УДК 004.056.53

О.О. Стрельницький

Харківський національний університет радіоелектроніки, Харків

ПРОТИРІЧЧЯ ТА ПРОБЛЕМА ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

Показана неможливість здійснення захисту інформації ідентифікаційних систем спостереження на відомих принципах без суттєвого зниження інформаційних здібностей цих систем, що породжує проблему.

Ключові слова: *захист інформації,система спостереження.*

Вступ

Постановка проблеми й аналіз літератури. Основними елементами процедури контролю повітряного простору (КПП) [1] є аналіз повітряної обстановки та прийняття рішень.

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 визначаються складом та достовірністю інформації, на основі якої особа приймає рішення. Таким чином інформація, що циркулює в системи КПП повинна бути всебічно захищена.

Мета роботи – захист інформації систем спостереження повітряного простору.

Основна частина. Робота системи КПП та інформація, що циркулює в них повинні бути всебічно захищені від різного роду дестабілізуючих та шкідливих факторів, до яких відносяться[2]:

- штучні завади та електромагнітна несумісність;
- акти активної протидії функціонуванню системи КПП;
- акти несанкціонованого використання інформаційних ресурсів;
- акти перекручування інформації.

Основним інформаційним ресурсом (ІР) системи контролю КПП є первинні та ідентифікаційні системи спостереження (СС). Первинна СС надає дані про місцезнаходження ПО, тобто відповідає на завданні «де», а ідентифікаційна СС (ІСС) відповідає на запитання «хто» та дозволяє отримати польотну інформацію з борту ПО.

Наведені СС в певній мірі можуть відчувати вплив різного роду дестабілізуючих факторів і вимагають захисту інформації на етапу її отримання.

Під загрозою безпеки розуміється дія або подія, яка може привести до руйнування, спотворення чи несанкціонованого використання ІР, включаючи отримання, збереження, передавання і оброблювання інформації.

Загрози, як правило, прийнято ділити на ненавмисні, і навмисні. Джерелом перших можуть бути помилки в програмному забезпеченні, виходи з ладу апаратних засобів, неправильні дії користувачів і т.п. Умисні загрози мають на меті нанесення шкоди користувачам інформаційної системи (ІС) і, в свою чергу, поділяються на активні і пасивні.

Пасивні загрози, як правило, спрямовані на несанкціоноване використання ІР, не надаючи при цьому впливу на їх функціонування. Широке використання несанкціонованого використання інформації вторинних СС направлено на дуальне виявлення повітряних об’єктів (ПО), що використають ці СС. Ця особливість викликана примітивністю використаємого сигналу відповіді (СВ). Дійсно, у якості СВ вторинних СС використаються інтервально-часові та часово-частотні коди, які 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 ПО призводить до того, що ЛВ є жаданим об’єктом засобів радіотехнічній розвідки (РТР) супротивника.

Активні загрози мають на меті порушення нормального процесу функціонування системи за допомогою цілеспрямованого впливу на ІР. До активних загроз відносяться, наприклад, постановка навмисних корельованих завад (НКЗ) ІСС, що призводить до перекручування інформації про ідентифікацію ПО.

Несанкціоноване використання ІР, з одного боку, є засобом розкриття або компрометації інформації, а з іншого - має самостійне значення, оскільки, навіть не торкаючись користувацької або системної інформації, може завдати певної шкоди користувачам. Можливість несанкціонованого використання є тільки у ІСС. Дійсно існуючі ІСС побудовані за однаковими принципами:

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

Побудова ІСІ за такими принципами виключила як часові так і просторові різниці між корисними та імітованими сигналами. Ця особливість призводить то того, що зацікавлена сторона має можливість як несанкціоноване отримувати інформацію від ЛВ розглядаємих ІСС, так і подавляти їх роботу імітованими сигналами потрібної інтенсивності тобто здійснювати перекручування інформації зазначених СС.

Проведемо оцінку скритності існуючих ІСС яка визначає можливість несанкціоновано використати зазначених СС. 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.

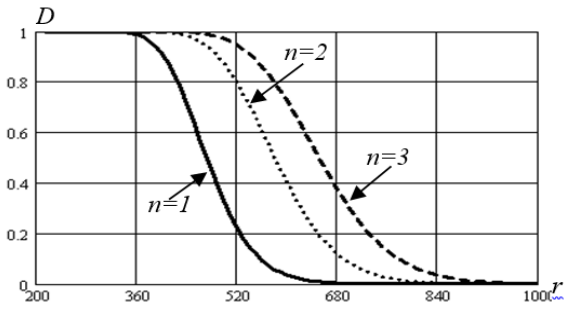

Рис. 1. Дальність виявлення СВ типових ЛВ

Наведені розрахунки показують, що виявлення СВ сучасних ЛВ типовою системою РТР не має складнощів, що указує на відсутність енергетичної скритності існуючих ІСС. При цьому слід зазначити, що виявлення сигналів здійснюється за зон дії первинних СС.

Проведемо оцінку імовірності одержання координатної інформації від ЛВ існуючих ІСС при впливі потоку СЗ, утвореного сумарним потоком СЗ сусідніх ІСС, потоком НКЗ супротивника і хаотичної імпульсної завади (ХІЗ).

При надходженні на вхід ЛВ ІСС потоку СЗ і ХІЗ будуть спостерігатися наступні основні ситуації, що приводять до виключення формування ЛВ сигналів відповіді (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 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 і зухвалих випромінювання СВ чи спрацьовування схеми ПБП.

Визначення імовірності цих подій будемо здійснювати у припущенні, що потоки СЗ (ПЗС) і ХІЗ діють на СЗ даного запитувача незалежно один від одного і що число 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 супротивника, інтенсивністю λ_1, та потік СЗ, що викликає спрацьовування схеми ПБП, інтенсивністю λ_2.

Використовуючи методику розрахунку зазначених імовірностей, досить докладно викладених у [3], одержуємо результати розрахунку імовірності вирішення інформаційної задачі (ІЗ) існуючими ІСС котрі наведені на рис. 2, 3.

На рис. 2 наведені розрахунки КГ відповідача, а на рис. 3 – імовірність виявлення ПО.

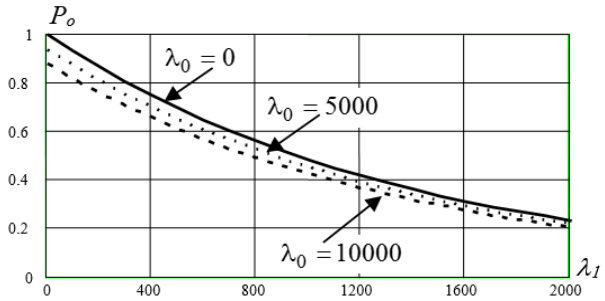

Рис. 2. Коефіцієнт готовності ЛВ

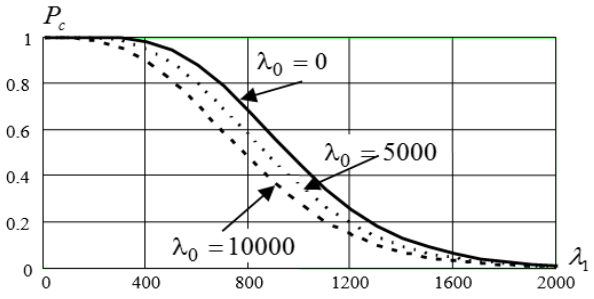

Рис. 3. Імовірність виявлення ПО ідентифікаційною СС

Аналіз наведених на рис. 2 і 3 розрахунків вирішення ІЗ існуючими ІСС показує, що можливість супротивника подавляти ІСС за рахунок несанкціо-

нованого використання ЛВ потрібної інтенсивності ставить під сумнів можливість роботи цих систем у конфліктних ситуаціях.

Дійсно, при постановці НКЗ інтенсивністтю 2000 імовірність вирішеня ІЗ практично дорівнює 0, що призводить до перекручивання інформації про ідентифікацію ПО.

Підвищення енергетичної скритності ІСС можливе за рахунок використання складних сигналів.

На рис. 4 показана дальність виявлення сигналів ЛВ при використанні у якості СВ складних сигналів з базою В=1000.

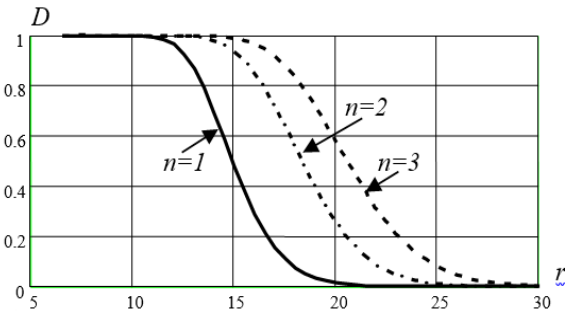

Рис. 4. Дальність виявлення сигналів ЛВ

Розрахунки, наведені на рис. 4, показують, що використання складних сигналів у якості СВ суттевим чином могли б підвищити енергетичну скритність ІСС і, як наслідок, захищеність інформації. 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 імовірності рішення ІЗ розглядаємими СС.

На рис. 5 і 6 наводяться розрахунки імовірності рішення ІЗІСС при використанні складних сигналів у ЛВ з базою 1000. Розрахунки наведені при фіксованих потоках СЗ.

Таким чином, використання складних сигналів у ІСС дозволяє підвищити енергетичну скритність, однак при цьому суттево погіршується імовірність вирішення ІЗ зазначеними СС, що є неприпустимим.

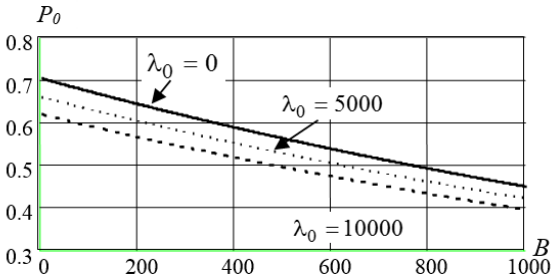

Рис. 5. Вплив бази СВ на КГ ЛВ

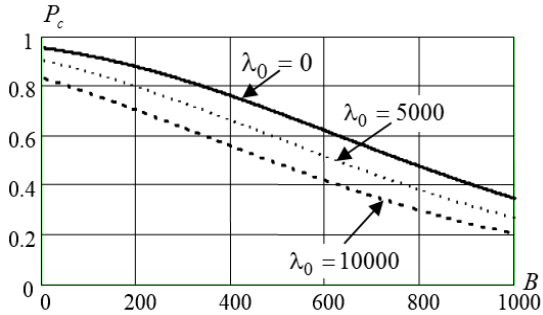

Рис. 6. Вплив бази СВ на виявлення ПО

Висновки

Наведені розрахунки показують протиріччя між потребою захисту інформації ІР та можливістю її реалізації на відомих принципах, що породжує проблему.

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. Захист інформації в системі організації повітряного руху / І.С. Биковцев, В.С. Дем'янчук, В.О. Клименко та інш. – К.: ДпОПР України, 2007. – 196 с.

3. Обод І.І. Інформаційна мережа систем спостереження повітряного простору / І.І. Обод, О.О. Стрельницький, В.А. Андрусевич. – Х.: ХНУРЕ, 2015. – 270 с.

Надійшла до редколегії 23.03.2017

Рецензент: д-р техн. наук проф. І.І. Обод, Національний технічний університет «ХПІ», Харків.

ПРОТИВОРЕЧИЕ И ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ СИСТЕМ НАБЛЮДЕНИЯ ВОЗДУШНОГО ПРОСТРАНСТВА

А.А. Стрельницкий

В статье показана невозможность осуществления защиты информации идентификационных систем наблюдния на известных принципах без существенного снижения информационных возможностей этих систем, порождает проблему.

Ключевые слова: *защита информации, система наблюдения.*

CONTRADICTION AND PROBLEM OF INFORMATION PROTECTION IN THE NETWORK OF OBSERVING AIR SYSTEMS

A.A. Strelnickiy

The article shows the impossibility of protecting the information of identification surveillance systems on known principles without significantly reducing the information capabilities of these systems, generates a problem.

Keywords: *information security, surveillance system.*