

УДК 621.396.967.2

І.В. Свид

Харківський національний університет радіоелектроніки

ПРОБЛЕМА ЗАВАДОЗАХИЩЕНОСТІ ЗАПИТАЛЬНИХ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

У статті на основі аналізу протиріч принципів побудови, роздільного та сумісного функціонування з багатопозиційними первинними системами спостереження показана неможливість забезпечення припустимих показників завадозахищеності існуючих запитальних систем спостереження, що породжує проблему.

Ключові слова: завадозахищеність, запитальні системи спостереження

Вступ

Постановка проблеми й аналіз літератури.

Основні елементи процедури контролю повітряного простору (ПП) [1] це:

- аналіз повітряної обстановки;
- прийняття рішень.

Розвідка повітряного простору здійснюється системами спостереження (СС), головна задача яких надати відповіді: де знаходиться повітряний об'єкт (ПО) та визначити державну приналежність. Відповідь на ці питання дають спільно первинні [2] та запитальні [3] СС. Первинні СС відповідають на запитання «де», а запитальні СС, тобто системи ідентифікації «свій-чужий», на запитання «хто». Якість інформації цих двох СС визначається завадостійкістю останніх та визначає, значною мірою, якість інформаційного забезпечення системи контролю ПП.

Рішення приймає особа на основі аналізу відповідним чином підготовленої інформації про стан повітряної обстановки. Правильне рішення може бути прийнято лише тоді, коли є досить повна, точна, достовірна й безперервна інформація про повітряну обстановку в зоні управління. Отже, якість прийняття рішень визначається складом та якістю інформації, на основі якої особа приймає рішення. Все це накладає дуже жорсткі вимоги до завадозахищеності СС ПП.

Мета роботи – оцінка завадозахищеності СС повітряного простору.

Основна частина

Запитальні СС до яких відносяться:

- вторинні СС;
- системи ідентифікація за ознакою «свій-чужий»;
- вбудовані канали вторинної радіолокації в первинні СС;
- канал спостереження радіосистеми ближньої навігації (РСБН),

значною мірою забезпечують рішення задач, котрі стоять перед системою контролю ПП.

Запитальні СС призначені для вирішення наступних задач:

- визначення координат ПО;
- радіолокаційної ідентифікації ПО за ознакою «свій-чужий»;
- отримання польотної інформації, яка необхідна для контролю управління польотами та наведення ПО;
- диспетчерської ідентифікації ПО.

Крім того, канал індикації РСБН призначений для визначення координат ПО, для чого користуються послугами радіомаяка.

Окремі типи запитальних СС можуть працювати або як автономні пристрої, або вбудовуватися в первинні СС.

Виходячи з принципу функціонування запитальних СС, антена відповідача є слабкоспрямованою. Це вносить суттєві недоліки в процес функціонування розглядаємих систем.

Обґрунтуємо імовірність завадозахищеності запитальних СС яка може бути визначена як:

$$P_{zz} = 1 - P_v P_{vim} P_{pr} ,$$

де P_v - імовірність виявлення сигналів; P_{vim} - імовірність вимірювання параметрів сигналів; P_{pr} - імовірність порушення роботи; $P_v P_{vim}$ - скритність; P_{pr} - завадостійкість; $P_{skr} = 1 - P_v$ - імовірність скритної роботи.

Будемо розглядати енергетичну скритність запитальних СС, яка характеризує здатність протистояти заходам, які направлені на виявлення сигналу приймачем розвідки.

За принципом обслуговування сигналів запиту (СЗ) літаковий відповідач (ЛВ) відноситься до одноканальних систем масового обслуговування (СМО) з відмовами, що вказує на те, що будь-який правильно прийнятий СЗ обслуговується відповідачем, якщо він не зайнятий обслуговуванням іншого, раніше

прийнятого СЗ. При обслуговуванні СЗ приймач відповідача закривається на час паралізації, величина якого визначається режимом роботи. У зв'язку з цим, відповідач системи запитальних СС характеризується коефіцієнтом готовності, що є ймовірністю відповіді на даний СЗ. Крім того, апаратура відповідача розраховується на деяку граничну кількість (максимальне завантаження) відповідей в секунду. При перевищенні кількості запитів максимального завантаження відповідач обмежує число відповідей шляхом виключення СЗ з найменшою амплітудою сигналу.

Особливістю запитальних СС є наявність внутрісистемних завад. Дійсно, сусідні запитальні СС є джерелами завад для розглядаємої запитальної СС. Ці завади проявляються двояко. По-перше, СЗ сусідніх запитальних СС закривають ЛВ на час обслуговування СЗ, що унеможливує відповідь на СЗ розглядаємої запитальної СС. По-друге, випромєнені СВ ЛВ на запити сусідніх запитальних СС, є завадою для розглядаємої запитальної СС. Ці обставини потребують використовувати несинхронну мережу запитальних СС. При такій організації мережі ефективним способом захисту вторинних СС від СВ, викликаних сусідніми запитальними СС, є міжперіодна обробка. Однак побудова запитальних СС на принципі несинхронної мережі та відсутність просторової вибірковості ЛВ дозволяє зацікавленій стороні або несанкціоновано отримувати інформацію від ЛВ, або подавляти запитальну СС шляхом постановки навмисних корельованих завад необхідної інтенсивності.

У запитальних СС кодується як СЗ, так і СВ. Для їх кодування використовуються інтервально-часові, частотно-часові та позиційні коди. Використання такого кодування по-перше потребує обирати смугу пропускання приймача значно більшу за потенціальну, що призводить до зниження завадостійкості розглядаємих систем, а по-друге – приводить до виключення енергетичної скритності. Можливо показати, що СВ можуть бути виявлені з дальності яка значно перебільшує дальність виявлення первинних СС. Використання сигналів з великою базою в якості СЗ та СВ неможливе так як це збільшує часову базу сигналу і, як наслідок, знижує завадостійкість запитальних СС.

Зазначені недоліки побудови існуючих запитальних СС, а також використання розглянутих способів кодування СЗ та СВ не дозволяє віднести їх ні до завадостійких систем, ні до енергетично скритних.

Таким чином, основне протиріччя роздільного функціонування запитальних СС закладено в принцип побудови і принцип обслуговування СЗ, що зумовила низьку завадостійкість останніх. При цьому необхідно відзначити, що створення імітостійко-

го режиму дозволяє закрити лише канал відповіді, залишивши повністю відкритим канал запиту. У цій ситуації, дійсно, протівна сторона ніколи не може відповісти «я свій». Однак, поставивши заваду каналу запиту, а він залишився відкритим, становиться не можливим визначити де «наш» ПО.

Важливим напрямком підвищення живучості та завадостійкості первинних СС є створення багато-позиційних (БП) первинних СС, за рахунок переходу від несинхронної мережі СС до синхронної мережі СС. Основною перевагою БП первинних СС є підвищення живучості та завадозахищеності у порівнянні з однопозиційними первинними СС. Це досягається територіальним розносом передавальної й приймальної позицій.

Однак, в теоретичних і в практичних роботах по БП первинним СС не розглядаються питання взаємодії рознесеної первинної та існуючого варіанту запитальної СС. Сучасні ж запитальні СС не можуть працювати в рознесеному режимі. Таким чином, підвищення живучості первинних СС шляхом рознесення передавальної й приймальної позицій наштотуються на неможливість реалізації на такому принципі запитальних СС. Розташування ж запитальних СС на приймальному пункті (невипромінюючому) рознесеної первинної СС повністю демаскує останню.

Отже, основне протиріччя спільного функціонування запитальних СС і рознесених первинних СС закладено в принцип побудови запитальних СС, який не дозволяє роботу запитальних СС в рознесеному режимі.

Таким чином, можливість несанкціонованого використання ЛВ запитальних СС визначена принципами побудови останніх.

Дійсно, існуючі запитальні СС побудовані за однаковими принципами:

- несинхронної мережі;
- одноканальної системи масового обслуговування з відмовами.

Побудова запитальних СС за такими принципами виключила як часову, так і просторову різницю між корисними та імітованими сигналами. Ця особливість призводить до того, що зацікавлена сторона має можливість як несанкціоновано отримувати інформацію від ЛВ розглядаємих СС, так і подавляти їх роботу імітованими СЗ потрібної інтенсивності.

Проведемо оцінку ймовірності виявлення ПО існуючими запитальними СС при впливі потоку СЗ, утвореного сумарним потоком СЗ (ПСЗ) сусідніх СС, потоком некорельованих завад (НКЗ) зацікавленої сторони і хаотичними імпульсними завадами (ХІЗ).

При надходженні на вхід ЛВ запитальної СС потоку СЗ і ХІЗ будуть спостерігатися наступні

основні ситуації, що приводять до виключення формування ЛВ СВ:

- подавлення СЗ даного запитувача через утворення з ХІЗ випереджальних хибних СЗ, що викликають випромінювання СВ або спрацьовування схеми подавлення бічних пелюстків (ПБП);
- подавлення СЗ даного запитувача через випереджальний СЗ як сусідніх запитувачів, так і запитувачів зацікавленої сторони;
- високочастотне подавлення окремих імпульсів СЗ даного запитувача при збігу за часом імпульсів потоку СЗ і несприятливих фазових співвідношень;
- подавлення СЗ даного запитувача через випереджальний хибний СЗ, що утворюється в результаті взаємодії першого імпульсу СЗ даного запитувача з випереджальними (на базу коду) імпульсами ХІЗ чи ПСЗ, що викликають випромінювання СВ чи спрацьовування схеми ПБП.

Визначення імовірності цих подій будемо здійснювати у припущенні, що ПЗС і ХІЗ діють на СЗ даного запитувача незалежно один від одного і що кількість джерел, які формують загальний ПСЗ, достатнє для того, щоб вважати потік пуасонівським.

Припустимо, що на вхід відповідача надходять ХІЗ інтенсивністю λ_0 , ПСЗ, що викликає випромінювання СВ, що включає потік СЗ сусідніх запитувачів і потік імітованих СЗ зацікавленої сторони, інтенсивністю λ_1 , та потік СЗ, що викликає спрацьовування схеми ПБП, інтенсивністю λ_2 .

Використовуючи методику розрахунку зазначених імовірностей, досить докладно викладених у [4], одержуємо результати розрахунку імовірності виявлення ПО (рис. 1). Наведені розрахунки отримані при $\lambda_0 = 5000$. Аналіз наведених розрахунків показує, що можливість зацікавленої сторони подавляти запитальні СС за рахунок несанкціонованого використання ЛВ потрібної інтенсивності ставить під сумнів можливість роботи цих систем у конфліктних ситуаціях. Дійсно, як показано на рис. 1, при інтенсивності СЗ $\lambda_1 = 5000$, які може імітувати заці-

кавлена сторона імовірність виявлення ПО запитальною СС складає всього 0,2.

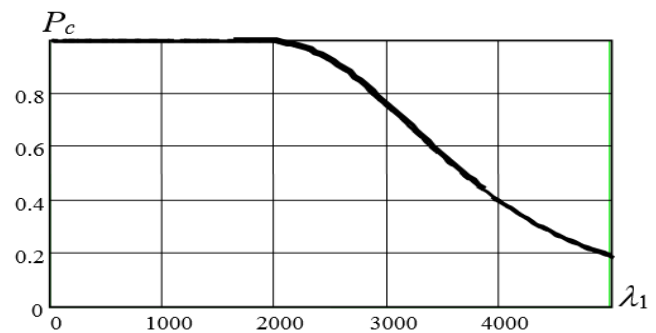


Рис. 1. Імовірність виявлення ПО

Висновки

У статті показано, що існуючий принцип побудови запитальних СС заклав протиріччя у забезпечення потрібної заводозахисності останніх як при роздільному, так і спільному функціонуванні з рознесеними первинними СС.

Показано, що наведені протиріччя між необхідністю заводозахисту запитальних СС та можливістю її реалізації на відомих принципах породжує проблему заводозахисту зазначених систем.

Список літератури

1. Автоматизированные системы управления воздушным движением: Новые информационные технологии в авиации / под ред. С.Г. Пятко и А.И. Краснова. - СПб.: Политехника, 2004. - 446 с.
2. Farina A. and Studer F., (1993), Digital radar data processing, Radio i svyaz, Moscow: 319 p. (in Russian).
3. Stevens M.C., Secondary Surveillance Radar, Artech House, 1988.
4. Обод І.І. Заводозахисність вторинних систем спостереження повітряного простору / І.І. Обод, І.В. Свид, І.А. Штих. - Х.: ХНУРЕ, 2014. - 310 с.

Надійшла до редколегії 23.07.2017

Рецензент: д-р техн. наук професор О.А.Серков, Національний технічний університет «ХПІ», Харків.

ПРОБЛЕМА ПОМЕХОЗАЩИТЫ ЗАПРОСНЫХ СИСТЕМ НАБЛЮДЕНИЯ ВОЗДУШНОГО ПРОСТРАНСТВА

И.В. Свид

В статье на основе анализа противоречий принципов построения, отдельного и совместного функционирования с многопозиционными первичными системами наблюдения показана невозможность обеспечения приемлемых показателей помехозащищенности существующих запросных систем наблюдения, что создает проблему.

Ключевые слова: помехозащита, запросные системы наблюдения.

THE PROBLEM OF PUTTING THE REQUIRED AIR POLLUTION OBSERVATION SYSTEMS

I.V. Svyd

Based on the contradictions analysis in the principles of constructing separate and joint operation with multi-position primary surveillance systems, the article shows the impossibility of providing acceptable indicators of noise immunity of existing query observing systems, which creates a problem.

Keywords: interference immunity, query observing systems.