УДК 004.045:621.396.96 **doi: 10.26906/SUNZ.2018.1.032**

І.І. Обод, О.О.Стрельницький

Харківський національний університет радіоелектроніки, Харків

ІНТЕГРАЛЬНИЙ ПОКАЗНИК ЯКОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

У статті обґрунтовано інтегральний показник якості захисту інформації в інформаційній системі яка створена на базі мережі систем спостереження повітряного простору, що дозволяє довести інформаційне забезпечення споживачів до рівня сучасних вимог шляхом інтеграції інформаційних ресурсів її підсистем. Показано, що інтегральним показником якості захисту інформації в зазначеній інформаційній системі може бути ймовірність інформаційного забезпечення яка є складовою ймовірностей виявлення повітряних об'єктів, виміру координат, поєднання інформації системи спостереження при формуванні формуляру повітряного об'єкту та імовірністю виявлення істинної траєкторії.

Ключові слова: *інтегральний показник якості, захист інформації, системи спостереження.*

Вступ

Постановка проблеми й аналіз літератури. Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Швидке вдосконалення інформатизації, проникнення її в усі сфери важливих інтересів зумовило, крім безперечних переваг, і поява ряду стратегічних задач. Посилюється небезпека несанкціонованого втручання в роботу інформаційних систем. Все це стосується і системи контролю повітряного простору (КПП) основними задачами котрої є 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 [1-4]. У зв'язку з цим, процеси отримання, обробки, зберігання, розподілу, сприйняття інформації та прийняття управлінських рішень в процесі КПП проходить в умовах гострого інформаційного протиборства і небезпечних дестабілізуючих (ненавмисних та навмисних) впливів, тому недооцінка питань їх інформаційної безпеки може привести до непередбачуваних наслідків, величезних матеріальних втрат і людських жертв.

Найбільш серйозними проблемами в області захисту інформації в системі КПП, як показано в [5], є захист інформації від несанкціонованого доступу до неї як в процесі отримання, так і в процесі розповсюдження та від навмисних програмно-технічних впливів на інформацію з метою її руйнування, знищення або спотворення.

Дійсно, інформаційним ресурсом системи КПП є системи спостереження (СС) [6]. Це зобов'язує захист інформації починати з моменту її отримання. Дійсно, як показано в [5] в інформаційних ресурсах системи КПП на етапі отримання інформації може бути здійснено несанкціоноване використання інформації, що призводить до зниження якості інформаційного забезпечення (ІЗ), а також перекручування інформації яке призводить до жахливих наслідків.

При оцінці систем захисту інформації (СЗІ) ІС фахівці стикаються з низкою труднощів, пов'язаних з проблемами формалізації предметної області та використанням статистичної інформацій. Це обумовлено неоднорідністю вибірки статистичної інформації, яка виникає через різноманітність ІТ, програмного забезпечення і технічних засобів, що використовуються при створенні інформаційних систем (ІС). У зв'язку з цим, в більшості випадків, для оцінки СЗІ ІС застосовуються експертні оцінки якісних характеристик з використанням слів професійної мови, що вносить нечіткість в підсумкові дані і є причиною складнощів, що виникають при їх обробці.

Мета роботи. Обґрунтування інтегрального показника якості (ІПЯ) захисту інформації в інформаційній мережі СС ПП.

Основна частина

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

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 [4].

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.

Таким чином, порушники технічного захисту інформації можуть створювати такі потенційні загрози для безпеки інформації в ІС:

- загрози конфіденційності (несанкціонованого отримання) інформації всіма можливими і можливими каналами її витоку;
- загрози цілісності (несанкціонованої зміни) інформації;;
- загрози доступності інформації (несанкціонованого або випадкового обмеження) і ресурсів самої інформаційної системи.

Для формування ефективної системи захисту інформації в мережі СС, що забезпечує її безпечне функціонування, необхідно використовувати комплексний підхід, що включає ряд етапів, одним з яких є формування системи критеріїв та розробка моделей-оцінки систем захисту інформації системи КПП.

Об'єктом спостереження у системі КПП є повітряний об'єкт (ПО) [6]. Для системи КПП основним видом спостереження є незалежне та некооперативне на основі локальної мережі спостереження в составі первинної СС та системи ідентифікації (СІ) за ознакою «свій-чужий». Дійсно, первинна СС надає дані про місцезнаходження ПО, тобто відповідає на завданні «де», а СІ відповідає на запитання «хто». Наявність вторинної СС дозволяє отримати польотну інформацію (*РІ*) з борту ПО.

Таким чином умова отримання достовірній та цілісній вищезазначеній інформації, особою що приймає рішення, і є показником якості захисту інформації. Дійсно, як показано в [5], найбільшу загрозу для ІС КПП є акт перекручування інформації, тобто виключення можливості достовірності визначення державної приналежності ПО. Ця можливість обумовлена принципом побудови вторинних СС, що дозволяє зацікавленій стороні, шляхом несанкціонованого використання цього інформаційного ресурсу здійснити перекручування інформації.

Ефективний захист інформації полягає не в тому, що боротьба із загрозами здійснюється під час їх прояву, а в тому, щоб ІС були притаманні такі завчасно надані властивості, які би виключали можливості реалізації будь-яких загроз. Тобто по суті це не боротьба з загрозами, а впровадження заходів щодо ліквідації вразливостей ІС, якими могли би скористатися потенційні загрози, наслідками яких можуть бути перекручення чи знищення інформації, несанкціоноване її використання.

При цьому слід зазначити, що історично (при низькій продуктивності ЕОМ та аналоговій обробці інформації у системах спостереження (СС) ІТ використалися починаючи з вторинної обробки даних (ВОД) СС ПП, а первинна обробка даних (ПОД) здійснювалася у СС. Це призводило до складностей у виборі показників якості ІЗ користувачів, тобто є неможливим єдиний параметр для оптимізації характеристик ПОД та ВОД [1]. Реалізація цифрової обробки інформації у СС та підвищення продуктивності ЕОМ дозволили здійснювати обробку даних СС починаючи з виходів фазових детекторів. У цьому разі використання ІТ дозволило підвищити рівень ІЗ, що забезпечило безпеку польотів, підвищення економічності й регулярності польотів цивільної й військової авіації в районі аеродрому, на повітряних трасах та у позатрасовому ПП. ІТ, у цій ситуації, припускають автоматизацію процесів отримання, збору, обробки й відображення інформації від різнорідних СС та здійснюють мережеву обробку даних. Тобто можливо стверджувати, що ІТ дозволили виконувати у СС первинну, вторинну та третинну обробки даних, що суттєвим чином збільшує надійність та якість ІЗ користувачів. ІЗ системи КПП здійснюється СС [1,2], як правило, сумісними, які включають до свого складу первинну та одну чи дві вторинні (запитальні). Це дає можливість сформувати повний формуляр ПО, який видається споживачам інформації.

При цьому слід зазначити, що ведучою є первинна СС, координатна інформація (КІ) ПО котрої і закладається у формуляр ПО. Обчислення КІ ПО вторинними (запитальними) СС потрібно тільки для поєднання даних первинних та запитальних СС, що суттєвим чином зменшує ІЗ користувачів.

Розглянемо структуру ІЗ користувачів на базі первинної та вторинної СС при виконанні первинної та вторинної обробки даних.

Завданням ПОД СС являється формування формуляру ПО, котрий включає:

- поточний вектор стану ПО з відповідною матрицею точності;
- польотну інформацію (РІ) за її наявності;
- ознаку «свій-чужий».

Це передбачає, що у кожній СС повинно бути здійснено:

- виявлення та вимірювання параметрів виявлених сигналів;
- виявлення та вимір координат виявлених ПО;
- декодування та обробка ПІ вторинною СС;
- поєднання координатної інформації (КІ) та РІ у вторинній СС;
- порівняння КІ ПО, отриманих ідентифікаційною і первинною СС, вторинною і первинною СС.

Задачами ВОД являються:

- виявлення траєкторії ПО;

- супровід траєкторій ПО;
- траєкторні розрахунки у інтересах споживачів інформації.

Структура містить виявлювачі сигналів (сигналів відповіді (СВ), з виходу якого знімається послідовність випадкових нулів і одиниць x_i. Таким чином, виявлення сигналу здійснюється за необхідними показниками якості, тобто F_{0i}, D_{0i}.

Послідовність нулів і одиниць з виходу виявлювачів сигналу проходить часову дискретизацію і поступає далі на входи виявлювачів і вимірювачів координат ПО. Алгоритм виявлення ПО зводиться до перевірки гіпотези H_0 про відсутність ПО проти альтернативної гіпотези H_1 про її наявність, тобто до утворення співвідношення правдоподібності й порівняння цього відношення з якимось наперед заданим числом, яке обирається, виходячи з припустимої ймовірності хибного виявлення. Рішення про виявлення об'єкту з показниками якості F_{li} і D_{li} надходить на вимірювач координат ПО. Оцінка координат миттєвого положення ПО робиться одночасно з виявленням ПО. Завдання вимірювача координат ПО полягає в тому, щоб на основі аналізу отриманої послідовності нулів і одиниць оцінити оптимальним чином координати ПО. Оптимальний алгоритм вимірювання координат синтезується, як правило, за критерієм максимальної правдоподібності.

Завдання виявлювача ПО полягає в тому, щоб на основі аналізу отриманої послідовності нулів і одиниць вирішити оптимальним чином, чи являє собою прийнята вибірка пачку сигналів або вона відноситься до завади.

Таким чином, при формуванні рішення про виявлення ПО з виходу вимірювача координат ПО видається оцінка вектору вимірювання координат $\hat{\vec{\alpha}}_i$, що характеризується кореляційною матрицею похибок $\vec{C}_i^{-1}$, тобто при формуванні сигналу про виявлення ПО з виходу вимірювача координат ПО кожної СС видається оцінка вектору вимірювання координат $\hat{\vec{\alpha}}_i$, що характеризується кореляційною матрицею похибок $\vec{C}_i^{-1}$.

Закінчується ПОД формуванням формуляру ПО, котрий включає:

$$\vec{W}_p, \vec{C}_p^{-1}, \text{PI}, \text{"свій – чужий"}.$$

При цьому слід зазначити, що поточний вектор стану ПО $\vec{W}_p$ з відповідною матрицею точності $\vec{C}_p$ складений на основі виміру координат ПО первинною СС. У результаті проведення ВОД формується результуючий вектор стану $\vec{W}_r$, котрий характеризується результуючою матрицею точності $\vec{C}_r$, а також екстрапольований вектор стану $\vec{W}_e$ з відповідною матрицею точності $\vec{C}_e$.

Виконання ТОІ передбачає поєднання інформації від декількох, рознесених на місцевості, СС, що потребує перерахунку координат ПО від різних СС у єдину координатну систему та приведення відміток до єдиного часу екстраполяцією векторів стану до чергового моменту поєднання інформації.

При цьому слід зазначити, що РІ та ознака «свій-чужій», отримані на етапі ПОД, автоматично приєднується до векторів стану та матриці точності, отриманих на етапах ВОД та ТОД.

ІПЯ ІЗ при використанні ІТ може бути ймовірність ІЗ, котра визначається ймовірністю ІЗ кожного з етапів обробки.

Для ПОД частковими показниками якості ІЗ можуть буди ймовірності правильного виявлення ПО кожною СС $P_i = D_{li}$, які є функціями

$$D_{li} = f(D_{0i}, F_{0i}, C_i, P_0) = f(q_{0i}, z_{0i}, C_i, P_0),$$

де $z_0(C)$ – аналоговий (цифровий) поріг виявлення сигналу (ПО), P_0 - коефіцієнт готовності відповідача літака, що є характерним для вторинної та ідентифікаційної СС.

При порівнянні та поєднанні даних, що потрібно для автоматичного складання формуляру ПО, критерієм є якість виміру координатної інформації, через імовірності цих дій до яких належать:

- ймовірність втрат правильної РІ;
- ймовірність спотворення РІ;
- ймовірність об'єднання КІ і РІ вторинної СС;
- ймовірність порівняння КІ первинної та ідентифікаційної СС;
- ймовірність об'єднання КІ і РІ у вторинній СС.

Коротко розглянемо названі ймовірності.

При обробці РІ схемою за критерієм k/m є ймовірність втрат правильної РІ у пристрої обробки

$$P_{vtr} = 1 - P_{PI}^k,$$

де P_{PI} - ймовірність видачі РІ з виходу запитальної СС у перших m інформаційних відповідях.

При вживанні у пристрої обробки схем підтвердження РІ за критерієм k/m ймовірність спотворення польотної інформації складе:

$$P_{isk.PI} = \sum_{i=k}^{m} C_m^i P_{isk}^i (1 - P_{isk})^{m-i},$$

де P_{isk} – ймовірність видачі запитальною СС хибної РІ.

РІ запитальних СС може поступати з деяким запізнюванням відносно КІ, т.з. номер дискрети приходу РІ.

$$N_d^{'} = N_d + T(KI)/r_d,$$

де N_d - номер дискрети приходу координатної інформації; T(KI) - запізнювання для запитальної СС, відповідне коду КІ; r_d - ціна дискрети дальності.

Практично ймовірність об'єднання координатної і польотної інформації складе:

$$P_{okp} = (1 - P_{vtr.p.i})(1 - P_{ick.PI})P\begin{Bmatrix} +N_o' \\ -N_o' \end{Bmatrix},$$

де $P\begin{Bmatrix} +N_o' \\ -N_o' \end{Bmatrix}$ - умовна імовірність приходу ПІ у стробі від $+N_o'$ до $-N_o'$ відносно КІ ПО.

Алгоритм об'єднання інформації в пристрої обробки побудований так, що одиночні відмітки СС об'єднуються, якщо азимутний кут між центрами пакетів не перевищує $\Delta\beta$, а різниця їх дальностей Δr.

За умови, що відхилення центрів пакетів в первинній і вторинній СС незалежні і підкоряються нормальному розподілу, імовірність об'єднання пакетів можна визначити з такого співвідношення

$$P_{poe} = 0,25 \times$$
$$\times \left[1 + \Phi\left(\frac{\Delta\beta}{\sqrt{2}\sqrt{\sigma_{\beta 1}^2 + \sigma_{\beta 2}^2}}\right)\right]\left[1 + \Phi\left(\frac{\Delta\beta}{\sqrt{2}\sqrt{\sigma_{r1}^2 + \sigma_{r2}^2}}\right)\right],$$

де $\sigma_\beta(\sigma_r)$ - середньоквадратичні відхилення азимутів (дальностей) центрів пакетів первинної та вторинної СС.

Ефективність алгоритмів виявлення траєкторії ПО характеризується ймовірністю виявлення істинної траєкторії D_{tr}, котра у загальному сенсі є складовою ймовірності виявлення ПО первинною СС, що є у свою чергу є складовою імовірності виявлення сигналів цією ж СС. Все це дозволяє визначити показник якості ІЗ на етапі ВОД у вигляді

$$P_{inf} = D_{tr}D_{12}D_{13}P_{okp}P_{poe1}P_{poe2}.$$

Висновки

Запропонований ІПЯ ІЗ споживачів дозволяє сумістити критерії ефективності обробки даних СС та захисту інформації в СС повітряного простору.

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 /Биковцев І.С., Дем'янчук В.С., та інш. – К.:ДпОПР України, - 2007. – 196 с.

3. Клименко В.О. Концептуальні положення інформаційної безпеки автоматизованих систем організації повітряного руху /В.О.Клименко // Захист інформації: Збірник наукових праць.– К.: НАУ, 2007. № 3. □ С. 55-64.

4. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Машиностроение, 2009 – 508 с.

5. Стрельницький О.О. Протиріччя та проблема захисту інформації в мережі систем спостереження повітряного простору / О.О.Стрельницький//Системи управління, навігації та зв'язку. □Полтава: □2017.□ Вип. 3(43). □ С. 66-68.

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 23.11.2017

Рецензент: д-р техн. наук, проф. О.А. Серков, Національний технічний університет «Харківський політехнічний інститут», Харків.

ИНТЕГРАЛЬНЫЙ ПОКАЗАТЕЛЬ КАЧЕСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ СИСТЕМ НАБЛЮДЕНИЯ ВОЗДУШНОГО ПРОСТРАНСТВА

И.И. Обод, А.А. Стрельницкий

В статье обоснована интегральный показатель качества защиты информации в информационной системе созданная на базе сети систем наблюдения воздушного пространства, что позволяет довести информационное обеспечение потребителей до уровня современных требований путем интеграции информационных ресурсов ее подсистем. Показано, что интегральным показателем качества защиты информации в указанной информационной системе может быть вероятность информационного обеспечения которая является составной вероятностей обнаружения воздушных объектов, измерения координат, объединения информации системы наблюдения при формировании формуляра воздушного объекта и вероятностью обнаружения истинной траектории.

Ключевые слова: *интегральный показатель качества, защита информации, системы наблюдения.*

INTEGRATED INDEX OF THE QUALITY OF INFORMATION PROTECTION IN THE NETWORK OF OBSERVING AIR SYSTEMS

I.I. Obod, A.A. Strelnickiy

The article substantiates the integral indicator of the quality of information protection in the information system created on the basis of the network of airspace surveillance systems, which allows to bring the information support of consumers to the level of modern requirements by integrating the information resources of its subsystems. It is shown that the information protection quality in the information system can be an integral indicator of the probability of information support, which is the composite probability of detecting air objects, measuring coordinates, combining the information of the observation system in the formation of the airspace form and the probability of finding the true trajectory.

Keywords: *integrated quality indicator, information security, surveillance systems.*