2 \cdot \pi \cdot f_m \cdot t + \varphi_o\right)\right), \quad (1)$$

де: P_o – задане значення потужності; f_m – частота модуляції перешкоди;

φ_o – початкова фаза перешкоди.

Отримані у [6] результати вказують на те, що використання нової завадостійкої системи супутникової навігації робить ГСП практично невразливою для засобів радіоелектронного придушення (РЕП).

Застосування модуляції сигналів передавачів перешкод з розумно вибраною частотою модуляції значно знижує ефективність роботи автокомпенсаторів приймачів ГСП.

Одночасне використання кількох передавачів перешкод з різних напрямків відносно об'єктів критичної енергетичної інфраструктури (ОКЕІ), навіть у кількості менших ступенів свободи автокомпенсатору приймача ГСП, призводить до зменшення коефіцієнта придушення автокомпенсатора на 20–30 дБ, а застосування взаємнокорельованих перешкод знижує ефективність автокомпенсатора до 7 дБ.

Виграш щодо «сигнал/перешкода+шум» у 5 разів (7дБ) скоротить дальність придушення приймача ГСП у 2,24 рази, тобто для прикладу із 145 км (як вказувалося в [4]) до 64,78 км для 4 Вт передавача.

Можна вважати, що ефективність застосування високоточної зброї по ОКЕІ, на якій є приймачі ГСП, у результаті дії ППО виявиться дуже низькою. Причому сторона, що атакує, може розкрити цей факт тільки після застосування цієї зброї, зазнавши значних матеріальних витрат на ураження ОКЕІ, що представляють собою систему точкових та розподілених об'єктів по всій території України (див. рис. 2).

Приймачі ГСП, що використовуються для навігації в наземних, морських і повітряних бортових інформаційно-управляючих комплексах і військовій техніці теж будуть піддаватися впливу ППП.

Отже, бойове застосування супротивником озброєння і військової техніки яка оснащена приймачами ГСП по ОКЕІ виявиться або під зривом взагалі, що призведе до невиконання бойових завдань, або навіть призведе до аварій, катастроф, внаслідок значних помилок у визначенні реального місцезнаходження.

Вплив ППП практично важко розкрити на фоні значної кількості працюючих передавачів супутників ГСП (десятки) і порівняно невеликої потужності випромінювання самими ППП (одиниці ватів), що робить їх мало помітними, слабко уразливими і несподіваними в застосуванні.

ППП можуть працювати автономно, у складі існуючих зразків озброєння і техніки, існуючих

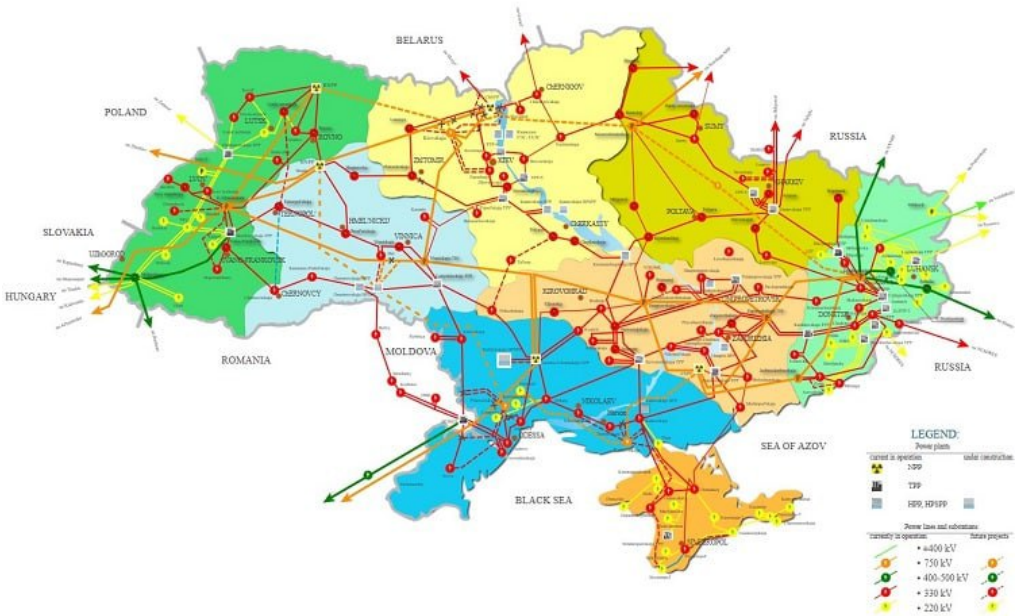

Рис. 2. Об'єкти критичної енергетичної інфраструктури України

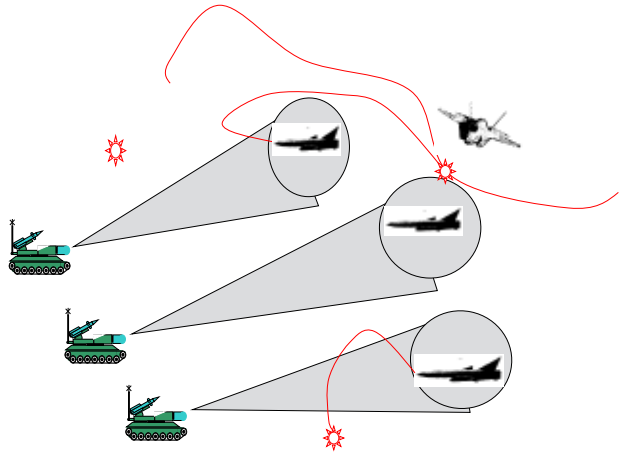

Рис. 3. Придушення роботи приймачів ГСП КР і БПЛА

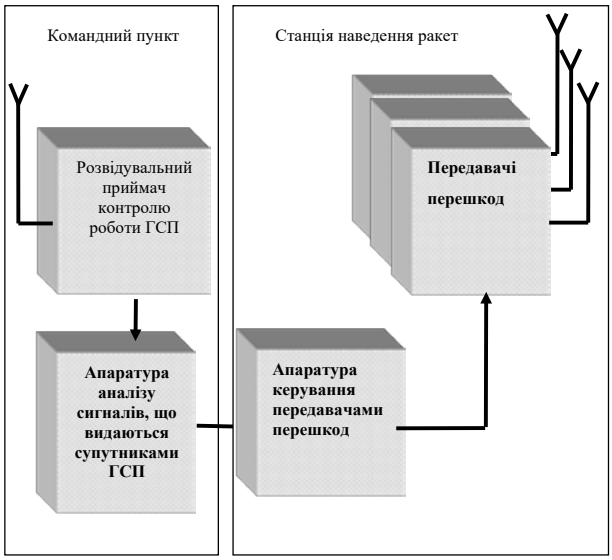

Рис. 4. Структурна схема ТСБ ГСП для ОКЕІ застосування глобальних систем визначення положення

систем озброєння з розвиненою інфраструктурою (наприклад системи ППО) або у складі перспективної **Територіальної Системи Блокування ГСП для ОКЕІ в Україні.** Найбільша ефективність може бути досягнута у випадку їхнього використання в складі **ТСБ** ГСП. У цьому випадку забезпечується детальний аналіз роботи супутників ГСП, вибір оптимальних режимів роботи передавачів перешкод і безпосереднє керування режимами і часом їхньої роботи.

ТСБ ГСП найбільш ефективно може бути інтегрована з системою ППО прикриття ОКЕІ. Можливість такого інтегрування обумовлена наявністю розвинутих підсистем розвідки повітряних цілей та автоматизованого управління в системі озброєння ППО, що забезпечує найбільш швидке реагування на зміни умов повітряної обстановки. При цьому зенітні комплекси ППО, оснащені ППП можуть здійснювати вплив на засоби повітряного нападу ОКЕІ постійно, як поза зонами ураження вогневих засобів, так і в зонах ураження. Зважаючи на невеликі масо-габаритні характеристики ППП, вони можуть бути розташовані безпосередньо на бойових засобах ППО (див. рис. 3) або самостійно шляхом створення безпровідної сенсорної мережі для створення сенсорного поля покриття ОКЕІ (див. рис. 4).

Попередні розрахунки та випробування показали, що одного передавача перешкод потужністю (8–10) Вт достатньо для спрямованого придушення роботи приймачів ГСП на відстанях до **100** км.

Висновки. Засоби боротьби та протидії з БПЛА доцільно розглядати з системних позицій. Кожна з чотирьох підсистем, що входять до складу технічної системи безпеки ОКЕІ і боротьби з БПЛА , вносить свій внесок у ефективність цієї системи, що у свою чергу допомагає виявляти найбільш ефективні способи боротьби та протидії в різних умовах обстановки.

Передавач перешкод повинен формувати декілька типів сигналів, які забезпечать вплив на роботу усіх типів приймачів супутникових навігаційних систем. Склад та характеристики цій сигналів потребують додаткових досліджень.

Вартість територіальної системи блокування роботи Глобальних систем визначення положення (GPS) залежить від її складу, необхідної площі прикриття, кількості і характеристик передавачів.

Список літератури:

1. 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

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

3. Абламейко, С. В. Глобальні навігаційні супутникові системи / С. В. Абламейко, В. А. Саєчніков, А. А. Спиридонів. Мінськ: БДУ, 2011. 147 с. ISBN 978-985-518-538-4.

4. Монзінго, Р. А. Адаптивні антенні решітки: введення в теорію / Р. А. Монзінго, Т. У. Міллер. М.: Радіо та зв'язок, 1986. 448 с.

5. 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.

6. Чумаченко С.М., Троцько В.В. Оцінювання загроз об'єктам критичної інфраструктури. К.: УкрНДІЦЗ. Науковий вісник: Цивільний захист та пожежна безпека. 2017. № 1 (3). С. 41–47.

7. Чумаченко С.М., Мурасов Р.К. Методика оцінювання загроз для потенційно-небезпечних об'єктів критичної інфраструктури в зоні проведення операції об'єднаних сил – Труди університету, № 1(170) 2022, С. 228–243. Інв. 49648.

Chumachenko S.M., Kutovoi O.P., Guida O.G., Popel V.A., Zaika N.V. COMPREHENSIVE APPROACH TO DETERMINING THE LEVEL OF SECURITY OF CRITICAL ENERGY INFRASTRUCTURE BASED ON AN INTEGRATED PROTECTION SYSTEM AGAINST UAV AND GUIDED BALLISTIC MISSILES.

The paper analyzes known approaches to expert assessment of security levels related to the use of unmanned aerial vehicles for reconnaissance, cruise and ballistic missiles for attacking critical energy infrastructure objects, and remote cyber attacks on them.

Today, security and protection of critical energy infrastructure occupy a key place in the system of national security and defense of Ukraine, in connection with the massive attacks on it by the Russian aggressor. This is primarily due to the key importance of energy and its decisive impact on the overall level of security of all critical infrastructure.

In the context of the modern scientific and technological revolution in the military sphere, which has been actively ongoing since the first half of the 3rd millennium, the search for effective means of combating a technically advanced opponent who widely uses new information technologies to attack critical energy infrastructure objects is becoming increasingly important. Taking into account the experience of hybrid wars in Iraq, Yugoslavia, Syria, and Ukraine, the use of air attack means from bombing aviation (strategic and frontline), ship-based (surface and underwater), and ground-based systems located outside the possible impact zone is typical.

Among the factors that lead to errors in assessing these threats is the problem of timely detection of aerial attack vehicles and setting up obstacles for them. Target detection and recognition issues are due to their small size and dimensions, which complicates their detection even at short distances. This applies to both radar and optoelectronic reconnaissance systems. In addition, the target detection process depends on the degree of its automation. The targeting process depends on the accuracy of the coordinates provided to the targeting systems and their tactical and technical characteristics regarding accuracy of aiming.

Proposed is to consider an information model for evaluating the effectiveness of a complex of protection means for critical infrastructure objects based on the effectiveness-cost criterion, which will help make informed decisions regarding the construction of optimal schemes for protecting critical infrastructure and combating air attack means on critical energy infrastructure.

Key words: *critical infrastructure, effectiveness, level of effectiveness, unmanned aerial vehicle, radar station, electronic warfare, criterion, weight coefficient.*