

**KAPITEL 1 / CHAPTER 1<sup>1</sup>****DEVELOPMENT OF THE COMPONENTS OF THE PROTECTION OF CRITICAL ENERGY INFRASTRUCTURE USING THE BLOCKING OF GLOBAL SATELLITE POSITIONING SYSTEMS AND POSSIBLE WAYS OF ITS INTEGRATION WITH THE AIR DEFENSE AND ANTI-MISSILE DEFENSE SYSTEM****DOI: 10.30890/2709-2313.2022-15-01-008****Вступ**

Безпека і захист критичної енергетичної інфраструктури займають сьогодні ключове місце в системі національної безпеки України у зв'язку з масованими атаками на неї російського агресора. В першу чергу, це пов'язано із значенням енергетики і її визначальним впливом на загальний рівень безпеки всієї критичної інфраструктури (КІ) [1, 2, 3].

Забезпечення заходів захисту об'єктів критичної енергетичної інфраструктури пов'язане із застосуванням радіоелектронних систем ПВО і ПРО при протидії масованим атакам крилатих ракет і дронів-камікадзе.

В умовах науково-технічної революції у військовій сфері, що активно продовжується в першій половині 3-го тисячоліття, все більше значення набуває пошук ефективних способів протидії 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 застосуванням бомбардувальної авіації (стратегічної й фронтової), корабельних (надводних і підводних) та наземних систем базування, що знаходяться поза зоною можливого ураження систем ПВО і ПРО.

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

---

<sup>1</sup>*Authors: Kutovoi Oleg, Chumachenko Serhii, Mudrak Yuriy, Popel Valeriy, Zaika Nazar, Murasov Rustam*



## **1.1. Аналіз останніх досліджень і публікацій**

На теперішній час застосування ГСП набуло масового характеру, як для військового так і для цивільного використання з метою визначення географічних координат та параметрів руху [1-6]. В арміях провідних країн світу крім наземного, морського озброєння та авіації приймачами ГСП оснащуються крилаті ракети, авіабомби, безпілотні та дистанційно пілотовані літальні апарати (БПЛА і ДПЛА) та ін. Це забезпечує високу точність вирішення навігаційних задач і задач наведення високоточної зброї на об'єкти ураження.

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.

В період ведення бойових дій багатонаціональних сил НАТО проти Югославії теж були відзначені часті випадки відхилення крилатих ракет і авіабомб від необхідних траєкторій польоту, які наводились з використанням ГСП, що могло бути наслідком застосування з боку Югославії засобів постановки перешкод для роботи приймачам ГСП. Цілком можливо, що в Югославії були випробувані генератори перешкод російського виробництва типу «Краснуха» [1].

У роботі [2] були наведені результати оцінки можливості навмисного впливу на роботу приймачів ГСП, які застосовуються у високоточній повітряній зброї. Була виявлена реальна можливість блокування роботи приймачів ГСП або створення навмисної їхньої дезінформації.

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

Тому щільність потоку потужності сигналу одного навігаційного супутника



на поверхні Землі навіть без урахування втрат мала і знаходиться на рівні (10–13) Вт/м<sup>2</sup>. Очевидно, що створення ефективних перешкод при передачі наземними передавачами на відстанях у (30–150) км від об'єктів критичної енергетичної інфраструктури (ОКЕІ) за такої малої потужності корисного сигналу не є технічною проблемою. Відстань у (30-150) км від ОКЕІ є прийнятною й обумовлена сферичністю Землі, та обмеженнями на висоту підйому антени передавача перешкод.

Наявні мобільні передавачі перешкод GPS на вказаних відстанях з потужностями випромінювання в одиниці-десятки Ватт можуть забезпечити перевищення супутникового сигналу за потужністю на (40-60) дБ навіть за боковими пелюстками променю антени.

Для досягнення стійкого придушення приймачів ГСП в районах біля ОКЕІ у роботі [2] запропоновано створити достатній рівень потужності перешкоди. При виборі просторової змінної слід взяти до уваги низку чинників:

- по-перше, практично встановлено, що в діапазоні частот, що розглядається, придушення ефективно строго в межах відстані прямого бачення ОКЕІ (див. рис.1);

- по-друге, конфігурація територіальної системи блокування (ТСБ) роботи ГСП має бути подібна до побудови системи стільникової зв'язку GSM 900/1800, тобто багатопозиційної з кроком сітки в (10÷30) км на відкритих ділянках місцевості та набагато меншим кроком у горах та населених пунктах (для реалізації ефекту прямого бачення);

- по-третє, питання визначення достатньої потужності сигналу перешкоди одного передавача. Компромісним варіантом доцільно вважати меншу потужність, але більшу кількість передавачів, розподілених на території прикриття ОКЕІ (див. рис.2). Це в свою чергу ускладнить виявлення та знищення елементів ТСБ і вона стає менш уразливою.

## **1.2. Формулювання мети дослідження**

Метою цієї роботи є розгляд перспективних підходів протидії застосуванню засобів ураження повітряного, корабельного та наземного базування проти ОКЕІ за рахунок можливого навмисного впливу на роботу ГСП.



### 1.3. Викладення основного матеріалу дослідження

Потужна і надійна енергетика в країні є головною умовою функціонування усіх її сфер діяльності, а тому стає с найважливішою системою стратегічних об'єктів «відповідальності» для сфери воєнної безпеки країни, а отже складовою критичної інфраструктури. До «систем енергетики» належать «системи енергоносіїв», «системи електроенергетики» та «системи теплоенергетики».

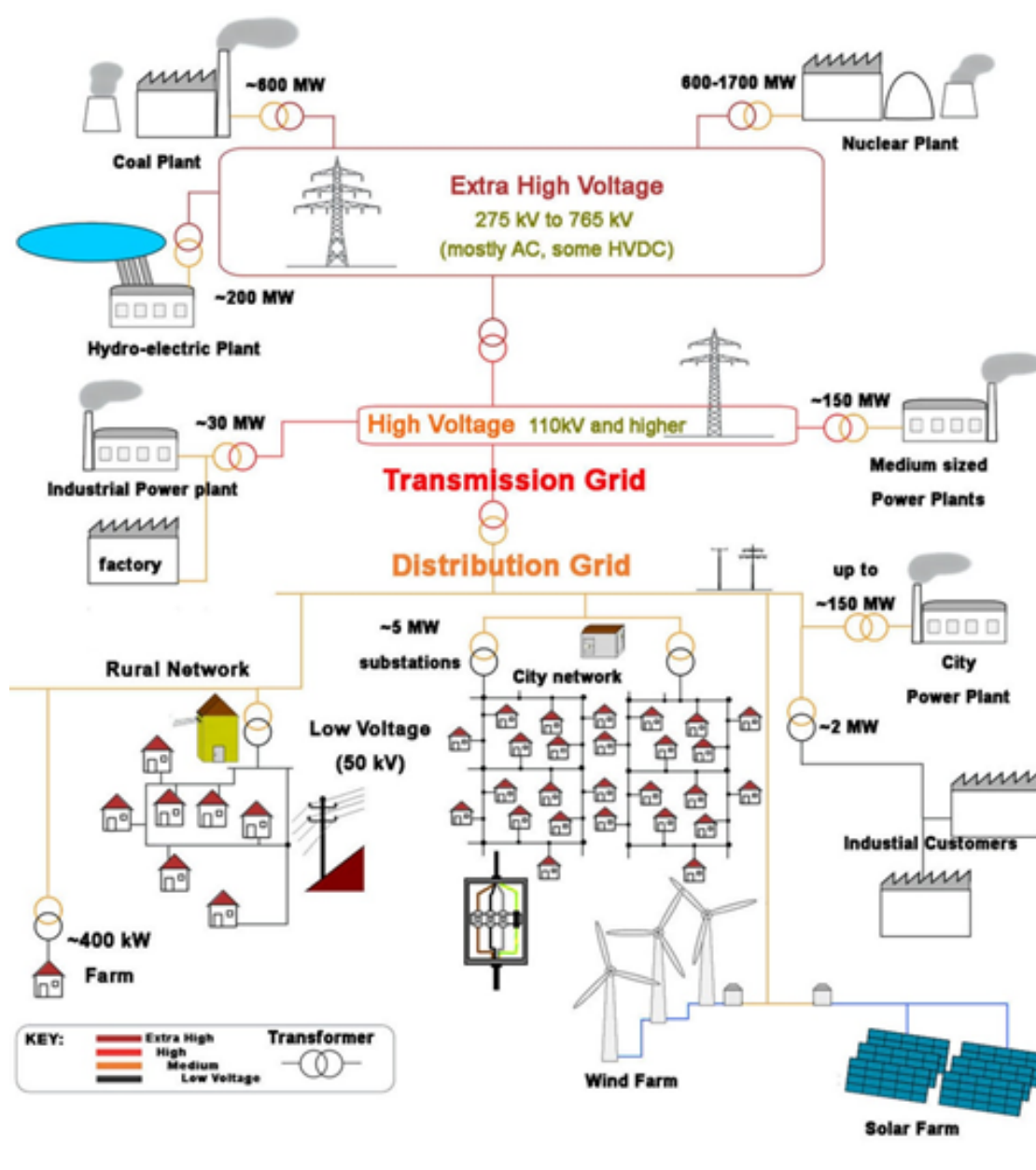
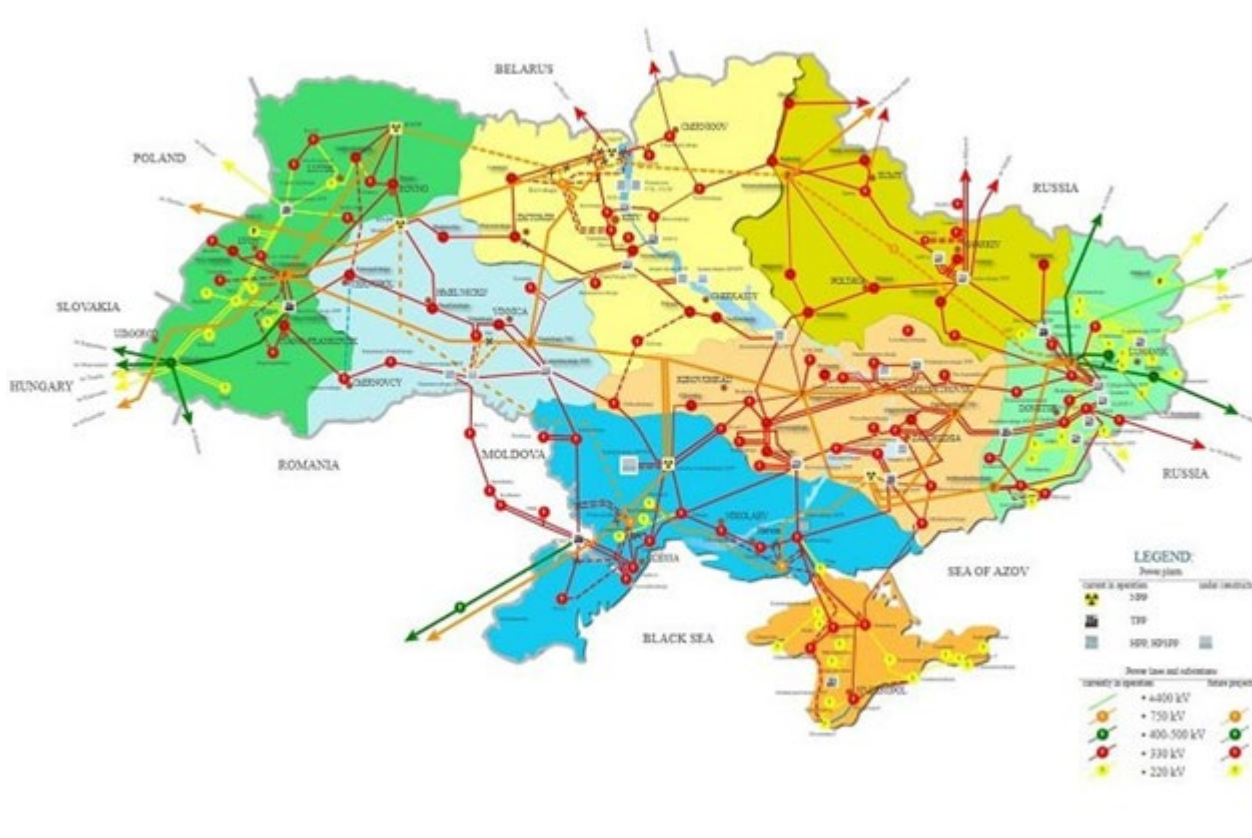


Рисунок 1 - Схема розподілення енергомережі та об'єднання об'єктів критичної енергетичної інфраструктури [7]

Систему енергоносіїв утворює критична інфраструктура об'єктів добичі



вуглеводневих енергоносіїв природного походження чи інших об'єктів – джерел сировини (вугілля, нафта, газ, радіоактивні матеріали, хімічна сировина для неорганічних енергоносіїв тощо), об'єктів їх переробки (у нафтопродукти, ракетне паливо, рідкий газ, активні елементи для ядерних реакторів) та об'єктів постачання перероблених енергоносіїв (транспортування, накопичення, зберігання та розподіл).



**Рисунок 2 - Об'єкти критичної енергетичної інфраструктури України [8]**

Систему електроенергетики утворює критична інфраструктура об'єктів запасів (сховищ) енергоносіїв, об'єктів вироблення («генерування») електроенергії (теплові, атомні та гідроелектростанції) та об'єктів її постачання (лінії електропередачі (ЛЕП), трансформаторні підстанції (ТП) розподілу електроенергії).

Систему теплоенергетики (ТЕ) утворює критична інфраструктура об'єктів накопичення (постачання) енергоносіїв (ЕН), об'єктів вироблення («генерування») теплової енергії (теплоцентралі) та об'єктів її постачання (теплотраси (ТТ) та пункти розподілу (ПР) теплоносіїв).

Системи енергетики є однією із основних складових забезпечення рівня



воєнно-економічного потенціалу країни, який визначає її обороноздатність. З іншого боку, Збройні Сили є також одним з основних споживачів для систем енергетики України, оскільки енергоносії, електроенергія та теплова енергія в цілому є головним джерелом боєздатності ЗС.

В Сухопутних Військах споживачами великих об'ємів пального, електро- та теплової енергії є механізовані, аеромобільні й танкові частини, армійська авіація, ракетні війська і реактивна артилерія, армійська ППО, війська (сили) бойового та матеріально-технічного забезпечення.

В Повітряних Силах споживачами різноманітного пального, електро- та теплової енергії є тактична та транспортна авіація, зенітно-ракетні і радіотехнічні війська та авіація ППО, сили бойового та матеріально-технічного забезпечення.

У Військово-Морських Силах споживачами різноманітного пального, електро- та теплової енергії є кораблі бойового складу та складу сил забезпечення, військово-морські бази, війська (сили) берегової оборони.

Пальне для військ (сил) у мирний час накопичується у сховищах на об'єктах споживання. Під час бойових дій постачання пального військам (силам) здійснюється як «танкерними» системами (залізничний, водний та автомобільний транспорт), так і «трубопровідними» системами (стаціонарними і тимчасовими, які розгортаються на території країни у воєнний час).

Окремими об'єктами системи енергоносіїв є сховища компонентів ракетного палива, які у великих об'ємах залишилися на території України після ліквідації позиційних районів Ракетних Військ Стратегічного Призначення колишнього СРСР. Дані компоненти (гептил й меланж) поступово утилізуються, але будуть знову потрібні у випадку створення авіаційно-космічних комплексів з повітряним стартом важких ракет-носіїв орбітальних об'єктів воєнного призначення (розвідки, попередження, навігації, зв'язку, управління, ударних) в інтересах Збройних Сил та загального призначення – в інтересах оборони країни.

У мирний час Збройні Сили використовують державні системи енергетики, під час бойових дій для систем зброї і військової техніки застосовуються накопичені запаси ЕН, штатні автономні системи електро- та теплоенергетики.

Об'єкти системи критичної енергетичної інфраструктури завжди відносять до об'єктів захисту («відповідальності») найбільшої оперативної-стратегічної важливості, які є для противника одними з «першочергових» об'єктів знищення або захоплення і, на жаль, мають високий ступень уразливості. Фахівцями США



досліджено, що диверсійна група з 7 осіб може паралізувати мільйонне місто діями саме по об'єктах системи критичної енергетичної інфраструктури.

«Системи енергоносіїв» ЕН мають у складі в основному стаціонарні об'єкти здобичі сировини (чи термінали зовнішніх джерел), об'єкти переробки сировини (нафтоперегінні і нафтогазові підприємства) та об'єкти транспортування ЕН (критична інфраструктура об'єктів «танкерного» водного, залізничного, авіаційного і автомобільного транспорту та стаціонарних об'єктів трубопровідних магістралей). Комплекси об'єктів ЕН мають масштабне у просторі розташування та значну уразливість щодо деструктивного впливу. У випадку ураження даних об'єктів можливі масштабні руйнівні та шкідливі екологічні наслідки, які пов'язані зі значними трудовитратами сил ДСНС, витратами засобів і часу на їх ліквідацію.

«Системи електроенергетики» ЕЕ мають у складі стаціонарні об'єкти накопичення ЕН (сховища пального, гідротехнічні споруди ГЕС), об'єкти генерування ЕЕ (ТЕС, ГЕС, АЕС) та об'єкти транспортування й розподілу ЕЕ. Об'єкти накопичення ЕН мають значну уразливість щодо деструктивного впливу крилатих ракет. Найбільш небезпечними щодо ураження об'єктами генерування ЕЕ є енергоблоки з ядерними реакторами АЕС. Наземні лінії електропередач, як об'єкти транспортування ЕЕ, найбільш уразливі щодо виведення їх з ладу та небезпечні для військ і населення при їх руйнуванні через виникнення масштабних пожеж при «короткому» замиканні в електромережах та ураження високою напругою. Кабельні лінії електропередачі менш уразливі щодо руйнування, але застосовуються лише на невеликих відстанях передачі ЕЕ.

«Системи теплоенергетики» ТЕ мають у складі стаціонарні об'єкти ЕН (сховища пального), об'єкти генерування ТЕ (ТЕЦ) та об'єкти транспортування й розподілу ТЕ. Об'єкти накопичення ЕН мають значну уразливість щодо деструктивного впливу, у випадку ураження даних об'єктів можливі масштабні руйнівні та шкідливі екологічні наслідки, які пов'язані зі значними трудовитратами сил і нарядами засобів на їх ліквідацію. Об'єкти генерування та транспортування ТЕ також мають уразливість щодо деструктивного впливу, але наслідки їх руйнування менш небезпечні.

Трубопровідні магістралі (ТМ) військового призначення в останній час набули поширення у збройних силах розвинутих країн. Вони розгортаються під час воєнного стану для постачання військам (силам) основних енергоносіїв (пального) для військової техніки та інших оперативних-стратегічних об'єктів.



Станції (пункти) забору (завантаження) енергоносіїв ТМ розгортаються на нафтопереробних підприємствах країни та сховищах ЕН.

Станції розподілу енергоносіїв розгортаються на об'єктах :

1. Аеродроми тактичної та транспортної авіації ПС.
2. Пункти заправки рухомої військової техніки.
3. Військово-морські бази ВМС.
4. Об'єкти військово-промислового (оборонного) комплексу.
5. Об'єкти критичної інфраструктури оперативно-стратегічного значення.

Кожна «нитка» ТМ від станції забору до стацій розподілу являє собою збірний трубопровід, секція якого має діаметр навколо 12,5 см і довжину до декількох десятків метрів. Секції з'єднуються гнучким герметичним манжетом та укладаються спеціальною технікою на глибину до 0.5 м в ґрунт (до 0,5 км за годину) чи на поверхню ґрунту (до 5 км за годину). Для підтримання потрібної продуктивності транспортування енергоносіїв вздовж «нитки» ТМ через кожні приблизно 50 км розташовуються компресорні станції, пункти управління та забезпечення ресурсами. Під час транспортування трубопровід завантажується енергоносієм об'ємом приблизно 10 м<sup>3</sup> продукту на 1 погонний км, швидкість транспортування – до 25 км/год. ТМ визнана значно більш ефективним засобом постачання енергоносіїв в порівнянні з «танкерним» транспортуванням, тому буде й в майбутньому головним засобом постачання енергоносіїв військам (силам) під час проведення операцій. Але ТМ, через стаціонарне розташування своїх елементів системи у великому просторі, нажаль, має підвищену уразливість як саме «ниток» трубопроводів, так й станцій забору, компресорних станцій, станцій розподілу та пунктів управління й забезпечення.

Таким чином, усі об'єкти систем енергетики у воєнний час безумовно можуть бути об'єктами вогневого ураження для ударної стратегічної авіації і ракетних комплексів наземного та морського базування, а також об'єктами диверсійних дій з боку противника. Виведення з ладу системи критичної енергетичної інфраструктури противником пов'язане, по-перше, зі зривом забезпечення енергією об'єктів воєнно-економічного (оборонного) потенціалу, об'єктів усіх інших сфер діяльності країни та бойових дій угруповань військ (сил) в операціях, і, по-друге, з нанесенням величезних економічних втрат, виникненням небезпечних екологічних наслідків для об'єктів критичної інфраструктури, населення й навколишнього середовища. Небезпека об'єктів





енергетики стає надзвичайно великою саме через максимально високу концентрацію хімічної енергії безпосередньо у енергоносіїв, так і механічної, електричної та теплової енергії на об'єктах її генерування, яка вивільняється при техногенних аваріях і катастрофах. Тому вже є багато прикладів техногенних катастроф із загибеллю людей та багатомільярдними збитками через знищення об'єктів і витратами на ліквідацію наслідків катастроф – пожежі та вибухи через аварії на вугільних шахтах, нафтопереробних підприємствах і сховищах пального, трубопровідних магістралях (найбільш важка подія – вибух газу через витік з магістрального трубопроводу зі знищенням двох пасажирських потягів – Росія, 1989 р.), техногенні катастрофи (Саяно-Шушенська ГЕС, Росія), руйнування АЕС із радіоактивним забрудненням середовища (Чорнобиль, Фукусіма).

В умовах науково-технічної революції, що продовжується у військовій сфері все більшого значення набуває пошук ефективних способів протиборства з більш оснащеним у технічному відношенні супротивником, який широко застосовує новітні інформаційні та телекомунікаційні технології.

Принципи побудови всіх ГСП дуже близькі один до одного і полягають у передачі із сузір'я навігаційних супутників (звичайно 24–30 штук) взаємно синхронізованих високочастотних широкосмугових радіосигналів з геостаціонарних орбіт висотою близько 20 000 км над Землею. Сукупність таких сигналів від кількох супутників одночасно приймається та обробляється навігаційним приймачем, що знаходиться або у складі бортової навігаційної системи засобів ураження або високоточних боєприпасів, з визначенням часу приходу сигналу кожного з навігаційних супутників у системі єдиного часу. При цьому просторові координати місцезнаходження кожного із цих супутників заздалегідь відомі. Використання отриманої та наявної апіорі інформації дозволяє однозначно визначити просторове положення приймача ГСП, та відповідно, об'єкту на якому він розташований, з високою точністю.

Головними критеріями вибору передавача перешкод для ТСБ ГСП можна вважати:

1. Невисока вартість.
2. Технічна можливість достатньої висоти підйому передавачів над землею в умовах реальної місцевості.
3. Використання звичайних антен мобільних передавачів з невеликим підсилення, не більше 10-15 дБ [5].



4. Можливість щодо тривалого (на час військового конфлікту) використання передавачів перешкод з існуючими джерелами електроживлення для забезпечення потужності перешкоди одного передавача в 10-50 Вт.

Використання меншої потужності спричиняє невиправдане зростання кількості передавачів для створення суцільного поля придушення. Використання більшої потужності негативно впливає на мобільність (є у вигляді версії передавачів перешкод, що носяться або возяться, час автономної роботи яких (хоча б одиниці годин) полегшує розвідку положення передавачів для вогневого ураження противником.

#### 1.4. 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 ( $K_{\Pi}$ ), характерного для даної перешкоди та конкретного типу приймача GPS. Інакше висловлюючись, перешкода ефективна, якщо виконується умова

$$\frac{P_{\Pi ВХ}}{P_{с ВХ}} \geq K_{\Pi}, \quad (1)$$

де  $P_{\Pi ВХ}$ ,  $P_{с ВХ}$  - 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  $K_{\Pi} = 0,5 \dots 1$ . 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  $P_{\text{Прд}}$  із коефіцієнтом підсилення його антени  $G_{\text{Прд}}$  опромінює приймач з ефективною площею антени  $S_{\text{эфПрм}}$ , віддалений від нього на відстань  $R$ .



Щільність потужності випромінювання у приймача  $\Pi_R$  [Вт/м<sup>2</sup>] визначається відношенням потужності  $P_{\text{Прд}}$  до площі поверхні сфери радіусу  $R$ , яке має бути збільшено в  $G_{\text{Прд}}$  разів:

$$\Pi_R = \left( \Pi_{\text{Прд}} \eta / 4\pi R^2 \right) G_{\text{Прд}},$$

де  $\eta$  - коефіцієнт втрат серед поширення.

Потужність сигналу перешкоди на вході приймача GPS дорівнюватиме :

$$P_{\text{пвх}} = \Pi_R S_{\text{эфПрм}} = P_{\text{Прд}} G_{\text{Прд}} S_{\text{эфПрм}} \eta / (4\pi R^2). \quad (2)$$

Використовуючи відоме співвідношення

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

де  $\lambda$  - довжина хвилі, отримуємо:

$$P_{\text{пвх}} = P_{\text{Прд}} G_{\text{Прд}} G_{\text{Прм}} \lambda^2 \eta / (4\pi)^2 R^2. \quad (3)$$

Враховуючи вирази 1 і 3 знаходимо необхідну потужність передавача перешкоди

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

де  $P_{\text{Прм min}}$  - 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, задаємо значення параметрів, що входять у формулу 4:

$$\begin{aligned} R &= 100 \text{ км}; \\ P_{\text{Прм min}} &= 10^{-12} \text{ Вт}; \\ K_{\text{п}} &= 1; \\ G_{\text{Прд}} &= 500; \\ G_{\text{Прм}} &= 5; \\ \lambda &= 19 \text{ см}, 24 \text{ см}; \\ \eta &= 1; \\ \theta(\beta, \varepsilon) &= 1. \end{aligned}$$

Тоді, необхідна потужність передавача перешкод після проведення розрахунку 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 прив'язного БПЛА або дирижабля). 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  $10^{-2} \dots 10^{-3}$ . 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 [2].

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 підсилення антени передавача перешкод вважали рівним 10 дБ). Модуляція потужності передавача перешкод здійснювалася згідно із законом:

$$P_i(t) = P_o \cdot (1 + \cos(2 \cdot \pi \cdot f_m \cdot t + \varphi_o)), \quad (5)$$

де:  $P_o$  - задане значення потужності;  $f_m$  - частота модуляції перешкоди;  $\varphi_o$  - початкова фаза перешкоди.

Отримані 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.

Однчасне використання кількох передавачів перешкод з різних напрямків відносно ОКЕІ, навіть у кількості менших ступенів свободи автокомпенсатора 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.

Цілком очевидно, що навіть при зниженні ефективності багатопозиційної керованої ТСБ для ОКЕІ захищених приймачів ГСП раціональне розміщення передавачів перешкод, керування їх потужністю та параметрами модуляції сигналів перешкод дозволить створити ефективну ТСБ для ОКЕІ та суцільну зону придушення ГСП.

Проведені дослідження дозволили визначити можливу структуру і характеристики передавачів перешкод приймачам ГСП а також структуру ТСБ ГСП в межах території України.

Передавач перешкод приймачам (ППП) ГСП розгорнутих США і Росією може забезпечити стійкий вплив на роботу приймачів ГСП – (GPS/GLONASS), сприяти виникненню значних помилок у визначенні положення об'єктів ураження. Об'єкти військового або цивільного призначення, оснащені приймачами ГСП, які опинилися в зоні дії такого передавача, стають нездатними до визначення свого реального просторового положення, що, як правило, буде приводити до зриву покладених на ці об'єкти ураження завдань щодо знищення ОКЕІ. ППП може бути повністю виконаний на сучасній твердотільній елементній базі, мати невеликі масо-габаритні характеристики для використання на БПЛА. Передавач перешкод дозволяє індивідуально або в складі системи вирішувати задачу блокування (перекручування) прийому сигналів ГСП над територією держави або окремих його районів розташування ОКЕІ і тим самим значною мірою забезпечити захист важливих ОКЕІ від ударів зброї, що використовує для свого точного наведення приймачі ГСП.

Можна вважати, що ефективність застосування високоточної зброї по ОКЕІ, на якій є приймачі ГСП, у результаті дії ППП виявиться дуже низькою. Причому сторона, що атакує, може розкрити цей факт тільки після застосування цієї зброї, зазнавши значних матеріальних витрат на ураження ОКЕІ. Приймачі ГСП, що використовуються для навігації в наземних, морських і повітряних бортових інформаційно-управляючих комплексах і військовій техніці теж будуть піддаватися впливу ППП.

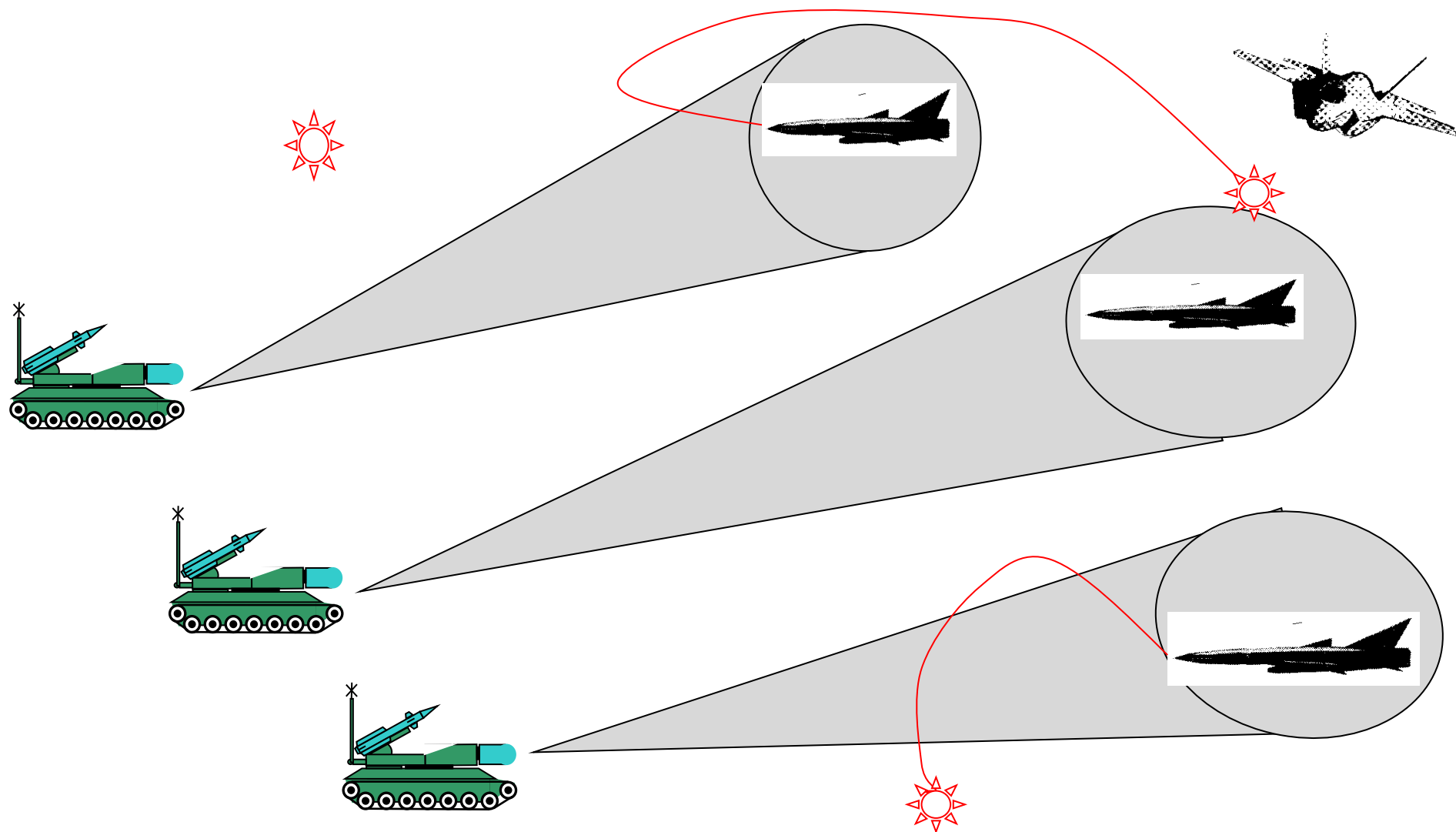
Отже, бойове застосування супротивником озброєння і військової техніки, що оснащена приймачами ГСП, по ОКЕІ виявиться або під зривом взагалі, що призведе до невиконання бойових завдань, або навіть призведе до аварій і катастроф внаслідок значних помилок у визначенні реального місцезнаходження.



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, слабо уразливими і несподіваними в застосуванні.

ППП можуть працювати як автономно, так і у складі існуючих зразків озброєння і техніки з розвинутою інфраструктурою (наприклад системи ППО) або у складі перспективної Територіальної Системи Блокування ГСП для ОКЕІ. 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 безпроводної сенсорної мережі для створення сенсорного поля покриття ОКЕІ (див. Рис.4).



**Рисунок 3 - Придушення роботи приймачів ГСП, встановлених на крилатих ракетах призводить до їх відхилення від необхідних траєкторій польоту і не виконанню покладених завдань**

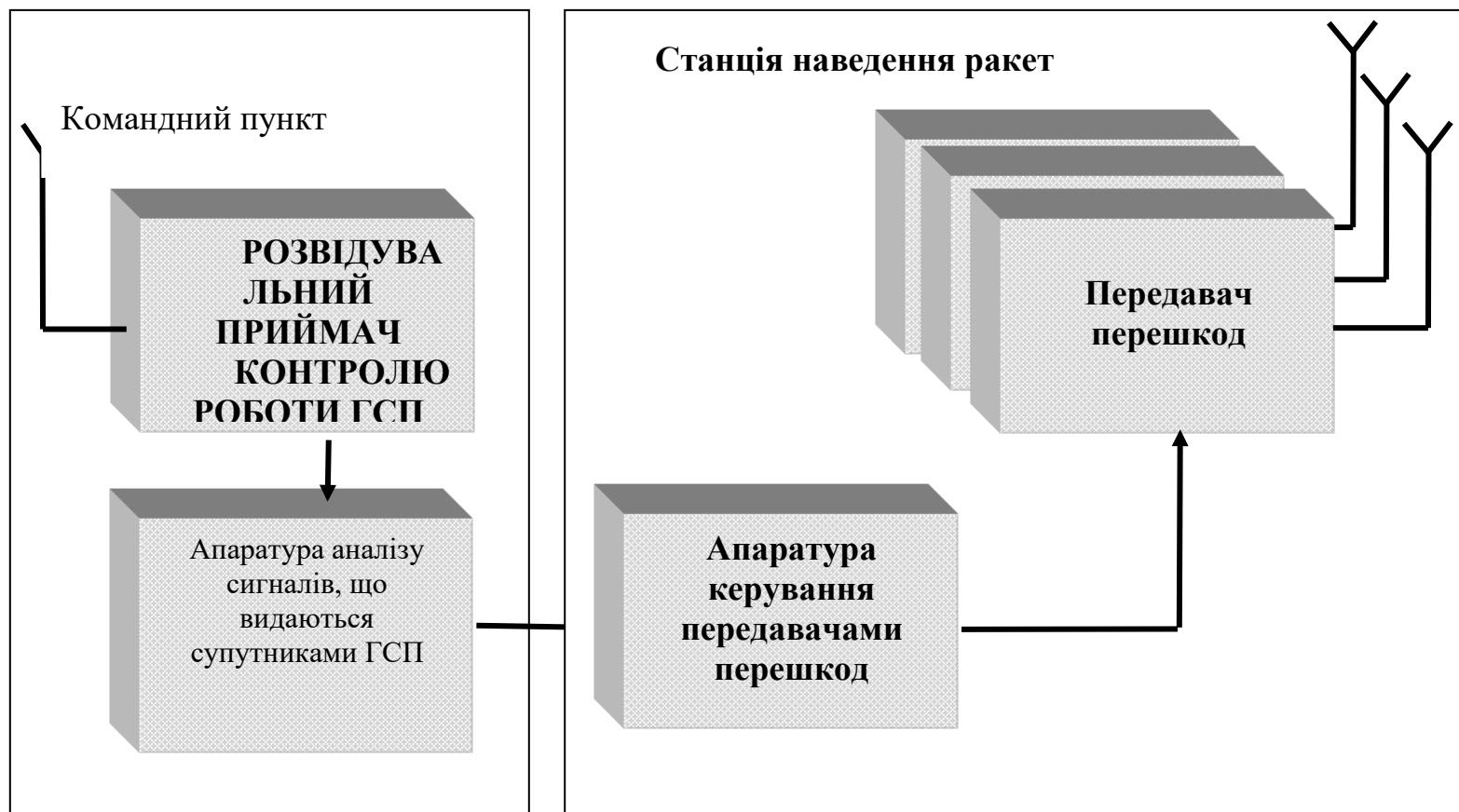


Рисунок 4 - Структурна схема ТСБ ГСП для ОКЕІ застосування глобальних систем визначення положення





## **Висновки**

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.

Передавачі перешкод можуть бути розміщені не тільки на наземних зразках озброєння. Вони можуть бути розташовані також на повітряних носіях (наприклад, на дистанційно пілотованих апаратах), закинутими на територію супротивника і включатися в необхідний або встановлений час. Очікується, що вартість, як окремого передавача, так і системи в цілому буде відносно низька, а ефективність від їхнього застосування буде досить високою.

До складу ТСБ ГСП можуть входити (Рис.4) :

1. Розвідувальний приймач контролю роботи ГСП.
2. Апаратура аналізу сигналів, що видаються супутниками ГСП.
3. Апаратура керування передавачами перешкод.
4. Передавачі перешкод.
5. Інші додаткові засоби.

У разі застосування даної системи в складі системи ППО вказана апаратура може бути розташована на командних пунктах (крім ППП), а керування ППП може здійснюватися за допомогою автоматизованих засобів управління.

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.