УДК 004.045:621.396.967.2

І.І.ОБОД, докт. техн. наук, НТУ «ХПІ»;
О.О.ТЮРІН, НТУ «ХПІ»

ЗАВАДОЗАХИЩЕНІСТЬ СИСТЕМ СПОСТЕРЕЖЕННЯ, ЩО ЗАПИТУЮТЬ ЄДИНОЇ ІНФОРМАЦІЙНОЇ МЕРЕЖІ З РОЗПОДІЛЕНОЮ ОБРОБКОЮ

Приводиться аналіз завадостійкості та скритності існуючих запитальних систем спостереження єдиної інформаційної мережі з розподіленою обробкою. Показано, що існуючі запитальні системи спостереження мають незначну завадостійкість при дії навмисних корельованих завад та малу енергетичну скритність, обумовлену використанням інтервально-часових кодів у якості сигналів запиту і відповіді. Аналізується можливість використання широкосмугових сигналів у якості сигналів запиту і відповіді.

Noise-immunity and hiding of existent query systems of supervision of unified information network with the distributed processing is brought . It is rotined that the existent query observing systems have insignificant noise-immunity at the action of the intentional correlated noise and small power hiding, conditioned by the use of interval-timecode as query and answer signals. Possibility of the use of broadband signal is analysed as query and answer signals

Постановка завдання та аналіз літератури. Рішення задач, які стоять перед користувачами системи контролю використання повітряного простору багато в чому визначається інформаційним забезпеченням. Основою інформаційного забезпечення є первинні системи спостереження (СС). Однак інформаційними системами що забезпечують, а іноді й основними інформаційними системами, є системи спостереження, що запитують, яки призначені для рішення наступних задач:

- визначення координат повітряного об’єкту (ПО);
- одержання додаткової польотної інформації, необхідної для контролю і керування польотами і наведення ПО;
- ідентифікації ПО за ознакою «свій-чужій»;
- диспетчерського опізнавання ПО.

Оцінка завадостійкості існуючих СС, що запитують достатньо повно розглянута у роботах [1-3]. Однак питанням завадозахищенності СС, що запитують не приділено достатньо уваги.

Мета роботи – оцінка завадозахищенності існуючих та перспективних СС, що запитують.

Основна частина. СС, що запитують, утворені запитувачем та відповідачем, побудовані за принципом несинхронної мережі, одноканального пристрою обслуговування першого правильно прийнятого сигналу запиту (СЗ) і відкритих систем масового обслуговування (СМО) з відмовами. Така побу-

дова останніх відкриває широкі можливості зацікавленій стороні по несанкціонованому використанню відповідачів цих систем для дальнього виявлення ПО, а також для повної паралізації шляхом постановки корельованих завад (КЗ) необхідної інтенсивності. Можливість зниження завадостійкості СС, що запитують зацікавленою стороною обумовлена тим, що відповідач має час паралізації, який дуже суттєвий при роботі у імітостійкому режимі. Дійсно, принцип побудови існуючих СС, що запитують виключив як часові так і просторові розходження між корисними та імітованими СЗ. При роботі відповідача тільки в полі дії своїх СС, що запитують, що створюють внутрішньосистемні завади (ВСЗ), коефіцієнт готовності (КГ) відповідача завжди менше одиниці. Під КГ відповідача розуміється імовірність відповіді на запит конкретного запитувача, що є ні чим іншим як відносною пропускною здатністю відповідача. КГ відповідача залежить від інтенсивності потоку СЗ, утвореного потоком СЗ від сусідніх СС, що запитують, потоком навмисних КЗ (імітовані завади), а також потоком ЗС, що утворився з потоку навмисних і ненавмисних некорельованих завад. Рівень ВСЗ може контролюватися і цим, отже, обмежується граничне зменшення КГ відповідача. Створення зацікавленою стороною навмисних КЗ, яке неможливо контролювати, може цілком паралізувати відповідач і цим істотно знизити завадостійкість СС, що запитують.

У якості сигналів відповіді (СВ) СС, що запитують використаються інтервально-часові та часово-частотні коди, яки утворюються декілька вузькосмуговими сигналами на одній чи двох несучих частотах, часова відстань між якими і є кодом СВ. Використання вузькосмугових сигналів, відомих несучих частот, апріорно відомих часових розстановок імпульсів СВ та наявність слабкоспрямованої антени на ЛА призводить до того, що ЛВ є жаданим об'єктом засобів радіотехнічній розвідки (РТР) зацікавленої сторони.

Оцінимо завадозахищеність СС, що запитують, тобто енергетичну скритність та завадостійкість. Розрахунки зробимо при роботі СС, що запитують у імітостойкому режимі.

Проведемо оцінку скритності існуючих СС, що запитують. Оцінку скритність будемо проводити за критерієм дальності виявлення СВ типових ЛВ. У якості системи РТР будемо використовувати різницево-дальномірну систему, яка складається з трьох приймальних пунктів. Рішення координатної задачі системою РТР можливе при виявлені сигналів на всіх приймальних пунктах. При цьому слід зазначити, що система РТР може вирішувати задачу виявлення координат ПО при виявленні одиночних імпульсів СВ (n = 1), а також усього СВ (n = 2 чи n = 3).

На рис. 1 наведена залежність дальності виявлення СВ типових ЛВ типовою системою РТР.

Наведені розрахунки показують, що виявлення СВ сучасних ЛВ типовою системою РТР не має складнощів, що указує на відсутність енергетичної

скритності існуючих СС, що запитують. При цьому слід зазначити, що виявлення сигналів здійснюється за зон дії систем первинних СС.

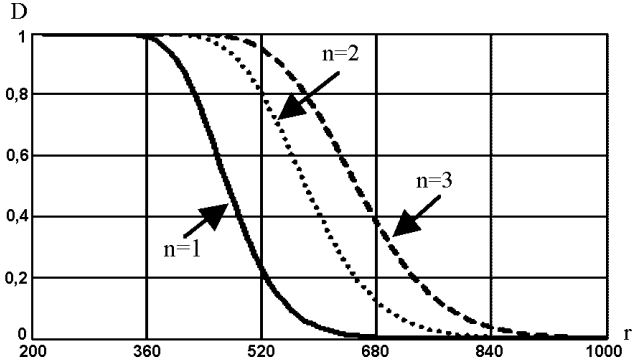

Рисунок 1 – Дальність виявлення СВ СС, що запитують

Проведемо оцінку завадостійкості існуючих СС, що запитують, для чого дослідимо вплив потоку СЗ, утвореного сумарним потоком СЗ сусідніх СС, що запитують, потоком навмисної корельованої завади супротивника і хаотичної імпульсної завади (ХІЗ) на імовірність одержання координатної інформації від ЛВ.

При надходженні на вхід ЛВ СС, що запитує потоку СЗ і ХІЗ будуть спостерігатися наступні ситуації, що приводять до виключення формування ЛВ сигналів відповіді (СВ) запитувачам:

- подавлення СЗ даного запитувача через утворення з ХІЗ випереджальних хибних СЗ (хибна тривога першого роду), що викликають випромінювання СВ або спрацьовування схеми подавлення бічних пелюстків (ПБП);
- подавлення СЗ даного запитувача через випереджальний СЗ як сусідніх запитівачів, так і запитувачів супротивника;
- 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 утворюються в результаті взаємодії першого імпульсу СЗ даного запитувача з випереджальним (на базу коду) імпульсами ХІЗ чи ПСЗ (імовірність хибної тривоги другого роду) і зухвалих випромінювання СВ чи спрацьовування схеми ПБП;
- подавлення СЗ у результаті роботи схем часової селекції відповідачів;
- подавлення СЗ у результаті інерційності схем вхідних формувачів дешифратора й обмеження завантаження відповідача.

Визначення імовірності цих подій будемо здійснювати у припущенні,

що потоки сигналів запиту (ПЗС) і ХІЗ діють на СЗ даного запитувача незалежно один від одного і що число джерел, яки формують загальний потік СЗ, достатнє для того, щоб вважати потік пуассонівським.

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 супротивника, інтенсивністю λ_1, та потік СЗ, що викликає спрацьовування схеми ПБП, інтенсивністю λ_2.

Використовуючи методику розрахунку зазначених імовірностей, досить докладно викладених у [2], одержуємо результати розрахунку завадостійкості існуючих СС, що запитують при вирішенні задачі ідентифікації виявлених ПО, наведені на рис. 2-3. На рис. 2 наведені розрахунки КГ відповідача, а на рис. 3 – ймовірність виявлення ПО СС, що запитує.

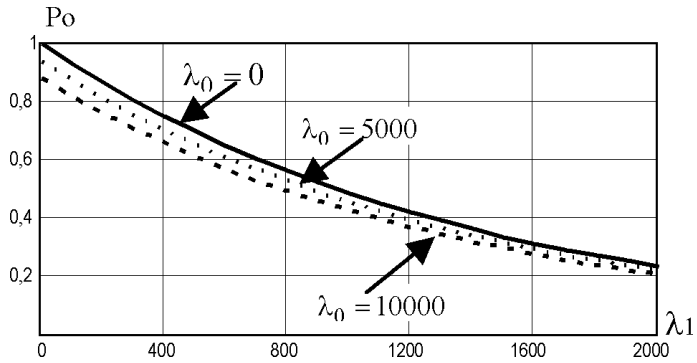

Рисунок 2 – Коефіцієнт готовності відповідача ПО

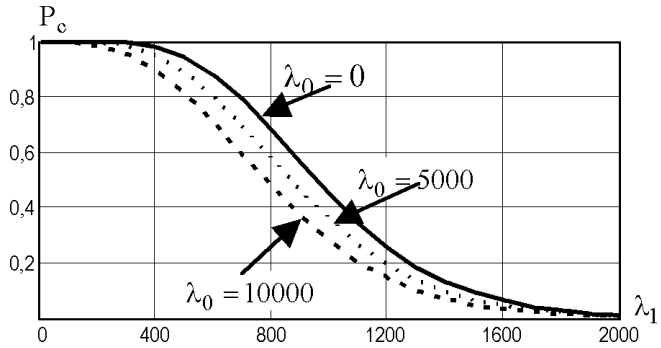

Рисунок 3 – Ймовірність виявлення ПО СС, що запитує

Аналіз наведених на рис. 2 і 3 розрахунків завадостійкості існуючих СС, що запитують показує, що можливість супротивника подавляти СС, що запитує за рахунок несанкціонованого використання ЛВ потрібної інтенсивності

ставить під сумнів можливість роботи цих систем у конфліктних ситуаціях.

Все це підтверджує твердження, що сучасні СС, що запитують характеризуються низькою завадостійкостю.

Таким чином, існуючі СС, що запитують характеризуються відсутністю енергетичної скритності та низкою завадостійкостю, що вказує на низьку існуючих завадозахищеність СС, що запитують.

Підвищення енергетичної скритності СС, що запитують можливе за рахунок використання складних (широкосмугових) сигналів [5]. Дійсно, на рис. 4, показана дальність виявлення сигналів ЛВ при використанні у якості СВ складних сигналів з базою В = 1000.

Розрахунки, наведені на рис. 4, показують, що використання складних сигналів у якості СВ суттєвим чином могли б підвищити енергетичну скритність СС, що запитують. Однак перехід до використання складних сигналів у якості СВ призводить до розширення часової бази СВ, яка у свою чергу призводить до збільшення часу паралізації ЛВ. Збільшення часу паралізації ЛВ призводить до зменшення завадостійкості ЛВ.

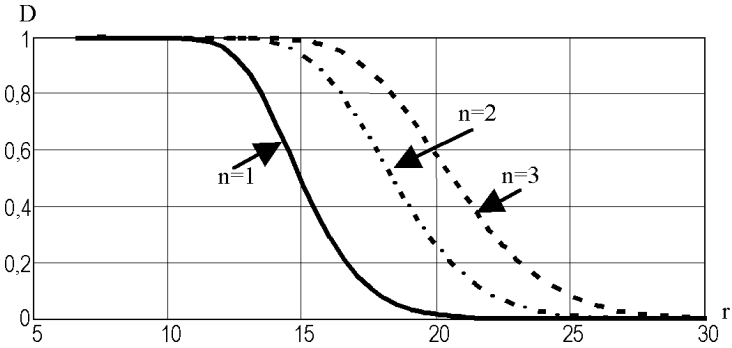

Рисунок 4 – Дальність виявлення сигналів ЛВ СС, що запитує

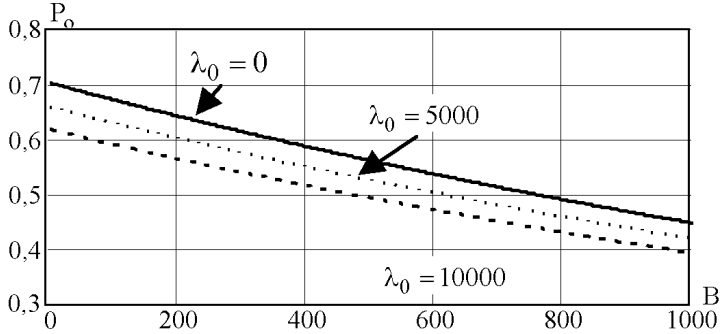

Рисунок 5 – Вплив бази СВ на КГ ПО

На рис. 5 і 6 наводяться розрахунки завадостійкості СС, що запитують при використанні складних сигналів у ЛВ з базою 1000. Розрахунки наведені при фіксованих потоках сигналів запиту.

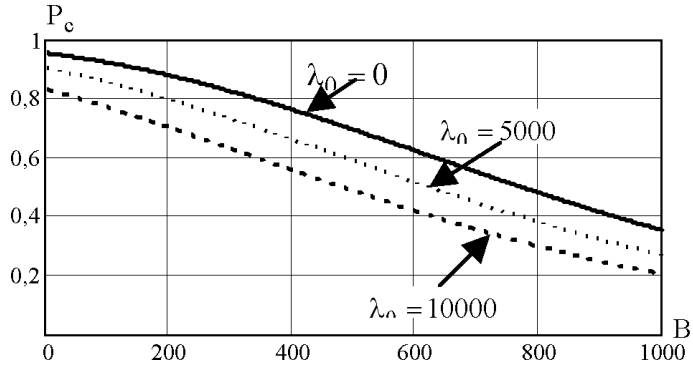

Рисунок 6 – Вплив бази СВ на виявлення ПО

Таким чином, використання широкосмугових сигналів у СС, що запитують дозволяє підвищити скритність, але при цьому погіршується завадостійкість, що не дозволяє підвищити завадозахищеності у цілому, розглядвємих інформаційних систем.

Висновки. Оцінка завадозахищеності СС, що запитують показує:
- існуючі СС, що запитують не мають енергетичної скритності та характеризуються низькою завадостійкістю;
- використання складних сигналів у якості СВ дозволяє підвищити скритність, але знижує завадостійкість.

У подальшому потрібно розглянути можливі шляхи та методи спадкоємного переходу до завадозахищених СС, що запитують.

Список літератури: 1. *Обод И.И.* Помехоустойчивые системы вторичной радиолокации. – М.: ЦНТИ, 1998. – 119 с. **2**. Теоретичні основи побудови завадозахищених систем інформаційного моніторингу повітряного простору / *В.В.Ткачев*, *Ю.Г.Даник*, *С.А.Жуков*, *І.І.Обод*, *І.О.Романенко*. – К.: МОУ, 2004. – 271 с. **3**. Комплексне інформаційне забезпечення систем управління польотами авіації та протиповітряної оборони / *В.В.Ткачев*, *Ю.Г.Даник*, *С.А.Жуков*, *І.І.Обод*, *І.О.Романенко*. – К.: МОУ, 2004. – 342 с. **4.** *И.И.Обод, А.А.Тюрин, А.В.Яровая* Сравнительный анализ существующих систем идентификации воздушных объектов // Системи управління, навігації та зв'язку: Збірник наукових праць. – Вип. 2(6). – К.: ЦНДІ НіУ, 2008. – С. 21-25. **5.** *Обод І.І., Тюрін О.О.* Спосіб ідентифікації об'єктів. Патент на корисну модель № 32641 від 26.05.2008.

Надійшла до редколегії 06.04.2009.