УДК 004.3.684:621.396.967.2

І.І. Обод, О.О. Стрельницький

Харківський національний університет радіоелектроніки, Харків

ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖІ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

У статті, на основі розгляду функцій системи контролю повітряного простору та вимог до інформації, що протікає в ній, надано аналіз існуючих систем спостереження. Показано, що захист інформації в мережі системи контролю повітряного простору повинен здійснюватися на етапах її отримання та при передачі. Показано, що в системі ідентифікації є можливість перекручування інформації, що не дозволяє прийняти вірне рішення та призводить до значних негативних наслідків.

Ключові слова: *система контролю повітряного простору, захист інформації.*

Вступ

Постановка проблеми й аналіз літератури. Досвід провідних країн світу свідчить, що в них вже досить тривалий термін існують національні єдині системи контролю повітряного простору (ПП) як військовою, так і цивільною авіацією. Очевидно, що при цьому досягається максимальна ефективність використання ПП.

Основні елементи процедури контролю ПП [1, 2] це: аналіз повітряної обстановки й 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

Вимоги до якості інформації та рівня її захищеності в системі контролю ПП визначаються її призначенням та роллю, яку вона відіграє.

Система контролю ПП як інформаційно-контролююча та інформаційно-керуюча система повинна забезпечувати виконання таких функцій:

- ведення безперервної розвідки ПП(*в реальному масштабі часу*);
- збору, накопичення і обробки даних від усіх засобів активного і пасивного радіоелектронного спостереження і розвідки;
- для розробки на основі цих даних карти повітряної обстановки;
- інформаційну достатність для функціонування системи контролю ПП;
- високу точність та неперекрученість інформації та ін.;
- втручання та організованої протидії.

Інформація, яка протікає в системі контролю ПП, повинна бути:

- функціонально та змістовно достатньою;
- своєчасною, оперативно поновлювальною;
- повнодосяжною за змістом та обсягом;
- точною та вірогідною;
- доступною для сприйняття та використання;
- завадостійкою та завадозахищеною;
- доступною для отримання, передачі, прийняття, обробки, зберігання, відображення, сприйняття, використання;
- об'єктивною;
- конфіденційною в міру потреби.

В системі контролю КПП існує багато джерел інформації. До них відносяться радіолокаційні, радіонавігаційні та зв'язкові засоби, електроні та магнітні носії інформації тощо. Всі вони в певній мірі можуть відчувати вплив різного роду дестабілізуючих факторів і вимагають захисту [3].

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

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

Слід зазначити, що захист інформації повинен здійснюватися на етапах її отримання, тобто в системах спостереження (СС) та при передачі в мережі.

Забезпечення завадостійкості та захищеності інформаційних систем (ІС) є органічною потребою у зв'язку з необхідністю забезпечення їх високонадійного функціонування.

Як показано у [5], ІМ складається з різноманітних СС як джерел інформації з відповідними етапами обробки інформації, каналів передачі інформації, засобів її отримання, аналізу, реєстрації, відображення, зберігання, операторів та користувачів інформації. Таким чином основою розглядаємої ІМ є СС.

Об'єктом спостереження у системі КПП є повітряний об'єкт (ПО) [4 – 6].Для системи контролю ПП основним видом спостереження є незалежне, некооперативне на основі локальної мережі спостереження в составі первинної СС та системи ідентифікації (СІ) за ознакою «свій-чужий» [6]. Дійсно, первинна СС надає дані про місцезнаходження ПО, тобто відповідає на завдання «де», а система ідентифікації відповідає на запитання «хто». Наявність вторинної СС дозволяє отримати польотну інформацію (РІ) з борту ПО. Первинна обробка інформації СС закінчується формуванням формуляру ПО, котрій включає:

$$\widehat{\vec{W}}_p, \vec{C}_p^{-1}, \text{РІ}, \text{"свій – чужий"}, T_i, \qquad (1)$$

де $\widehat{\vec{W}}_p$ – вектор стану ПО, $\vec{C}_p^{-1}$ – кореляційна матриця помилок, T_i – час формування інформаційного пакету (ІП).

Таким чином можливо стверджувати що якість та достовірність первинного ІП про ПО значною мірою визначає правильність рішення особи, що приймає рішення. Розглянемо коротко характеристики СС, інформація котрих формує ІП, тобто первинної, вторинної та ідентифікаційної. Характеристики цих СС наведені в табл. 1. Дійсно перераховані СС мають задовільну завадостійкість при роботі при наявності внутрішньосистемних та навмисних завад.

Таблиця 1

Характеристики СС, які формують первинний ІП

Інформаційна система	Завадостійкість	Скритність	Можливість несанкціонованого використання	Можливість перекручування інформації
Первинна	задовільна	задовільна	немає	немає
Вторинна	задовільна	відсутня	не обмежена	немає
Ідентифікаційна	задовільна	відсутня	не обмежена	висока

Енергетична скритність СС визначається інформаційним сигналом, який вони використають. Енергетична скритність передавачів первинних СС може бути підвищення за рахунок використання широкосмугових сигналів. Використання широкосмугових сигналів у вторинних та ідентифікаційних СС неможливе за принципом побудови цих інформаційних засобів. Це призводить до практичної відсутності енергетичної скритності цих інформаційних засобів (як наземних запитувачів, так і літакових відповідачів (ЛВ)) і, як наслідок, до широкого використання ЛВ зацікавленою стороною як до дальнього виявлення та навмисного інформаційного подавлення.

Можливість несанкціонованого використання є тільки у вторинних та ідентифікаційних СС. Дійсно існуючі запитальні СС, до яких відносяться і вторинні і ідентифікаційні, побудовані за однаковими принципами:

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

Побудова ІС 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 ІС, так і подавляти їх роботу імітованими сигналами потрібної інтенсивності. Покажемо це для системи ідентифікації.

Для цього припустимо, що на вхід ЛВ надходять хаотична імпульсна завада (ХІЗ) інтенсивністю λ_0, ПСЗ, що викликає випромінювання сигналів відповіді (СВ), що включає потік сигналів запиту (СЗ) сусідніх запитувачів і потік імітованих СЗ, інтенсивністю λ_1, і потік СЗ, що викликає спрацьовування схеми подавлення бокових пелюсток, інтенсивністю λ_2.

Допустимо, що загальні потоки СЗ складаються з k частин неімітостійкого режиму і $(1-k)$ частин імітостійкого режиму.

Коефіцієнт готовності (КГ) ЛВ, тобто імовірність відповіді на конкретний СЗ, наведено на рис. 1. Інтенсивність ХІЗ складала $\lambda_0 = 0;500;1000$.

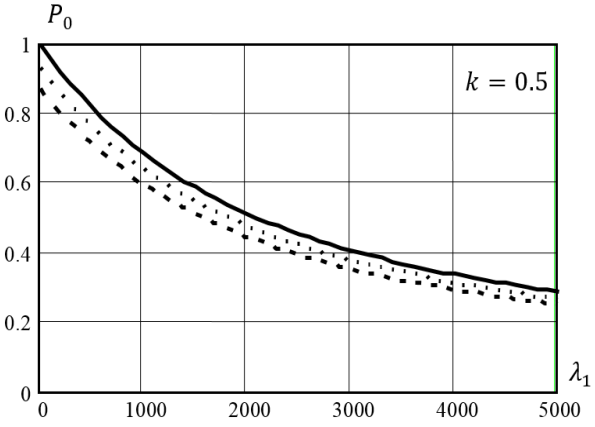

Рис. 1. Оцінка КГ ЛВ

Аналіз рис. 1 наглядно показує, що коефіцієнт готовності ЛВ ІС при інтенсивності потоку СЗ $\lambda_1 = 5000$ складає менш ніж 0,3. Наведені розрахунки показують можливість зацікавленій стороні як отримувати координати ПО за рахунок несанкціонованого використання його ЛВ, так і паралізувати ЛВ за рахунок постановки імітованої завади потрібної інтенсивності.

Наведені розрахунки показують, що існуючі вторинні та ідентифікаційні системи мають необмежену можливість несанкціонованого використання.

При цьому слід зазначити, що СІ має високу можливість перекручуванні інформації. Дійсно, СІ вирішують одну задачу – ідентифікації виявлених ПО за ознакою «свій-чужий». Існуючи СІ мають однаковий принцип функціонування і мають імітостійкий режим. Цей режим дозволяє, за рахунок використання значного поля СЗ та СВ, випадковим вибором чергового СЗ з поля СЗ та постійною зміною відповідності СВ конкретному СЗ, не дозволяє імітувати зацікавленій стороні «Я свій». Однак імітування СЗ потрібної інтенсивності (рис. 1) дозволяє зацікавленій стороні перекрутити інформацію про ідентифікацію ПО, тобто створити ситуацію при який ми не можемо ідентифікувати «свої» ПО.

Ця особливість СІ істотно знижує ефективність її використання, тому що зацікавлена сторона може паралізувати цю систему на значному видаленні за допомогою одного запитувача, що імітує СЗ необхідної інтенсивності.

Практика використання ІС знає немало випадків активної протидії їх функціонуванню, тому виникає необхідність в існуванні спеціальних засобів захисту від такої організованої протидії.

Деякі інформаційні системи, до яких відносяться і КПП, повинні бути захищені від можливого несанкціонованого втручання, недозволеного використання інформації.

Цінність інформації може змінюватись не тільки з часом, але й в залежності від міри її захищеності – завадозахищеності, захищеності від несанкціонованого доступу.

Висновки

Несанкціоноване втручання в роботу окремих СС інформаційної мережі може здійснюватися як на етапі отримання інформації, так і на етапах розповсюдження даних спостереження з метою порушення процесу її функціонування. Все це показує, що захистом інформації в системі контролю повітряного простору потрібно починати з систем спостереження.

Список літератури

1. Агаджанов П.А. Автоматизация самолетовождения и управления воздушным движением / П.А. Агаджанов, В.Г. Воробьев, А.А. Кузнецов. – М.: Транспорт, 1980. – 342 с.

2. Грачев В.В. Радиотехнические средства управления воздушным движением / В.В. Грачев, В.М. Кейн. – М.: Транспорт, 1975. – 237 с.

3. 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.

4. Комплексне інформаційне забезпечення систем управління польотами авіації та протиповітряної оборони / [Ткачев В.В., Даник Ю.Г., Жуков С.А. та інш.] – К.: МОУ, 2004. – 342 с.

5. Автоматизированные системы управления воздушным движением: Новые информационные технологии в авиации / под ред. С.Г. Пятко и А.И. Краснова. – СПб.: Политехника, 2004. – 446 с.

6. 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 19.01.2016

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

ЗАЩИТА ИНФОРМАЦИИ В СЕТИ СИСТЕМ НАБЛЮДЕНИЯ ВОЗДУШНОГО ПРОСТРАНСТВА

И.И. Обод, А.А. Стрельницкий

В статье, на основе рассмотрения функций системы контроля воздушного пространства и требований к информации, протекающей в ней, дан анализ существующих систем наблюдения. Показано, что защита информации в сети системы контроля воздушного пространства должна осуществляться на этапах ее получения и при передаче. Показано, что в системе идентификации имеется возможность искажения информации, что не позволяет принять верное решение и приводит к значительным негативным последствиям.

Ключевые слова: *система контроля воздушного пространства, защита информации.*

DATA PROTECTION IN THE NETWORK OF OBSERVATION AIRSPACE

I.I. Obad, A.A. Strelnickiy

The article, based on consideration of the functions of the control of air space and information requirements flowing in her analyzes of existing surveillance systems. It is shown that the protection of information in the control of air space should be carried out at the stages of its preparation and transmission. Show-but that the identification system it is possible to twist the information, which does not make the right decision and leads to significant negative consequences.

Keywords: *airspace control system, information security.*