**Y. Scherbina,** PhD, **N. Kazakova,** DSc, **R. Bratchenko, H. Grabovskii**

## CALCULATION IN C # SPECIAL FUNCTIONS *ERF(X)* AND *ERFC(X)* FOR THE NEEDS OF CRYPTANALYSIS

*A variant of computation in C # language such special features as a function of an error, an incomplete error function and the function of the normal distribution, commonly used in the performance of tasks related to the testing of symmetric cryptographic systems. This software module is the most compact of the created in Visual Stu-dio.NET environment and can be used by developers of ciphers as part of their software.*

***Keywords:*** *cryptographic systems, cryptographic analysis, special functions, calculation.*

УДК 629.05:621.317

**О. О. Шелуха**

*Національний авіаційний університет, м. Київ*

## ОБРОБКА ІНФОРМАЦІЇ В СИСТЕМАХ СТЕЖЕННЯ ЗА ДИНАМІЧНИМИ ОБ'ЄКТАМИ

*В статті розглянуто методику обробку інформації для системи візуального спостереження за динамічними об'єктами. Визначено необхідність створення підсистеми обробки даних рухомої системи спостереження та виділення математичного апарату для визначення положення об'єкта, що постережуться, за даними, що передаються з оптично-електронного модуля. Першим кроком було наведено методику для визначення координат об'єкта спостереження в кадрі переданому з оптично-електронного модуля. Другим кроком було наведено розрахунки координат об'єкта в системі прямокутних координат в горизонтальній площині за допомогою кутових координат. В подальшому пропонується створення комплексної системи обробки даних для побудови тривимірної моделі об'єкта спостереження.*

***Ключові слова :*** *система прямокутних координат, рухома система стеження, спостереження динамічних об'єктів.*

**Вступ**

Сучасні системи обробки і аналізу інформації широко застосовуються в різних областях людської діяльності. Найбільш широке поширення вони отримали в областях навігації, системах стеження, забезпечення безпеки різних об'єктів, передачі та зберігання відеоінформації [1 – 3]. Особливе місце в розкритті проблеми сприйняття, інтерпретації, ідентифікації та опису руху об'єктів займає завдання стеження. Необхідність стеження за динамічними об'єктами і визначення параметрів їх руху пояснюється великою кількістю практичних застосувань, наприклад, при визначенні параметрів руху автотранспорту, при проведенні випробувань для забезпечення безпеки руху повітряних і морських об'єктів, при обробці і реалізації взаємодії цих об'єктів між собою.

При цьому важливим завданням є автоматична реєстрація, відстежування відносного переміщення і визначення параметрів динамічних об'єктів, розташованих в полі зору мобільного пристрою. Рішення даного завдання істотно розрізняються за складністю залежно від виду об'єкта, фону і розташування мобільної оптико-електронної системи.

Сучасний етап розвитку техніки характеризується переважним використанням плоских стаціонарних систем візуалізації зображень [4, 5]. У той же час виникає безліч проблемних питань, пов'язаних з аналізом тривимірних зображень, отриманих від рухомих систем відеоспостереження, які не можуть бути вирішені стаціонарними системами. Плоска проекція не є реальним відображенням дійсності, тому частина інформації про первинне зображення, незважаючи на високу якість, як правило, втрачається. Звідси виникає об'єктивна необхідність у створенні технологій, що будуть виконувати обробку цієї інформації та відновлювати втрачені дані. Підвищення вимог до точності, надійності і мобільності автоматичного виявлення і подальшого супроводу об'єктів змушує шукати нові рішення в сфері розробки алгоритмічного забезпечення для аналізу та обробки відеопослідовностей та застосовувати інформаційні технології нових типів. У зв'язку з цим необхідно вирішити такі завдання у сфері стеження за об'єктами.

**Постановка завдання**

Навігаційна система або комплекс, встановлений на рухомому носії – вертольоті або літаку, повинен забезпечувати швидке виявлення та розпізнавання об'єктів на значній відстані та визначати кутові координати для точної прив'язки об'єкта в системі прямокутних координат. Відомі статичні методи обробки інформації, такі як вимірювання кутових координат у системі прямокутних координат по двох координатах візування при точній прив'язці кожної з точок у прямокутній системі координат. Якщо ж вимірювання координат об'єкта виконуються рухомою системою, виникають додаткові труднощі, що вимагають використання точних методів інформаційної обробки, реєстрації координат об'єкта носія під час візування об'єкта пошуку, розробки спеціальних алгоритмів розрахунку координат об'єкта. Отже, необхідно створити математичний апарат для підсистеми обробки інформації в рухомій системі спостереження за динамічними об'єктами в системах реального часу [6].

**Викладення матеріалу**

Для виконання поставленого завдання широке застосування знаходять оптико-електронні пристрої (ОЕП), що володіють технічним зором і адаптуються до змінних умов роботи. Особливе місце у використанні ОЕП займає процес стеження за рухомими об'єктами, який застосовується в автоматичних системах відеоспостереження, системах аутентифікації доступу, при контролі якості виробів у виробничих процесах, проведенні випробувань і так далі. Також, для вирішення даного завдання в блоці обробки інформації можливо використовувати додаткові процедури оцінки таких геометричних параметрів спостережуваних зображень як, координати об'єкта, його траєкторію і швидкість. Це завдання дозволить вирішити використання якогось стаціонарного об'єкта, відносного якого і будуть обчислюватися дані параметри. Використання подібного методу дозволить ефективно і без істотних похибок здійснювати обробку інформації в блоці спостереження за динамічними об'єктами. Дані мобільні ОЕП можуть обробляти тривимірні зображення, функціонувати в реальному масштабі часу і ефективно використовуватися при практичній реалізації.

Завдання виділення динамічного об'єкта, що рухається по невідомої траєкторії, включає в себе одночасно відновлення зображення об'єкта і визначення параметрів його траєкторії. Етапи обробки інформації в бортовому комп'ютері включають наступне:

- локалізацію областей зображення;
- ідентифікацію динамічного об'єкта;
- визначення та створення бази даних просторових координат динамічних об'єктів.

Під локалізацією динамічних об'єктів розуміється виділення областей зображення як матриці $M \times N$, в яких безпосередньо містяться зображення динамічних об'єктів. Процес виявлення та локалізації об'єктів зображення відбувається шляхом обробки первинного та коригуючого кадрів $n$ та $(n+t)$:

$$Kp_{i,j} = Kn_{i,j} - K(n+t)_{i,j},$$

де $Kp_{i,j}$ – результуючий кадр зображення; $Kn_{i,j}$ – первинний кадр; $K(n+t)_{i,j}$ – коригувальний кадр. Первинний і коригувальний кадри зображення розбиваються на множині прямокутних областей $B_n$. Розмір області $B_n$ підбирається експериментальним шляхом залежно від розмірів динамічних об'єктів.

Первинний і коригувальний кадри зображення розбиваються на множину прямокутних областей $B_n$. Розмір області $B_n$ підбирається експериментальним шляхом залежно від розмірів динамічних об'єктів.

Позначимо сусідні с областю $B_n$ області як $B_n^m$, де $m$ – номер сусідньої області. Локалізація динамічних об'єктів зводиться до послідовної обробки множини прямокутних областей $B_n$ та перевіркою на умову (1), де $P$ – значення порога яскравості, що обирається дослідним шляхом. Якщо умова істинно більш ніж в половині області $B_n$, то робиться висновок про знаходження в даній області динамічного об'єкта, при цьому решта $B_n$ не аналізується, в іншому випадку область очищається, а всі посилання на неї від сусідніх областей видаляються. На наступному кроці перевіряється умова (1) для області, що відповідає $B_n^m$, якщо воно істинне, то область $B_n^m$ і область $B_n$ об'єднуються, при цьому область $B_n$ успадковує посилання на множини сусідніх областей області $B_n^m$:

$$\text{Якщо } |E_{K,n}^m(x,y) - E_{K+t,n}^m(x,y)| \geq P, \qquad (1)$$

де $E_{K,n}^m(x,y)$ – значення яскравості пікселя з координатами $(x,y)$ в $K$-му кадрі, $m$-й області, сусідній області $B_n$.

Тоді сусідніми областями створеної області будуть всі сусідні області вихідної і приєднаної області. В результаті утворюються зв'язкові області, які містять зображення рухомих об'єктів. Пошук динамічних об'єктів

починається по периметру кадру зображення, так як об'єкти в основному з'являються переважно по краях кадру. Після обробки $K$ і $K+t$ кадру отримуємо замкнуті області, в яких містяться динамічні об'єкти. Під ідентифікацією динамічних об'єктів розуміється зіставлення об'єктів на первинному і коригуючому кадрі, шляхом порівняння зовнішнього контуру і площі об'єкту. На першому етапі виділяються крайні точки контуру динамічного об'єкта:

$$d_1^i = \min(y);$$
$$d_2^i = \min(x);$$
$$d_3^i = \max(y);$$
$$d_4^i = \max(x),$$

де $i$=1, 2 – номер кадру.

На другому етапі відбувається зіставлення відповідних крайніх точок контурів динамічного об'єкта, отриманих при аналізі первинного та коригуючого кадрів, і за результатами зіставлення – перевірка наступної умови:

$$|d_1^1 - d_1^2| \,\&\, |d_2^1 - d_2^2| \,\&\, |d_3^1 - d_3^2| \,\&\, |d_4^1 - d_4^2| \le \varepsilon,$$

де ε – допустиме значення розбіжності, визначається дослідним шляхом. Якщо умова виконується, то об'єкт вважається ідентифікованим.

На наступному етапі відбувається визначення площі виділених об'єктів $S_1$ і $S_2$ для об'єктів, що перебувають на первинному і коригуючому кадрах відповідно. Для розрахунку площі об'єкта $S$ позначимо область всередині зовнішнього контуру об'єкта як $R$, що складається з множини пікселів $p$. Тоді площа об'єкта визначається виразом

$$S_i = \sum_{R_i} p_i,$$

де $i$ – номер кадру.

Розрахунок площі здійснюється як для об'єкта, отриманого при аналізі первинного кадру, так і для об'єкта, отриманого при аналізі коригуючого кадру.

Далі перевіряється умова відповідності площ об'єктів знаходяться на різних кадрах:

$$|S_1 - S_2| \le \xi,$$

де ξ – допустима похибка, обумовлена дослідним шляхом.

У разі, якщо лінійного переміщення не виявлено, а відбувається збільшення площі об'єкта, об'єкт ідентифікується як динамічний, такий, що рухається в площині $Z$. Для визначення просторових координат динамічних об'єктів розташуємо датчики зображення так, що їх оптичні осі будуть паралельні, а пряма, що проходить через оптичні центри, перпендикулярна оптичним осям, ця пряма називається базовою лінією, а її відрізок, укладений між оптичними центрами, В – базою.

Груба оцінка положення об'єкта може бути також отримана однією візирною точкою Ц. Для визначення координат об'єкта необхідно мати хоча б дві різні точки зчитування кутів візування, а відстань між цими точками – базу локації пеленгації – використати в якості відсутнього лінійного елемента обчислення координат.

Загальна ідея вирішення завдання прив'язки координат об'єкта в системі прямокутних координат полягає в наступному: нехай $B_1$, $B_2$ – точки візування на базі $B_1B_2$; $x_1$, $y_1$, $x_2$, $y_2$ – їх координати; $\beta_1$, $\beta_2$ кути візування. Тоді $X_Ц$, $Y_Ц$ – координати, об'єкта (цілі) однозначно визначаються шляхом обчислень (рис. 1).

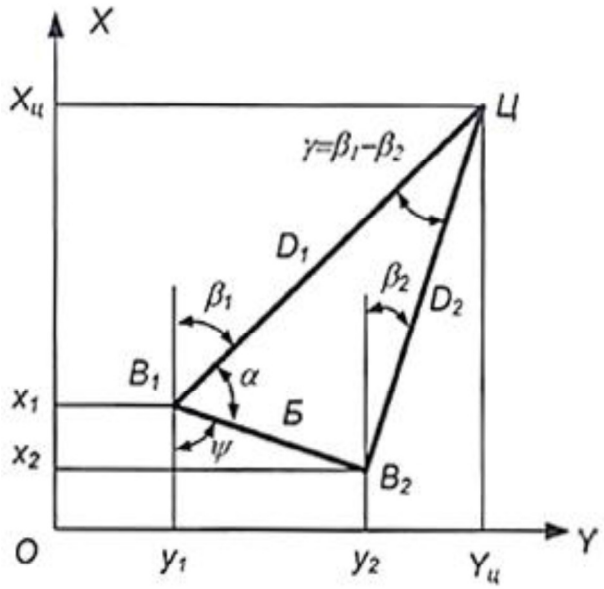


Рисунок 1 – Обчислення координат об'єкта в системі прямокутних координат

Безпосередньо з геометричних співвідношень маємо

$$X_Ц = x_2 + D_2 \cos\beta_2,$$
$$Y_Ц = y_2 + D_2 \sin\beta_2,$$

де $D_2$ – дальність $B_2Ц$. Відповідно до теореми синусів отримуємо

$$\frac{D_2}{\sin\alpha} = \frac{Б}{\sin(\beta_1 - \beta_2)}, Б = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2},$$

де $Б$=$B_1$, $B_2$ – лінійна база пеленгації, що може бути реалізована за допомогою

прямолінойної траєкторії руху носія. З рис. 1 можна одержати

$$\alpha = 180^{\circ} - \beta_1 - \psi,$$

де $\psi = arcsin\frac{y_1 - y_2}{Б} = arccos\frac{x_1 - x_2}{Б}$.

Звідки, провівши розрахунки отримуємо координати об'єкта в системі прямокутних координат [1]

$$X_{Ц} = x_2 + \frac{1}{\sin(\beta_1 - \beta_2)}[(y_2 - y_1)\cos\beta_1 - (x_2 - x_1)\sin\beta_1]\cos\beta_2,$$

$$Y_{Ц} = y_2 + \frac{1}{\sin(\beta_1 - \beta_2)}[(y_2 - y_1)\cos\beta_1 - (x_2 - x_1)\sin\beta_1]\sin\beta_2,$$

або

$$X_{Ц} = x_2 + \frac{1}{\sin\gamma}[\Delta y\cos\beta_1 - \Delta x\sin\beta_1]\cos\beta_2$$

$$Y_{Ц} = y_2 + \frac{1}{\sin\gamma}[\Delta y\cos\beta_1 - \Delta x\sin\beta_1]\sin\beta_2 \quad (2)$$

де $\gamma = \beta_1 - \beta_2$, $\Delta x = x_2 - x_1$, $\Delta y = y_2 - y_1$.

**Висновки**

Проведені дослідження дозволяють зробити наступні висновки. Запропоновано методику обробки інформації, що полягає у локалізації зображення динамічного об'єкта з можливістю подальшої його ідентифікації та вимірюванні кутових координат візування системи спостереження, встановленої на рухомому носії. Використання цієї методики спрощує обчислення координат об'єкта спостереження, але потребує прямолінійного руху відносно цього об'єкта.

Отримані результати можуть бути застосовані для створення бортового комп'ютеру, обробки інформації та створення керуючих сигналів для пристроїв, що встановлюються на рухомих носіях [6].

Використання визначених координат положення об'єкта, що спостерігається, в кадрі оптично-електронного модуля та визначення горизонтальних координат дозволить створювати базу даних тривимірних положень об'єкта спостереження.

**Список використаних джерел**

1. Кузьмин С. З. Основы теории цифровой обработки радиолокационной информации / С. З. Кузьмин. – М.: «Сов. радио», 1974. – 432 с.

2. Цибульська Є. О. Математичні моделі рухомих об'єктів / Є. О. Цибульська // Реєстрація, зберігання і обробка даних. – 2012. – № 2. – С. 25 – 37.

3. Кузнецов А. В. Многоканальная система повышения точности и живучести. – К.: Вища школа, 1994. – 258 с.

4. Малышев В. В. Оптимизация наблюдения и управления летательных аппаратов / В. В. Малышев, М. Н. Красильщиков, В. И. Карлов. – М.: Машиностроение, 1989. – 312 с.

5. Основы проектирования следящих систем. / под ред. Н. А. Лакоты. – М.: Машиностроение, 1978. – 392 с.

6. Шелуха О. О. Інформаційна технологія обробки даних в системах спостереження технічних об'єктів / О. О. Шелуха // Вимірювальна та обчислювальна техніка в технологічних процессках. – 2015. – № 4. – С. 202 – 205.

*Надійшла до редакції: 04.05.2016*

**Рецензент:** д.т.н. проф. Квасніков В. П., Національний авіаційний університет, м. Київ.

**А. О. Шелуха**

## ПОДВИЖНАЯ СИСТЕМА НАБЛЮДЕНИЯ ЗА ДИНАМИЧЕСКИМИ ОБЪЕКТАМИ

*В статье рассмотрена система визуального наблюдения за динамическими объектами. Выделена необходимость создания подвижной системы наблюдения и также математического аппарата для определения положения наблюдаемого объекта. Первым шагом приведено методику для определения координат объекта наблюдения в кадре оптико-электронного модуля. Вторым шагом приведены расчеты координат объекта в системе прямоугольных координат в горизонтальной плоскости с помощью угловых координат. В дальнейшем предлагается создание комплексной системы для построения трехмерной модели объекта наблюдения.*

***Ключевые слова**: система прямоугольных координат, подвижная система слежения, наблюдение динамических объектов.*

**O. O. Shelukha**

## MOBILE SURVEILLANCE SYSTEM OF DYNAMIC OBJECTS

*The article describes a system of visual observation of dynamic objects. It highlighted the need to create a mobile surveillance system and also the mathematical apparatus for determining the position of the observed object. The first step shows the methodology for determining the coordinates of the observation of the object in the optoelectronic module frame. The second step shows the calculations of the coordinates of the object in of a rectangular coordinate system in the horizontal plane using angular coordinates. In the future, we propose the creation of an integrated system for the construction of three-dimensional model of the object the mobile surveillance system.*

***Keywords:*** *rectangular coordinate system, mobile tracking system, monitoring of dynamic objects.*

УДК 519.715

**Ю. Б. Коваленко,** к.пед.н.

*Національний авіаційний університет, м. Київ*

## КОМП'ЮТЕРИЗОВАНА СИСТЕМА ЗАХИЩЕНОГО ЗАСТОСУВАННЯ НА ОСНОВІ ТЕХНОЛОГІЇ VOIP

*Розвиток електронної комерції і зацікавленість технологією IP як єдиного транспорту для передачі інформації будь-якого виду, дали можливість зв'язати мережу Інтернет з традиційною телефонною мережею загального користування і запропонувати клієнтам персоналізоване обслуговування та зручний засіб спілкування. Розроблено захищений програмний застосунок, що на відміну від існуючих підтримує встановлення захищеного з'єднання та забезпечує захист медіа даних, при цьому ґрунтується на рекомендаціях RFC, а отже може вільно взаємодіяти з іншими апаратними і програмними технологіями VoIP. На додаток, у застосунку реалізовано керування доступом на основі ролей, що підвищує безпеку та удосконалює можливості моніторингу діяльності користувача.*

***Ключові слова :*** *контролер конференцій, технології VoIP, мережа SIP з проксі-сервером.*

Все більшої популярності серед користувачів в усьому світі набувають телекомунікаційні рішення на основі технологій VoIP. VoIP – система зв'язку, що забезпечує передачу мовного сигналу по мережі Інтернет або по будь-яким іншим IP-мережам. Сигнал по каналу зв'язку передається в цифровому закодованому вигляді з метою усунення надмірності.

Програми для VoIP використовуються для проведення по мережах, заснованих на протоколі IP, розмов подібних телефонним [1].

Деякі програмні VoIP-додатки включають в себе сервери для конференцій, системи внутрішнього зв'язку, віртуальні FXO і адаптовані телефонні додатки, що підтримують одночасно VoIP і ТМЗК, такі як системи IVR, сервери dial in dictation, утримання дзвінка і запису розмов.

Отже, можна стверджувати, що IP-телефонія не лише покращує ефективність ведення роботи, а й створює нові ризики. Залишаються проблеми безпеки інформації, адже навіть найбільш використовувані софтфони є вразливими для найпростіших атак. Отже актуальним є питання розробки програмного телефону з використанням захищених протоколів зв'язку.

Існує два основних фактори які впливають на голосовий трафік по захищених каналах IP. Перший – час, необхідний для шифрування змісту повідомлення і заголовків і створення нових заголовків. Другий – збільшення розміру пакета із заголовками доданими до вихідного пакету IP. Також існують проблеми стиснення даних Quality of service.

Зауважимо, перші VoIP методи, які використовували голосовий потік як прихований носій інформації, запропонував Діттманн.

Була запропонована оцінка існуючої стеганографії з особливим акцентом на рішеннях, які підходять для VoIP. Був описаний інструмент SteganRTP, використовуючи молодший біт (LSB) із кодеку G.711.

Ванг та Ву в роботі «Інформація, прихована у VoIP потоках» запропонували використовувати