

**ШУМЕНСКИ УНИВЕРСИТЕТ „ЕПИСКОП
КОНСТАНТИН ПРЕСЛАВСКИ”
Факултет по математика и информатика
Катедра „Компютърни системи и технологии”**

СТАНИМИР КУНЧЕВ ЖЕЛЕЗОВ

**ОЦЕНКА НА ЕФЕКТИВНОСТТА НА СИСТЕМИ ЗА ЗАЩИТА НА
ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ**

А В Т О Р Е Ф Е Р А Т

на

ДИСЕРТАЦИЯ

за присъждане на образователна и научна степен „**Доктор**”

Професионално направление: 4.6 „Информатика и компютърни науки”

Научен ръководител:

Професор д.т.н. инж.. Атанас Иванов Начев

ШУМЕН

2013

**ШУМЕНСКИ УНИВЕРСИТЕТ „ЕПИСКОП
КОНСТАНТИН ПРЕСЛАВСКИ”
Факултет по математика и информатика
Катедра „Компютърни системи и технологии”**

СТАНИМИР КУНЧЕВ ЖЕЛЕЗОВ

**ОЦЕНКА НА ЕФЕКТИВНОСТТА НА СИСТЕМИ ЗА ЗАЩИТА НА
ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ**

А В Т О Р Е Ф Е Р А Т

на

ДИСЕРТАЦИЯ

за присъждане на образователна и научна степен „**Доктор**”

Професионално направление: 4.6 „Информатика и компютърни науки”

Научен ръководител:

Професор д.т.н.инж. Атанас Иванов Начев

ШУМЕН

2013

Дисертацията съдържа 183 стр., от които 21 фигури, 7 таблици и 15 стр. приложения. Използваната литература включва 120 литературни източници на български, руски и английски език. По темата на дисертацията са направени 6 публикации.

Дисертационният труд е обсъден и насочен за защита от разширен съвет на катедра „Компютърни системи и технологии“ при Факултета по математика и информатика на Шуменски Университет „Епископ Константин Преславски“ от 12.11.2013 г. и заповед на Ректора на Университета РД - 16 - 217/7.11.2013 г.

Докторантът работи в катедра „Компютърни системи и технологии“ на Факултета по математика и информатика при Шуменския Университет „Епископ Константин Преславски“.

Защитата на дисертационния труд ще се състои на ...02.2014 г. от 11:00 часа в зала 219 на Корпус 1 на Шуменския Университет, на открито заседание на научно жури в състав:

1. проф. д-тн Атанас Иванов Начев
2. проф. д-р Иван Кръстев Цонев
3. проф. д-р Маргарита Кръстева Тодорова
4. доц. д-р Иван Стефанов Христозов
5. доц. д-р Георги Стоянов Тодоров

Материалите за защитата са на разположение на интересуващите се в библиотеката на Шуменския Университет, корпус 3, етаж 1.

Автор: Станимир Кунчев Железов

Заглавие: ОЦЕНКА НА ЕФЕКТИВНОСТТА НА СИСТЕМИ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ

Тираж: 30 броя

Излиза от печат на 25 ноември 2013 год.

Университетско издателство „Епископ Константин Преславски“,
Шумен, 2013 г.

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Представената дисертация е във вид на научно - изследователски труд с формулирани цели и задачи, анализ и оценка на проблемите, формулиране и моделиране, модифициране на методи, разработване на алгоритми и компютърното им експериментиране.

1. Актуалност на проблема

Актуалността на проблема за повишаване на ефективността на системите защитата на информацията (СЗИ) се определя от тенденцията през последните години да се увеличават вътрешните заплахи за изтичане на чувствителна за организациите информация и от липсата на необходимите научно - технически и методически основи за осигуряване на защитата на информацията от използване на модерните стеганографски методи и средства за скриване на информация и създаване на скрити канали за предаване на данни. Използваните у нас сега средства за защита на информацията от инсайдери, използващи стегометоди за изтичане на чувствителна информация от организациите, не могат да осигурят достатъчна степен на сигурност на субектите, участващи в информационните взаимоотношения, и не могат в необходимата степен да противостоят на различни въздействия с цел скриване на тази дейност.

2. Цел и задачи на дисертационния труд

Необходимо е прилагането на ефективни системи и методи за стеганализ, които не само да се откриват скрити канали за изтичане на информация, но и това да се извършва в реално време. С използването на съществуващите методи за стеганализ това трудно може да се реализира поради тяхното недостатъчно бързодействие, което налага използване на методи за паралелна обработка на информацията.

Това определя **основната цел** на дисертационния труд:

Разработване на ефективни методи и средства за стеганалитична защита на информация, работещи в реално време.

За постигане на тази цел, в дисертационния труд се решават следните **основни задачи**:

1. Анализ на проблема за защита на информацията в компютърните системи в контекста на темата на дисертационното изследване.

2. Изследване на факторите, влияещи върху създаване на адекватни математическите модели за оценка и анализ на системите за защита на информацията.

3. Създаване на адекватни математически модели за оценка и анализ на системите за защита на информацията в компютърните системи и мрежи.

4. Формулиране на критерии за ефективност на системи за стеганалитична защита на информацията и предлагане на подходи за повишаване ефективността на системите за защита.

5. Анализ на съществуващи методи и средства за стеганализ с цел тяхното усъвършенстване за работа в реално време.

6. Разработка на програмни средства за стеганализ реализиращи предложените методи и алгоритми.

7. Определяне на състава на подсистема за стеганалитична система за защита на информацията (ССЗИ) и дефиниране на основните български термини в стеганографията и стеганализа, и на системите за стеганалитична защита на информацията.

3. Предмет на изследването: Аспекти на стеганалитичните средства за сигурност в компютърни системи и мрежи и методи за оценка на ефективността на СЗИ.

4. Работна хипотеза: Разработването на ефективни ССЗИ ще повиши ефективността на комплексната СЗИ.

5. Обект на изследването: Ефективността на стеганалитични методи и системи за защита на информацията в компютърните системи и мрежи.

6. Методи на изследването: Теория на вероятностите, математическа статистика, цифрова обработка на информацията, аналитично моделиране, метод Монте Карло, емпиричен анализ на ефективността на разработените методи чрез компютърно моделиране.

7. Научна значимост и новост на резултатите от дисертационния труд

Разработени са обобщени аналитични и статистически модели за оценка на заплахите и загубите в компютърните системи.

Формулирани са основни критерии за оценка на ефективността на стеганалитични алгоритми и програми.

Направена е модификация на алгоритми за последователен стеганализ и са разработени алгоритми за паралелната им реализация с кълъстерна система.

8. Практическа полезност и приложимост на резултатите

Направена е класификация на методите за стеганализ. Разработени са програми за паралелна реализация за стеганализ в реално време. Определен е съставът на подсистема за стеганалитична система за защита на информацията (ССЗИ) и подходи за определяне на нейната ефективност.

9. Аprobация на резултатите, получени в дисертационния труд:

Основните части от дисертационния труд са докладвани на различни научни семинари на обучаващото звено, на 5 научни конференции с международно участие в чужбина и у нас, и са публикувани в сборници и др. научни издания.

10. Структура и обем на дисертационния труд

Дисертационният труд е структуриран в увод, четири глави и заключение, използвана литература, списък на публикациите, свързани с темата на дисертацията и приложения.

Дисертационният труд съдържа 167 страници основен текст, 21 фигури, 7 таблици и 3 приложения. Използваната литература включва 120 литературни източници на български, руски и английски език. По темата на дисертацията са направени 6 публикации.

Номерацията на математическите формули, таблиците и фигурите в автореферата, съответстват на тези в дисертационния труд.

II. КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

В Увода са формулирани целта и задачите на дисертацията.

ГЛАВА ПЪРВА. ПРОБЛЕМИ ПРИ ОЦЕНКАТА НА СИСТЕМИТЕ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ И МРЕЖИ

Първа глава е въвеждаща в дисертационната проблематика. Съдържа следните параграфи:

1.1 Актуалност на проблема на дисертацията и приети ограничения

В дисертацията се разглежда подсистема за стеганалитична защита на информацията, тъй като това съответства на целта на дисертацията и работната хипотеза.

1.2 Подходи при разработката на системите за защита на информацията (СЗИ) за компютърните системи

Разгледани са основни положения при разработването на СЗИ. Определен е състава на ССЗИ, които се разглеждат като подсистеми на комплексните СЗИ.

1.3 Подходи за оценка на ефективността на системите за защита на информацията

Посочени са изисквания към СЗИ и показатели за ефективността им. Оценка на ефективността може да се осъществи само с използване

на комплексни показатели, имащи вероятностен или стойностен характер, защото съществуващите стандарти и документи не дават отговор на въпроса какво е реалното ниво на сигурността и колко ефективна е СЗИ.

1.4 За ефективността на стеганалитичната система за защита

Анализираны са редица критерии и показатели за ефективност на СЗИ. За оценка на ефективността на системите за стеганализ, е предложено да се използва комплексния показател

$$E_{ss} = f(P(S/D), P_{br}, T_{sa}, Q_m) \quad (1.1)$$

където T_{sa} – е време за изпълнение на стеганализа, $P(S/D)$ е вероятността за това, че в зададен интервал от време при определени условия системата за стеганализ ще открие скритото в контейнера съобщение, Q_m - разходи за въвеждане и функциониране на хардуера и софтуера, P_{br} е вероятността за безотказна работа на системата.

В дисертацията е въведен критерий за обща оценка на програми за стеганализ K_{sa} , който определя в каква част от тестваните стегофайлове са открити скрити съобщения.

$$K_{sa} = N_f / N_t, \quad (1.2)$$

където N_f е броят на стего файловете, в които стегоаналитичната програма е открила скрито съобщение, а N_t е общият брой на тестваните стего файлове.

1.5 Заплахи и атаки към компютърните системи

Един от най-важните аспекти на осигуряване на сигурността на компютърните системи е определянето, анализа и класификацията на възможните заплахи за тях. Оценката на вероятността за появата им, а така също и разработването на модели на заплахите и нарушенията могат да послужат за добра основа за провеждане на анализ на риска и формулиране на изискванията към СЗИ и подбор на най-ефективните средства за защита. Направена е класификация на видовете заплахи. Въведен е нов термин – **стегаинцидент** и е предложен негов модел. Чрез него е показана заплахата от реализиране на стегоканал за трансфер на секретна информация от инсайдери.

1.6 Изводи

1. За оценка на качествата на системите за защита на информацията (СЗИ) на компютърните системи трябва да се прилага системният подход, отчитащ всички взаимно свързани, взаимодействащи и изменящи се във времето елементи, условия и фактори. Голямата сложност на проблема и необходимостта от привличането на големи финансови ресурси често принуждават фирми и организации да не обръщат достатъчно внимание на този въпрос. Трудно е в рамките на едно изследване да се разгледат всички аспекти

2. През последните години значително нарастнаха заплахите и реалните щети за компютърните системи и мрежи от изтичане на чувствителна за организациите информация чрез злонамерени техни служители (инсайдери). Поради това в дисертацията се разглежда ролята на СЗИ в тази насока.

3. Акулен, но недостатъчно изследван у нас проблем е използването на теорията и практиката на съвременната компютърна и мрежова стеганография като ефикасно средство за защита на информацията.

4. Стеганалитичната СЗИ (ССЗИ) е съвкупност от апаратни и програмни средства за защита на данните в компютърните системи и мрежи от несанкционирано разгласяване, разкриване или използване, чрез методите на стеганографията и стеганализа. Тя е подсистема на комплексната СЗИ и се състои от две основни части - подсистема за стеганографско скриване на информация и подсистема за стеганалитична защита от НСД и изтичане на информацията чрез скрити канали.

5. На базата на анализа на външните и вътрешните заплахи и атаки за компютърните системи, е формулиран терминът „стегаинцидент“ и е разработен модел на стегаинцидент за реализиране на скрит стегоканал за кражба на секретни данни. Обоснован е изборът на подсистемата за стеганалитична защита от НСД и изтичане на информацията чрез скрити канали.

6. Оценка на ефективността на ССЗИ е необходимо да се извърши при вземане на решение за използване на СЗИ в конкретна ситуация, определяне на теглото на различни фактори за достигане на целта на защитата, намиране на способности за повишаване на ефективността на СЗИ и сравняване на алтернативни варианти на системи за защита. За целта са анализирани редица критерии и показатели за ефективност на СЗИ.

7. Производителността на системата за стеганализ може да се оцени чрез ефективността, приложимостта, практичността и сложността. За разлика от критерия „устойчивост“ на стегосистемите, за ефективността на стеганализа е необходимо определянето на други количествени критерии, което е сложна за изследване задача. Като такива за стеганалитичната СЗИ може да се използват вероятността за откриване на стегосъобщението, времето за това откриване, и др. В дисертацията е предложен комплексен показател за оценка на ефективността на системи за стеганализ. Посочено е, че ефективността

на реалната стегосистема не е идентична с ефективността на използвания в нея метод за стеганализ.

8. Ефективността на методите за стеганализ отразява точността на откриване. Предложени са количествени показатели за чувствителността, отчитащ теглото на грешките от 1 и 2 тип при стеганалитичното тестване, и точността, чрез коефициент на ефективност.

9. Анализът на достъпните литературни източници показва, че за да се разработят ефективни мерки и средства за стеганалитична защита е необходимо да се моделират и анализират заплахите за обработваната и обменяна информация в компютърните системи и мрежи, да се оценят последствията от евентуалните атаки, да се определят необходимите мерки и средства за защита, при обезателна оценка на ефективността.

ГЛАВА ВТОРА. МОДЕЛИ НА СИСТЕМИТЕ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ И МРЕЖИ

Във **втора глава** са разработени аналитични и статистически математически модели за оценка на системата за защита на информацията в компютърните системи и мрежи.

2.1 Особенности, влияещи на създаването на адекватни математическите модели за оценка и анализ на системите за защита на информацията

СЗИ представляват неделима част на компютърните системи и поради своята сложност могат да се разглеждат като самостоятелни системи, характеризиращи се редица специфични особености.

В тази глава се използва теорията на математическата статистика, теорията на вероятностите, в съчетание на методите за обработване на качествена експертна оценка. Причината да се избере това съчетание на подходи се определя от факта, че само използването теорията на вероятностите и математическата статистика изискват наличие на експериментални данни, притежаващи определена точност и достоверност, което за случаите на проблемната област не винаги могат да се осигурят и получат.

2.2 Обобщен модел за оценка на загубите в компютърната система (мрежа) от въздействието на възможни заплахи

Разработен е обобщен модел за оценка на загубите в компютърната система (мрежа) от въздействието на възможни заплахи.

Показано е, че общите загуби, причинени от настъпването на всичките n заплахи, при условия на тяхната независимост и адитивност на последствията от тях ще се определят като:

$$\bar{z} = \frac{1}{\sum_{i=1}^n \lambda_i} \sum_{i=1}^n \lambda_i z_i . \quad (2.6)$$

където z_i са относителните загуби, причинени от i – та заплаха, а λ_i е параметър на случайна величина с експоненциален закон на разпределение.

Загубите причинени от i – та заплаха трудно може да се определят в абсолютни стойности, тъй като икономическите загуби, загубите на време, обема унищожена информация и пр. не се поддават на обективна предварителна оценка в такъв формат. Поради това в дисертацията се предлага да се използват оценки на относителните загуби, получени в резултат на проведени експертни оценки, в предположение, че всичките заплахи за компютърната мрежа (система) представляват пълна група събития.

Оценката на загубите, причинени от всяка една заплаха се предлага да се извърши на базата на проведена експертиза.

$$z_{ij} = \frac{\sum_{\gamma=1}^3 z_{ij\gamma} \alpha_{\gamma}}{\sum_{\gamma=1}^3 \alpha_{\gamma}} . \quad (2.16)$$

Изразът (2.16) представлява експертната оценка за загубите, причинени от възникване на i – та заплаха, дадена от j – ти експерт.

2.3 Обобщен модел за оценка на въздействието на заплахите за компютърните системи и мрежи и определяне на степента на ефективност на системата за защита

За оценка на ефективността на системата за защита се въвежда показателя - коефициент на защита:

$$K = \frac{\bar{z}}{W} . \quad (2.20)$$

където \bar{W}_i са относителните загуби от въздействието на i – та заплаха.

Вероятността за предотвратяване на последствията от възникнали заплахи зависи от това до колко са отчетени всички фактори, качествени и количествени изисквания към системата за

защита на информацията в компютърните системи и мрежи при тяхното проектиране.

$$P_{ni} = f_i(x_{i1}, x_{i2}, x_{i3}, \dots, x_{ij}, \dots, x_{ik}) \quad (2.22)$$

където k е количеството предприети мерки за предотвратяване на последствията при възникване на i – та заплаха.

2.4 Статистически модел за оценка на въздействието на заплахите за компютърните системи и мрежи

Използването на аналитични модели за решаване на проблема за определяне на общите загуби от възникнали заплахи е свързано със следните ограничения:

- трудно може да се отчете въздействието на различните заплахи, когато количествата на възникването им за определен период от време представляват случайни величини с различни закони на разпределение;
- с редица ограничения може да се определи влиянието на едновременните възниквания на две и повече заплахи;

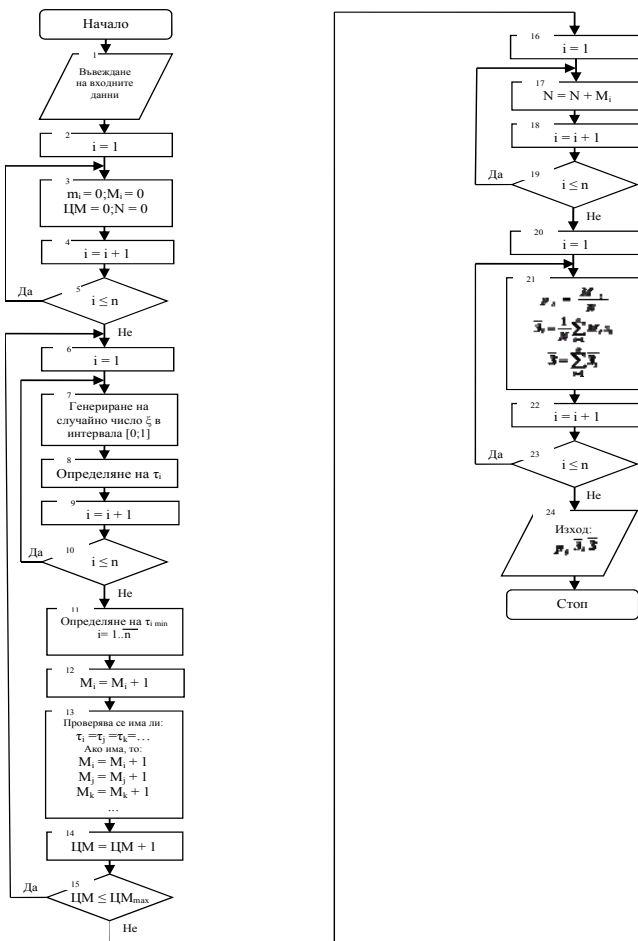
Използваният в дисертацията метод за статистическо моделиране (Монте-Карло) позволява да се избегнат посочените ограничения.

Разработен е статистически модел за оценка на въздействието на заплахите за компютърните системи и мрежи, който е представен със структурната схема, изобразена на фиг. 2.1. Схемата съдържа блокове за: въвеждане на входните данни (бл. 1); задаване на входните условия за моделиране (бл. 2 – бл. 3); непосредствено моделиране на възникването на заплахи (бл. 6 - бл. 15); проверка на зададените условия за количеството цикли (ЦМ) на моделиране (бл. 15); определяне на общия брой „възникналите” заплахи (бл. 16 – бл. 19); определяне на вероятностите на възникване на съответните заплахи, загубите, „възникнали” от всяка една заплаха и общите загуби от „възникналите” заплахи. За реализацията на статистическия модел са дефинирани следните броячи: броячи $M_i, i = \overline{1, n}$ на „възникналите” конкретни въздействия; брояч N на общия брой на „възникналите” смущаващи въздействия; брояч $ЦМ$ на количеството цикли на моделиране.

Загубите Δw_i , които настъпват с настъпването i – та заплаха ще се определят в съответствие с вероятността на възникването ѝ, т.е.

$$\Delta w_i = p_i z_i = \frac{M_i}{N} z_i, \quad (2.46)$$

където z_i са относителните загуби, причинени от i – та заплаха.



Фиг. 2.1

Общите загуби, причинени от всички n заплахи, при условия на тяхната независимост и адитивност на последствията от тях ще се определят като:

$$\bar{Z} = \sum_{i=1}^n \bar{Z}_i . \quad (2.47)$$

2.5 Статистически модел за оценка на степента на ефективност на системата за защита на компютърните системи и мрежи.

Разработен е статистически модел за оценка на степента на ефективност на системата за защита, схемата на който е изобразена на фиг. 2.2. Схемата съдържа блокове за: въвеждане на входните данни (бл. 1); формиране на началното състояние (бл. 2 – бл. 5) на следните броячи: броячи $M_i, i = \overline{1, n}$ на „възникналите” конкретни въздействия, брояч N на общия брой на „възникналите” смущаващи въздействия, брояч $ЦМ$ на количеството цикли на моделиране; определяне на времето на възникване на заплахи и дефиниране на типа на „възникнала” заплахата (бл. 6 – бл. 12); определяне на вероятността P_i за отстраняване на възникналата i – та, $i = \overline{1, n}$ заплахата (бл. 14 – бл. 16); проверка на изпълнението на зададените цикли на моделиране (бл. 17 – бл. 18); определяне на резултатите от моделирането (бл. 19 – бл. 22).

Степента на ефективност на системата за защита на компютърните системи се оценява чрез общите предотвратени загуби \overline{W} от въздействието на n заплахи

$$\overline{W} = \sum_{i=1}^n W_i . \quad (2.50)$$

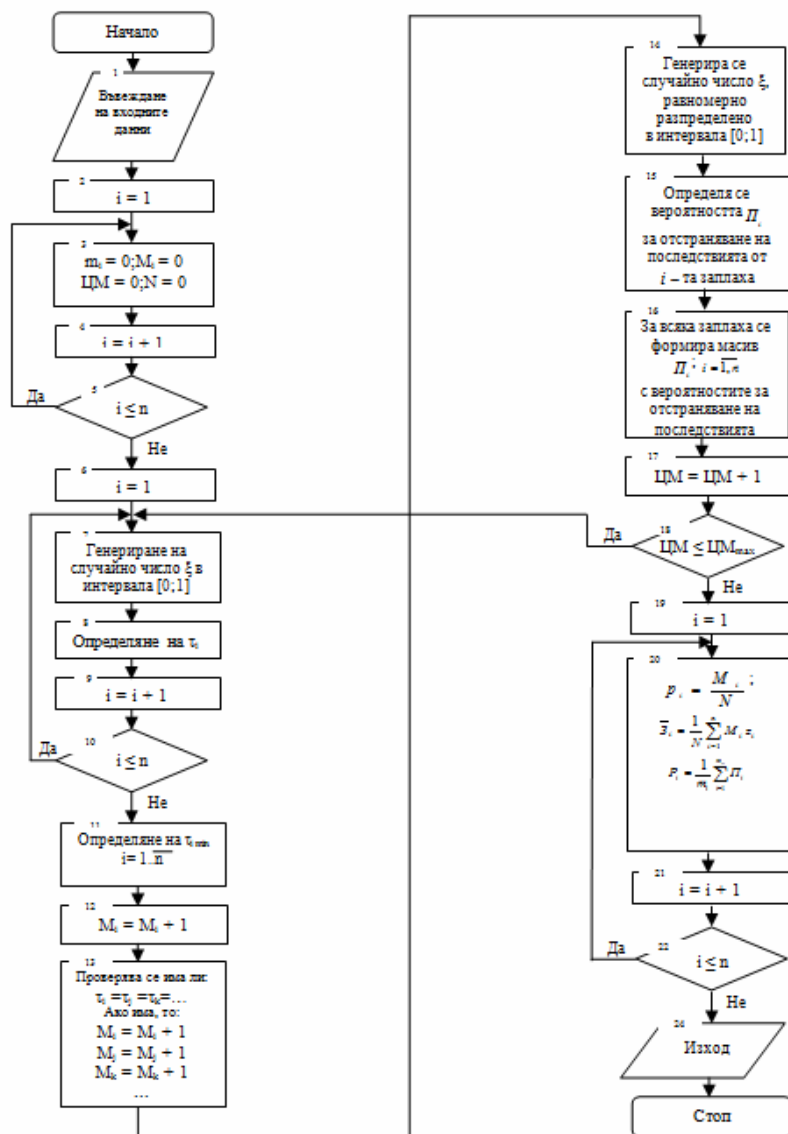
където Предотвратените загуби от въздействието на i - та заплахата.

2.6 Метод за синтез на оптимални системи за защита на информацията в компютърните системи и мрежи

Предложен е метод за синтез на системи за защита на информацията с отчитане на надеждностните характеристики на използваните средства, при следната теоретична постановка:

Системата за защита на информацията се състои от k структурни елемента и осигурява защита от n заплахи, при спазване на m изисквания към СЗИ. Всяко изискване $x_{i,j}$ дефинира съответен параметър на системата за защита на информацията, стойностите на който може да се мени в пределите:

$$x_{i,j \min} \leq x_{ij} \leq x_{ij \max} . \quad (2.51)$$



Фиг. 2.2

Известни са способите на организиране и структуриране на СЗИ на информацията, а така също и цената C_{η} на използваните технически и програмни средства за реализиране на СЗИ.

Решаването на задачата за синтез на СЗИ се извършва в два етапа:

1. Анализ на загубите в компютърната система (мрежа) от въздействието на възможните заплахи и определяне на степента на ефективност на защита от всяка една заплаха.

2. Синтез на оптимална система за защита на информацията с използване на методите на нелинейното програмиране.

Процесът на оценка на ефективността на системата за защита на информацията, в общия случай се изпълнява в следната последователност:

1. Анализ на компютърната система (мрежа), която може да бъде обект на атака.

2. Анализ на възможни злоумишленици, които биха могли да атакуват компютърната система (мрежа);

3. Анализ на потенциалните методи, които могат да се използват с най-голяма вероятност осъществяване на атаки.

4. Анализ на способността на системата за защита на информацията да противодейства на дефинираните, анализирани атаки.

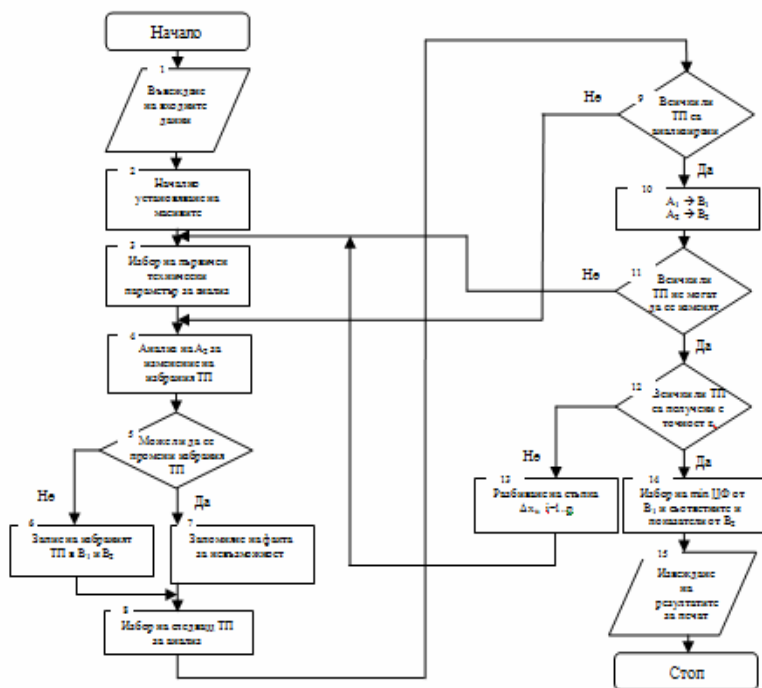
5. Оценка явява ли се икономически изгодно използването на системата за защита в конкретните условия.

За оценка на системата за защита на информационните ресурси в дисертацията е дефинирано подмножеството на заплахи и атаки, на чието въздействие може да бъде подложена компютърната система (мрежа), с оглед на определянето на устойчивостта на СЗИ, т.е. на способността ѝ да противодейства на тези атаки.

За решаване на задачата синтез на системата за защита на информацията в компютърната система (мрежа) се използва метода за представяне на условния екстремум във формата на последователност от задачи на безусловен екстремум с въвеждане на функция на „глоба”, която увеличава ценовата функция при нарушаване на допустимата област Ω . Това е комбинация от операции за търсене на безусловен екстремум с използване на метода на динамичното програмиране. Стойността на „глобата” зад предела на областта Ω е равна $+\infty$, а за областта допустими значения на аргумента - θ .

На фиг. 2.3 е представена схемата на алгоритъма за синтез на оптимална структура на система за защита на информацията в компютърна мрежа (система). За нейната реализация са дефинирани и

организираните следните масиви: A_1 и A_2 , съответно предназначени за съхраняване на значенията на целевата функция и техническите параметри на СЗИ, които характеризират предходните състояния на СЗИ:



Фиг. 2.3

B_1 и B_2 - съответно масиви, в които се съхраняват значенията на целевата функция и техническите параметри на СЗИ; $D(\Delta X_i), E(\varepsilon_i)$ – за съхраняване на текущи и предишни значения на стъпките на изменение $\Delta X_1, \Delta X_2, \Delta X_3, \dots$ на техническите параметри на системата за защита на информация; $X_{\min i}$ – за съхраняване на минималните значения на техническите параметри на

системата за защита на информацията; $X_{\max i}$ – за съхраняване на максималните значения на техническите параметри на СЗИ; P_{ki} – за съхраняване на показателите за качество, получени при всяка стъпка на процеса на моделиране.

2.7 Изводи :

1. Извършен е анализ на факторите, влияещи на разработването на адекватни математически модели за оценка и анализ на системите за защита на информацията и е избран подход за математическо описание на СЗИ в контекста на дефинираната тема за дисертационно изследване.

2. Разработен е обобщен аналитичен модел за оценка на въздействието на възможните заплахи за информацията, обработвана, предавана и съхранявана в компютърните системи (мрежи).

3. Разработен е обобщен аналитичен модел за оценка на загубите в компютърните системи (мрежи) от въздействието на възможни заплахи. Дефинирани са основни показатели за извършване на такъв тип оценки.

4. Предложен е статистически модел за оценка на въздействието на възможните заплахи за информацията, обработвана, предавана и съхранявана в компютърните системи (мрежи). Доказана е адекватността на разработения за целта аналитичен математически модел.

5. Разработен е статистически модел за оценка на загубите в компютърните системи (мрежи) от въздействието на възможни заплахи. Доказана е адекватността на разработения със същата цел аналитичен математически модел.

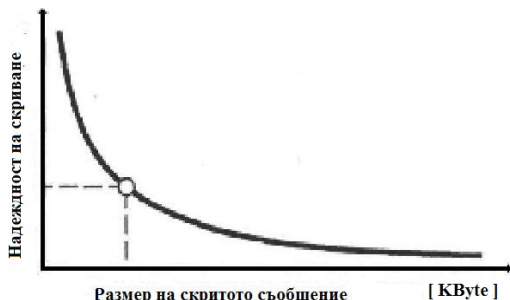
6. Предложен е метод за синтез на оптимални системи за защита на информацията в компютърните системи (мрежи), базиращ се на разработения за целта аналитичен математически модел.

ГЛАВА ТРЕТА. АНАЛИЗ И ОЦЕНКА НА ЕФЕКТИВНОСТТА НА МЕТОДИТЕ ЗА ОТКРИВАНЕ НА СТЕГАНОГРАФСКА ИНФОРМАЦИЯ

Глава трета е въведение в стеганализа и оценка на ефективността му.

3.1 Основни термини в стеганализа.

Формулирани са основни термини в стеганографията и стеганализа. Много термини свързани с конкретните стегометоди и стегоалгоритми, постоянно се обновяват, поради това едва ли всички могат да се разгледат в дисертацията. За оценка на предимствата и недостатъците на стегосистемите, трябва да се имат пред вид техните основни характеристики - сигурност и стегокапацитет.



Фиг. 3.1 Зависимост на надеждността на скриване на съобщението от неговия размер

В зависимост от поставените пред стеганалитика задачи и ресурсите, с които той разполага, могат да бъдат използвани както пасивни методи за стеганализ (анализ на наличност на скрита информация) и активни методи (промяна на потенциалните стего с цел модификация или унищожаване на скритата информация). В някои публикации стеганалитикът се класифицира като пасивен, активен или злонамерен. В зависимост от това той може да създава различни **стегозаплахи**.

В зависимост от наличната предварителна информация за стеганалитика, и по аналогия с криптоанализа, може да се разграничат следните условия за провеждане на **пасивни** стегоатаки, които са най – характерни в практиката на стеганализа.

- при известен само стегофайл – това е най-сложната за реализация пасивна атака, при която трябва да се установи наличието на секретен канал;

- при известен контейнер – стеганалитикът разполага със стего и оригиналния празен контейнер, и разкрива тайното съобщение чрез сравняването им.

- при известна стеганография – известен е стегоалгоритъма, празния контейнер и стегофайла;

- при известно скрито съобщение;

- при известен стегометод и стегофайл;

- при избрано съобщение - известни са стегоалгоритъма и тайното съобщение, и се създава стеганалитичен файл с цел бъдещ стеганализ и сравнение.

3.2 Класификация на методите на компютърния стеганализ

Подобно на всеки друг сложен процес, стеганалитичните методи могат да бъдат класифицирани по много критерии . По принцип има два генерални похода при стеганализа – субективен и технологичен,

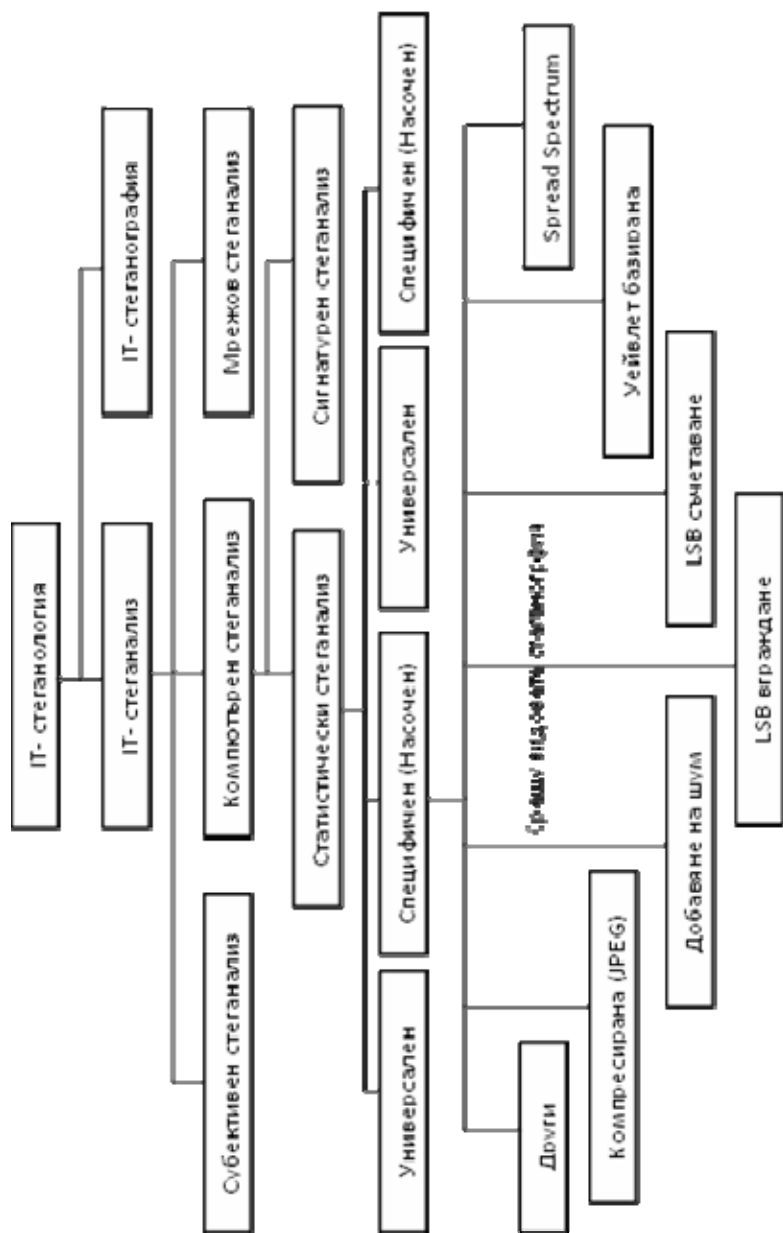
осъществяван с високотехнологични средства – компютри, физически, химически, електронни, биологични и други средства . Според това, дали за откриването на използването на стеганографски техники за скриване на съобщения в контейнерите се използват сигнатурите на тези методи или статистическата обработка на стегофайла, класификацията на методите за стеганализ може да се направи в два големи класа- сигнатурен и статистически. Това е и най-често срещаната в публикациите класификация. Статистическият стеганализ е по - мощен от сигнатурния, защото математическите методи са по - чувствителни от човешките възприятия . Тази група методи определят същността на стеганализа - откриване на наличието на скрита информация.Статистическият анализ може даде информация дали дадено изображение е стеганографско като провери дали статистическите му характеристики се отклоняват от нормалните.

Насочените (специфичните) методи за статистически стеганализ от своя страна могат да бъдат класифицирани на базата на съответните стегометоди, срещу които са насочени.

Направена е класификацията на методите и алгоритмите за стеганализ (Фиг. 3.2).

Извършен е анализ и оценка на следните известни методи за стегоанализ и са определени предимствата и недостатъците им, с цел усъвършенстване на подобни методи:

- Хистограмна атака (Хи-квадрат)
- Метод на анализа на двойки извадки
- Метод за стеганализ на графични файлове с използване на компресия на данните
- Стеганализ използващ показателите за качество на изображението
- Метод на универсален сляп стеганализ основан на цветови уейвлет преобразувания
- Метод за стеганализ базиран на разликите в изображението при калибриране и субдискретизация
- Обобщен метод на универсален стеганализ
- Изчислителни имунни системи (Computational Immune Systems - CIS)



Фиг. 3.2

В дисертацията са разработени са няколко алгоритъма за стеганализ.

3.3. Алгоритъм за стеганализ на графични файлове с използване на метода χ^2

Разработен е алгоритъм за стеганализ на графични файлове с използване на метода χ^2 структурата на който е представена на фиг.

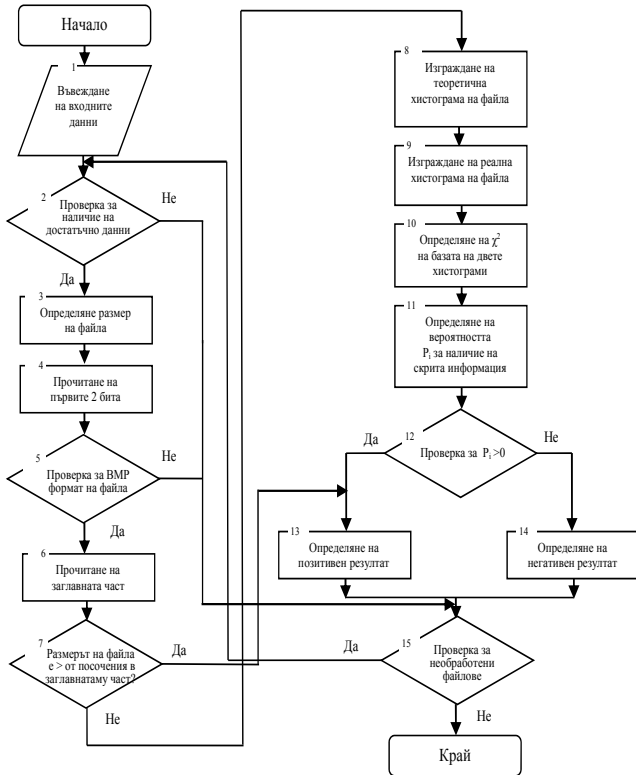
3.4. Той включва следните блокове: въвеждане на входни данни, т.е предстоящите за анализ графични файлове-бл. 1; проверка на наличието на достатъчна информация в изходните данни и дали са в нужния формат за извършване на стеганализ-бл. 1-5; проверка на съответствие между зададения обем на файла и реалната му големина-бл. 6 и бл. 7; определяне на наблюдаваните и очакваните честоти на срещане на двойките от съседни стойности (PoV)-бл. 8-9; определяне на параметъра χ^2 -бл. 10; определяне на вероятността за наличие на скрито съобщение (стегограма) – бл. 11; вземане на решение за наличие на стегограма в анализирания файл – бл. 13 или за неговото отсъствие – бл. 14; проверка за наличие на неанализирани файлове за съдържание на скрита информация – бл. 15.

Анализ на времевите характеристики на разгледания алгоритъм е даден в глава 4 на дисертацията.

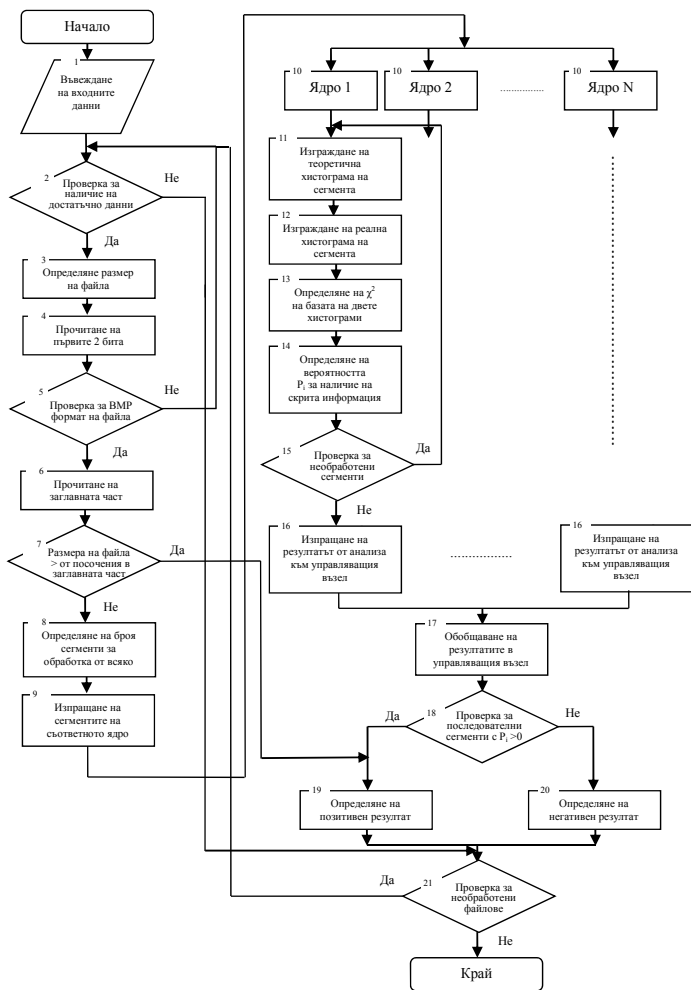
3.4. Алгоритъм за паралелен стеганализ на графични файлове с използване на метода χ^2

Разработен е алгоритъм за паралелен стеганализ на графични файлове, представен на фиг.3.5. Той съдържа: въвеждане на входни данни, т.е предстоящите за анализ графични файлове-бл. 1; проверка на наличието на достатъчна информация в изходните данни и дали са в нужния формат за извършване на стеганализ-бл. 1-5; проверка на съответствие между зададения обем на файла и реалната му големина-бл. 6 и бл. 7; разделяне на входния файл на сегменти – бл. 8; изпращане на сегментите към ядрата на клъстера – бл. 9; във всяко ядро на клъстерната система се реализира следната обработка: определяне на наблюдаваните и очакваните честоти на срещане на двойките от съседни стойности (PoV) - бл. 11 - 12; определяне на параметъра χ^2 -бл. 13; вземане на решение за наличие на стегограма в текущия сегмент – бл. 14; проверка за наличие на неанализирани сегменти – бл. 15; изпращане на резултатите от анализа към управляващият възел на на клъстерната система – бл. 16; обобщаване на резултатите от всички възли на системата – бл. 17; вземане на решение за наличие на скрита информация в анализирания файл, на базата на обобщените резултати –

бл. 18; проверка за наличие на неанализирани файлове за съдържание на скрита информация – бл. 21.



Фиг 3.4



Фиг. 3.5.

3.5. Алгоритъм за стеганализ на графични файлове с използване на компресия на данните

Алгоритъмът е модификация на метода за стеганализ на графични файлове с използване на компресия на данните.

В основата на разработения алгоритъм стои факта, че изходния контейнер и добавяната в него информация са статистически независими, за това при добавянето на скрити данни в контейнера размера му при компресиране е по-голям в сравнение с размера при компресиране на изходния празен контейнер.

Разработения алгоритъм за стегоанализ на графични данни използва алгоритми за компресиране на данни за проверка на статистическата независимост на данните. За компресиране се използват широко разпространени архивиращи програми.

Нека Z е бинарната последователност от байтове в полето на данните на избрания контейнер – изображение с формат BMP, и $|Z| = N$ е дължината на последователността - размер на контейнера.

Нека $Arh(Z)$ е алгоритъмът за компресия, реализиран с архивиращата програма, приложена към входната последователност Z на контейнера, а $Steg(Z)$ е стегоалгоритъма, реализиран чрез софтуера, скриващ последователността на съобщението M в контейнера. Последователността $S = Steg(Z)$ е получената от Z нова двоична последователност на стегофайла след приложен върху нея стегоалгоритъм.

Нека с $K_e(Z)$ бъде означен коефициентът на компресия на входната последователност, определен с формулата:

$$K_e(Z) = \frac{|Z|}{|Arh(Z)|} \quad (3.19)$$

Нека с $K_f(S)$ бъде означен коефициентът на компресия на S , определен с формулата:

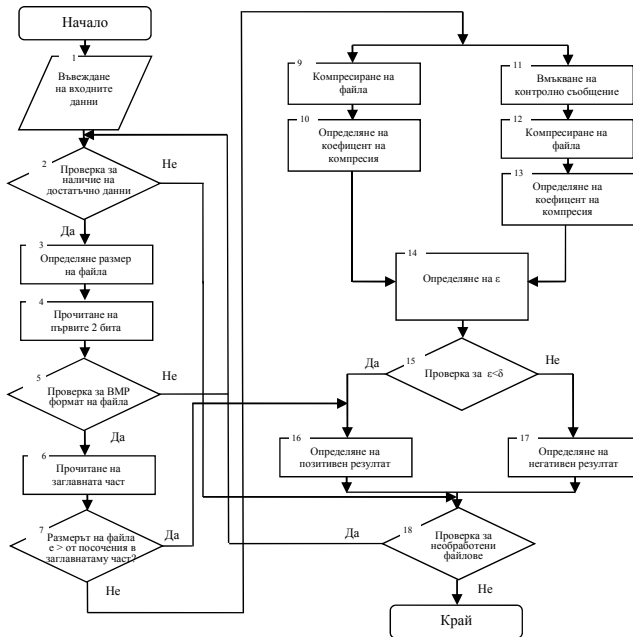
$$K_f(S) = \frac{|S|}{|Arh(S)|} \quad (3.20)$$

Нека ε е разликата между тези два коефициента зададена с:

$$\varepsilon = K_e(Z) - K_f(S) \quad (3.21)$$

$\varepsilon_f = K_f(S) - K_{ff}(S)$ е разликата между коефициентите на компресия на S и същия след вграждане на контролно стегосъобщение, тогава параметър $\delta = \varepsilon - \varepsilon_f$ може да се използва за да се определи

факта на въвеждане на информация. Избират се гранични значения за δ и се прави оценка на стойност на величината, дали превишава граничната стойност.



Фиг. 3.6

Структурата на предложения алгоритъм е представена на Фиг. 3.6 и съдържа следните блокове: въвеждане на входни данни, т.е. предстоящите за анализ графични файлове - бл. 1; проверка на наличието на достатъчна информация в изходните данни и дали са в нужния формат за извършване на стеганализ - бл. 1 – бл. 5; проверка на съответствие между зададения обем на файла и реалната му големина - бл. 6 и бл. 7; компресиране на входния файл – бл. 9; определяне на коефициент на компресия на входния файл – бл. 10; въвеждане на контролно стегосъобщение – бл. 11; компресиране на получения стегофайл – бл. 12; определяне на коефициент на компресия на стегофайла – бл. 13; определяне на ϵ - бл. 15; вземане на решение за наличие на стегограма в анализирания файл – бл. 16 или за неговото

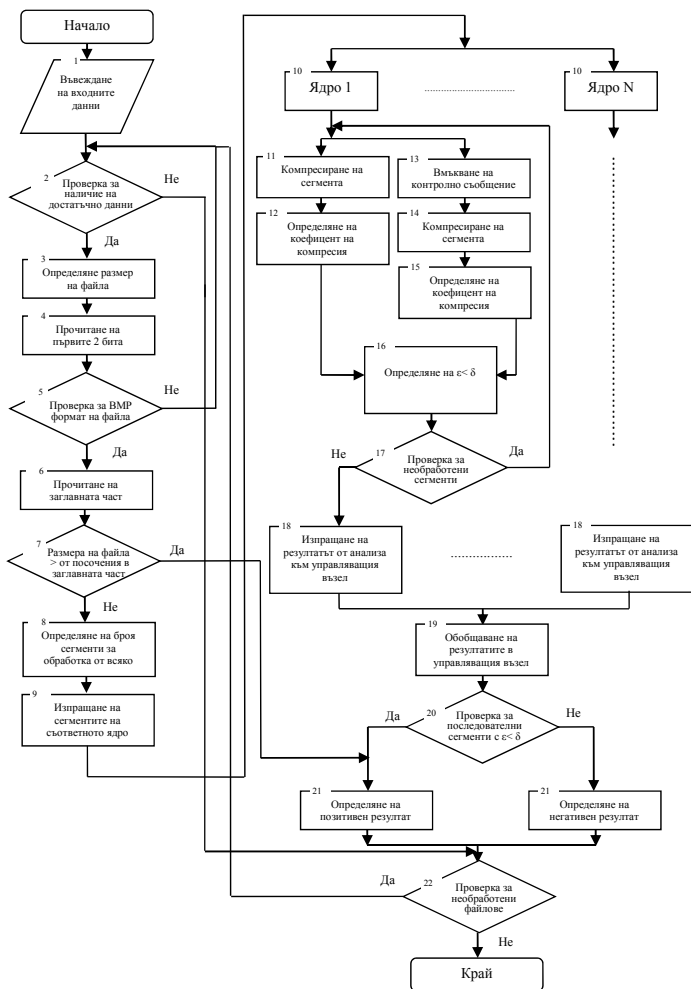
отсъствие – бл. 17; проверка за наличие на неанализирани файлове за съдържание на скрита информация – бл. 18.

Анализ на времевите характеристики на разгледания алгоритъм е даден в глава 4 на настоящото изложение.

3.6. Алгоритъм за паралелен стеганализ на графични файлове с използване на компресия на данните

Разработеният алгоритъм за паралелен стеганализ на графични файлове с използване на компресия на данните е представен на фиг. 3.7. Той съдържа: въвеждане на входни данни, т.е. предстоящите за анализ графични файлове-бл. 1; проверка на наличието на достатъчна информация в изходните данни и дали са в нужния формат за извършване на стеганализ-бл. 1-5; проверка на съответствие между зададения обем на файла и реалната му големина-бл. 6 и бл. 7; разделяне на входния файл на сегменти – бл. 8; изпращане на сегментите към ядрата на клъстера – бл. 9; във всяко ядро на клъстерната система се реализира следната обработка: компресиране на входния сегмент – бл. 11; определяне на коефициент на компресия на входния сегмент – бл. 12; вграждане на контролно стегосъобщение – бл. 13; компресиране на получения стегосегмент – бл. 14; определяне на коефициент на компресия на стегосегмента – бл. 15; определяне на ε - бл. 16; проверка за наличие на неанализирани сегменти – бл. 17; изпращане на резултатите от анализа към управляващият възел на клъстерната система – бл. 18; обобщаване на резултатите от всички възли на системата – бл. 19; вземане на решение за наличие на скрита информация в анализирания файл, на базата на обобщените резултати – бл. 20; проверка за наличие на неанализирани файлове за съдържание на скрита информация – бл. 21.

Анализ на времевите характеристики на разгледания алгоритъм е даден в глава 4 на дисертацията.



Фиг. 3.7

3.7 Оценка на ефективността на процеса на стеганализ

Нека по k информационни канала постъпва съобщения, във вид на файлове, която трябва да бъде проверена за наличие на скрита стегоинформация. Количеството $n_i, i = \overline{1, k}$ на постъпилите по

$i - tu, i = \overline{1, k}$ канал файлове, за даден период от време е случайна величина с поасонов закон на разпределение с параметър $\lambda_i, i = \overline{1, k}$. При наличие на скрита стегоинформация в даден файл (такива файлове ще наричаме заразени файлове) той се привежда в състояние, изключващо възстановяването и използването на стегоинформацията. Времето за проверка наличието на стегоинформация в даден файл е случайна величина с експоненциален закон на разпределение с параметър $\mu_i, i = \overline{1, k}$.

Времето $t_i, i = \overline{1, k}$ за предаване на един файл, предаван по $i - tu, i = \overline{1, k}$, канал е случайна величина, с експоненциален закон на разпределение с параметър $\eta_i, i = \overline{1, k}$.

В указаните условия е необходимо да се определи ефективността на системата за защита от стегоинформация.

За решаване на така дефинираната задача ще определим средното време \bar{t} за предаване на един файл, при условие, че не се извършва проверка за наличие на скрита стегоинформация:

$$\bar{t} = \frac{n_1 t_1 + n_2 t_2 + n_3 t_3 + \dots + n_k t_k}{n} = \frac{1}{n} \sum_{i=1}^k n_i t_i, \quad (3.21)$$

където $n = \sum_{i=1}^k n_i$ е общото количество на постъпилите за зададен период $T_{\text{эф}}$ на функциониране файлове; $t_i = 1/\eta_i$ - време за предаване на $i - tu, i = \overline{1, k}$ файл.

Във формула (3.21) отношението

$$p_i = \frac{n_i}{n}, \quad (3.22)$$

представлява вероятността, че при обмен на файл, същият ще е осъществен по i -ти, $i = \overline{1, k}$, канал. Тогава (3.21) ще добие вида:

$$\bar{t} = \sum_{i=1}^k p_i t_i = \sum_{i=1}^k \frac{p_i}{\eta_i}. \quad (3.23)$$

Ще определим средното време за проверка на един файл за наличие на скрита стегоинформация:

$$\bar{\tau} = \frac{n_1 \tau_1 + n_2 \tau_2 + n_3 \tau_3 + \dots + n_k \tau_k}{n} = \frac{1}{n} \sum_{i=1}^k n_i \tau_i . \quad (3.24)$$

Предвид на (3.22) изразът (3.24) ще запишем като:

$$\bar{\tau} = \sum_{i=1}^k p_i \tau_i = \sum_{i=1}^k \frac{p_i}{\mu_i} . \quad (3.25)$$

За оценка на ефективността на алгоритмите за извършване на стеганализ ще въведем показателя коефициент на ефективност K_E на системата за защита на информацията:

$$K_E = \frac{\bar{\tau}}{t + \tau} . \quad (3.26)$$

Колкото коефициентът на ефективност K_E приема по-малки стойности, толкова системата за защита от скрита стегоинформация се характеризира с по-висока ефективност.

3.8. Изводи :

1. Извършен е подробен анализ на методите за стеганализ от достъпните литературни източници. Определени са основни им характеристики.

2. Дефинирани са основните български термини в стеганографията и стеганализа и е направена е класификация на методите за стеганализ на базата на подробен анализ на достъпните литературни източници.

3. С цел определяне и сравнение на ефективността на анализиранияте методи са разработени последователни алгоритми за реализация на методи за стеганализ „Хистограмна атака“ и „Компресия на данни“.

4. Направена е модификация на алгоритъм за последователен стеганализ на базата на подхода за компресия на подозрителни файлове.

5. Разработени са два паралелни алгоритъма, повишаващи ефективността на предложените последователни алгоритми за стеганализ за работа в реално време.

6. Разработен е математически модел и е изведен основен показател - коефициент на ефективност K_E , за оценка на ефективността на алгоритмите за стеганализ.

ГЛАВА ЧЕТВЪРТА. АНАЛИЗ И ОЦЕНКА НА ЕФЕКТИВНОСТТА НА ПРЕДЛОЖЕНИТЕ АЛГОРИТМИ ЗА ОТКРИВАНЕ НА СТЕГАНОГРАФСКА ИНФОРМАЦИЯ

В началото на глава 4 са формулирани са условията за провеждане на експериментите с цел изследване ефективността на предложените алгоритми за стеганализ. На базата на повече от 200 теста за експерименти е избрана стегопрограмата Invisible Secrets 4 за вграждане на скрити съобщения. Във всеки един файл от формираната база от bmp - контейнери са вградени скрити стеганографски съобщения - графични и текстови обекти.

4.2 Изследване на характеристиките на алгоритъма за стеганализ на базата на χ^2

С използване на програмата Camouflage за вграждане на скрита информация са създадени 20 файла за тестване. Наличието на скрита информация се проверява с използване на разработена програма за анализ на 24-битови битмап изображения (Приложение 1), реализираща предложения алгоритъм за стеганализ на базата на χ^2 (т. 3.5). В резултат на проверката във всичките 20 файла беше открита скрита информация.

За да се определи ефективността на предложения алгоритъм са извършени тестови проверки на 800 файла, подбрани и настроени по начин, посочен по-горе. В резултат на това беше установено (фиг. 4.1):



Фиг. 4.1

1. При файлове, с малък обем вградена информация (коэффициент на вграждане по-малък от 5%) предложения алгоритъм не винаги открива стего информация. Тази особеност е характерна за всички аналогични алгоритми, но предложения такъв позволява откриване на скрита информация при значително по-нисък коефициент

на вграждане (от около 5 % вместо достигнатата до сега долна граница от 10-12%).

2. За файлове с нисък коефициент на вграждане в т. 3.6 е предложен алгоритъм, базиран върху компресията на данни, който открива скрита информация при коефициент на вграждане по-малък от 5 %.

4.3 Изследване на характеристиките на алгоритъма за паралелен стеганализ на базата на χ^2

Характерна особеност на алгоритмите за последователен стеганализ е значителното време за обработване на изображенията, което в редица случаи ги прави неприложими в системи, работещи в реално време. В тази връзка е разработен и описан в т. 3.4 алгоритъм за паралелен стеганализ на базата на χ^2 . За реализацията му е разработена програма за анализ на скрита информация в битмап изображения , с която са извършени и съответните изпитвания, за определене на следните параметри:

- време за анализ на пълната база данни от изображения, при обработката от различен брой ядра на паралелната клъстерна система;
- коефициент на ускорение при паралелна обработка на изображенията;
- общо време за обработване на информацията, което включва: време за прочитане на изображенията, трансфера на информация между възлите на клъстера, времето за извеждане на екрана на получените резултати

Показани са резултатите от примерно изпълнение на програмата за паралелен стеганализ с използване на 32 ядра на системата за паралелна обработка.

В резултат на получените данни от проведените изследвания могат да се направят следните изводи:

1. Достоинство на предложени алгоритъм за паралелен стеганализ е, че осигурява еднаквото информационни натоварване на ядрата на клъстерната система, което е условия за ефективна работа, както по отношение на натоварването на процесорите ѝ, така и от гледна точка на осигуряване на минимално време за анализ.

2. Равномерното натоварване на ядрата на клъстерната система осигурява линейно нарастване на относителната ѝ производителност в отношение на нарастването на количеството ядра на клъстерната система.

3. Времето за изпълнение съществено зависи от броя на паралелно работещите ядра, като тази зависимост става силно изразена при брой на ядрата над 13.

4. В сравнение с алгоритъма за последователен стеганализ (т. 4.2.) алгоритъмът за паралелен стеганализ при реализация с 31 ядра дава възможност над 30 пъти да се съкрати времето за проверка на файловете за наличие на скрита информация, което го прави приложим в системи, работещи в реално време.

5. Алгоритъма за паралелен стеганализ има недостатък, по сравнение с алгоритмите за последователна работа, състоящ се в лъжливо „откриване” на файлове със скрита информация в контейнери, които се характеризират с голямо цветово насищане (фиг. 4.5).



Фиг. 4.3 Време за стеганализ на изображенията от базата данни



Фиг. 4.4 Ускорение при стеганализ с различен брой процесори

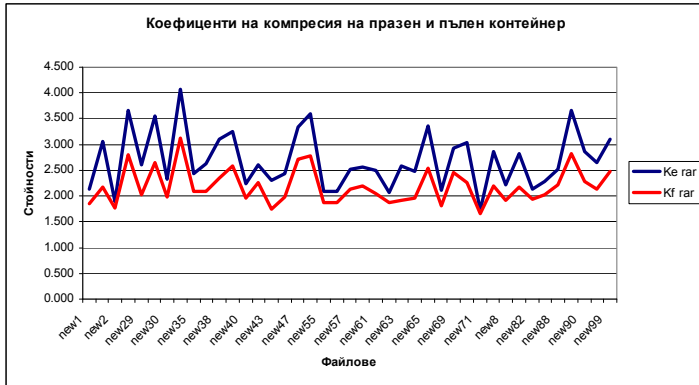
Резултатите от проверката за наличие на вградена информация са показани графично на фиг. 4.5.



Фиг. 4.5.

4.4 Изследване на характеристиките на алгоритъм за последователен стеганализ на базата на компресия на данни

Резултатите, получени от изследване на предложения в т. 3.5 алгоритъм за последователен стеганализ, базиран на компресия на данните са следните:



Фиг. 4.6.



Фиг. 4.7.



Фиг. 4.8.

4.5 Изследване на характеристиките на паралелния алгоритъм за стеганализ на базата на компресия на данни

Получени са следните резултати:

1. Предложения паралелен алгоритъм за стеганализ се характеризира с аналогични възможности за откриване на скрита информация като разработения и представен в т. 4.3 алгоритъм за последователен стеганализ.

2. Равномерното натоварване на ядрата на клъстерната система осигурява линейно нарастване на относителната ѝ производителност с увеличаване на броя на ядрата на клъстер системата.

3. Времето за изпълнение на програмата, реализираща разглеждания алгоритъм за стеганализ съществено зависи от броя на паралелно работещите ядра, като тази зависимост става силно изразена при брой на ядрата над 13.

4. По сравнение с алгоритъма за последователен стеганализ (т. 3.6) алгоритъма за паралелен стеганализ дава възможност над 30 пъти да се съкрати времето за проверка на файловете за наличие на скрита информация, което го прави приложим в системи, работещи в реално време.

4.6 Изводи:

1. Разработена е процедура за извършване на анализ и оценка на ефективността на разработените алгоритми чрез база от 800 контейнера и програма за вграждане на скрита информация.

2. Изследвана е ефективността на разработения алгоритъм за стеганализ на базата на χ^2 . Експериментално е доказано, че той

позволява откриване на скрита информация при нисък коефициент на вграждане (от около 5 %), вместо посочената в литературата долна граница от 10 - 12% за аналогични алгоритми.

3. Експериментално е изследвана ефективността на разработения алгоритъм базиран на компресия на данните. Резултатите показват стойности на коефициента K_{sa} по – големи от 0,9, надвишаващ ефективността на аналогични методи.

4. Изследвани са характеристиките на предложения алгоритъм за паралелен стеганализ на базата на χ^2 . Експериментално е доказано, че той осигурява равномерно информационно натоварване на ядрата на кълъстерната система и минимално време за стеганализ.

5. С паралелна кълъстерна компютърна система „Радан - М“ на ФМИ, ШУ и разработени програми за паралелна обработка са извършени тестове на разработените алгоритми. Изследвана е ефективността на програмите в зависимост от броя на процесорните ядра. Показано е, че при n на брой паралелно работещи ядра на кълъстерната система, програмите, реализиращи разработените алгоритми за паралелен стеганализ дават възможност над $(n - 1)$ пъти да се съкрати времето за стеганализ, което ги прави приложими в системи, работещи в реално време.

ЗАКЛЮЧЕНИЕ

В резултат на извършената научно - изследователска работа, в дисертационния труд са получени следните по-важни резултати:

1. Анализирани са актуалният проблем за заплахите и реалните щети от изтичане на чувствителна за организациите информация чрез злонамерени техни служители (инсайдери) и е разгледана ролята на системите за защита на информацията (СЗИ) в това направление.

2. Формулиран е терминът „стегаинцидент” и е разработен модел на стегаинцидент за реализиране на скрит стегоканал за кражба на секретни данни. Обоснован е изборът на подсистемата за стеганалитична защита от НСД и изтичане на информацията чрез скрити канали.

3. Анализирани са редица критерии за оценка на ефективността на ССЗИ и са предложени количествени показатели за нейната оценка. Формулиран е комплексен показател за оценка на ефективността на СЗИ.

4. Извършен е анализ на факторите, влияещи на разработването на адекватни математически модели за оценка и анализ на системите за защита на информацията и е избран подход за математическо описание на СЗИ в контекста на дефинираната тема на дисертационното изследване. Разработени са обобщени аналитични и статистически модели за оценка на въздействието на възможните заплахи за информацията и за оценка на загубите в компютърните системи (мрежи). Доказана е адекватността на разработените модели.

5. Извършен е подробен анализ на методите за стеганализ от достъпните литературни източници. Определени са основни им характеристики. Направена е класификация на методите за стеганализ и са дефинирани основните български термини в стеганографията и стеганализа.

6. На базата на направения анализ, с цел определяне и сравнение на ефективността на анализирани методи са разработени:

- алгоритъм за стеганализ на графични файлове с използване на метода χ^2 ;
- алгоритъм за паралелен стеганализ на графични файлове с използване на метода χ^2 ;
- алгоритъм за стеганализ на графични файлове с използване на компресия на данните;
- алгоритъм за паралелен стеганализ на графични файлове с използване на компресия на данните;
- метод за оценка на ефективността на процеса на стеганализ, основаващ се на предложен за целта математически модел.

За оценка на ефективността на алгоритмите за извършване на стеганализ е изведен показател – коефициент на ефективност.

7. Експериментално е доказана по – високата ефективност на разработените в дисертацията алгоритми за стеганализ от тази на аналогичните достъпни от литературата методи.

8. С паралелна клъстерна компютърна система „Радан - М“ във ФМИ на Шуменския университет „Епископ Константин Преславски“ и разработени програми за паралелна обработка са извършени тестове на разработените алгоритми. Изследвана е ефективността на програмите в зависимост от броя на процесорните ядра. Показано е, че при n на брой паралелно работещи ядра на клъстерната система, програмите, реализиращи разработените алгоритми за паралелен стеганализ дават възможност над $(n - 1)$ пъти да се съкрати времето за стеганализ, което ги прави приложими в системи, работещи в реално време.

III. НАУЧНО - ПРИЛОЖНИ ПРИНОСИ В ДИСЕРТАЦИЯТА:

1. Разработени са обобщени аналитични модели за оценка на въздействието и загубите в компютърните системи от възможните заплахи за информацията, обработвана, предавана и съхранявана в компютърните системи (мрежи).

2. Направена е модификация на алгоритъм за последователен стеганализ на базата на подхода за компресия на подозрителни файлове. Разработен е алгоритъм за паралелен стеганализ по този метод.

3. Разработени са последователен и паралелен алгоритъм за стеганализ тип „Хистограмна атака“.

4. Доразвито е решаването на проблема за защита на информацията в компютърните системи посредством разработване на методи за оценка на ефективността на системи за защита на информацията.

5. Формулирани са основни критерии за оценка на ефективността на стеганалитични алгоритми и програми.

IV. ПРИЛОЖНИ ПРИНОСИ В ДИСЕРТАЦИЯТА:

1. Дефинирани са основни показатели за извършване на оценка на загубите в компютърните системи от въздействието на възможни заплахи.

2. Разработени са програми за паралелна обработка чрез клъстерна система на предложените алгоритми за стеганализ в реално време.

3. Определен е състава на подсистема за стеганалитична защита на информацията (ССЗИ).

4. Дефинирани са основните български термини в стеганографията и стеганализа и на системите за стеганалитична защита на информацията.

5. Направена е класификация на методите за стеганализ на базата на подробен анализ на достъпните литературни източници.

V. СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ТЕМАТА НА ДИСЕРТАЦИЯТА:

1. Железов, С., С. Станев, Т. Великова, В. Неделчева и М. Иванова. К вопросу применения термина „Эффективность стегосистем” в учебном курсе „Компьютерная стеганография”, Трудове на международната научно - практическа конференция на НПУ „М. П. Драгоманов”, Киев, 2011, стр. 310 - 311.

2. Станев, С., С. Железов, Т. Великова и М. Иванова. За ефективността на стеганографските програми. Сборник научни трудове на конференция с международно участие „40 години Шуменски университет”, Том на ФМИ, Шумен, 2011, стр. 97 - 102.

3. Железов, С., С. Станев и И. Якимов, Подход за паралелен стеганализ чрез компресиране на данни. Сборник трудове на юбилеен международен конгрес "40 години България – космическа държава", Варна, 2012, стр. 360 - 367.

4. Железов, С. и В. Янакиева, Модифициран алгоритъм за стеганализ. Сборник научни трудове на Научна сесия на НВУ-факултет АПВО и КИС, Шумен, 2013.

5. Железов, С., А. Начев, Статистически модел за оценка на въздействието на заплахите за компютърните системи и мрежи. Сборник трудове на научна конференция „Защитата на личните данни в контекста на информационната сигурност”. Секция Информационна сигурност. ФАПВОКИС на НВУ, Шумен, 2013.

6. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Информационные технологии и безопасность, Журнал Акад. наук Украины., Спец. выпуск, Киев, 2013, стр. 79 - 86.