Нехай дано послідовну композицію двох алгоритмічних структур *COMP(TAS1(f1), TAS2(f2)).* Оскільки *dZ ◦cZ=id*, то з останньої діаграми випливає наступна діаграма оптимізованих перетворень *COMP(TAS1(f1), TAS2(f2)) = TAS2(f2) ◦ TAS1(f1) = cY ◦ f2 ◦ dZ ◦ cZ ◦ f1 ◦ dX*

Для даного випадку легко відшукати набір оптимізуючих правил перетворень, що виключають лишні функції розсилки та збору проміжних результатів.

Висновок

У роботі запропоновано повну систему правил оптимізації, що дозволяє уникнути зайвих операцій пересилки даних та виключити обчислення взаємообернених функцій розв'язання суперрідких матриць великої розмірності в задачах криптоаналізу системи RSA з використанням алгоритму загального решета числового поля.

Список використаних джерел

1. Романец Ю. В. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина.// Ю. В. Романец, П. А.Тимофеев, В. Ф. Шаньгин / – М.: Радио и связь, 1999 – 328 с.
2. Закон України «Про інформацію» //ВВР, 1992, № 48, ст. 650.
3. Закон України «Про державну таємницю» //ВВР, 1994, №16, ст. 94.
4. Закон України «Про Національну програму інформатизації» //ВВР, 1998, № 27-28, ст. 181.
5. Стэггерс Н. Історія і тенденції розвитку медичних інформаційних систем у США / (російський переклад).// Н. Стэггерс, Ч. Бэгли Томпсон, Р. Снайдер-Халперн/ – Journal of Nursing Scholarship. – 2001. – № 33. – С. 75–81.

УДК 004.492.2

МЕТОДИ ЗАХИСТУ РОБОЧИХ СТАНЦІЙ ВІД DDOS-АТАК

Шпінталь М.Я.[1)], Орловський Н.М.[2)]

Тернопільський національний економічний університет

[1)] к.т.н., доцент; [2)] магістрант

I. Постановка проблеми

Однією з найбільш актуальних задач у сфері послуг надання інформації є забезпечення стабільної роботи і можливості доступу до баз даних у будь-який час. При роботі в такому режимі так само необхідно забезпечення певної міри надійності і стресостійкості системи. Одним з найбільш серйозних і поширених способів атак є DDoS-атака (від англ. Distributed Denial of Service, розподілена атака типу "відмова в обслуговуванні").

Робота присвячена вивченню джерел шкідливого трафіку і їх параметрів, створення моделі мережі підприємства у якій є мережевий фільтр (обробляє запити ззовні), створення алгоритму для відмінності шкідливого трафіку генерованого атакуючими.

II. Мета роботи

Мета дослідження є підвищення якості фільтрації трафіку від шкідливих навантажень шляхом розробки моделі обробки зовнішніх запитів, що поступають в мережу підприємства, та вдосконалення алгоритмів їх фільтрації.

Завдання:

- аналіз структури і параметрів моделі мережі підприємства;
- дослідження даних отриманих в процесі моделювання для створення алгоритму;
- створення алгоритму фільтрації шкідливого трафіку;
- оцінка ефективності роботи отриманого алгоритму.

III. Методи захисту від DDoS-атак

Існують при основні рішення захисту від атак: програмні, апаратні, хмарні.

Програмні рішення - найпопулярніші на ринку, вони представляє собою набір засобів фільтрації трафіку, які складені розробником з використання особистого досвіду. Дане рішення досить простим у використанні, але допоможе тільки від малопомітних атак виду вандалізм.

Апаратні рішення - представляють собою створення розподіленої мережевної структури з великим запасом пропускного трафіку. Використовуються в масштабних мережевих структурах, таких як: точки обміну трафіком, дата-центри, великі регіональні провайдери.

Хмарні рішення представлені у вигляді мережевних структур з великою пропускною здатністю, до складу якої вводяться сервери для фільтрації шкідливого трафіку. Таким чином, така мережа поступово буде фільтрувати шкідливий трафік і знижувати кількість шкідливих пакетів.

Висновок

DDOS-атаку дуже складно виявити й запобігти, оскільки "шкідливі" пакети не відрізняються від "легітимних". Мережеві пристрої й традиційні технічні рішення для забезпечення безпеки мережевого периметру, такі як міжмережеві екрани й системи виявлення вторгнень (IDS), є важливими компонентами загальної стратегії мережевої безпеки.

Список використаних джерел

1. Цирульник С.М., Кисюк Д.В., Говорущенко Т.О. DDoS-атаки й методи боротьби з ними [Електронний ресурс]. – Режим доступу: http://www.chnu.edu.ua/res/csn/druk/visnyk/2009_446/446_23_Cirulnik.pdf

УДК 004.056

ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ФАЛЬСИФІКАЦІЇ АУДІО У ФОРМАТІ MPEG

Якименко І.З.[1)], Паздрій І.Р.[2)], Кузьмич А.В.[3)]
Тернопільський національний економічний університет
[1)] к.т.н., доцент; [2)] к.т.н., доцент; [3)] магістрант

І. Постановка задачі

З відкритих джерел відомі деякі методи виявлення фальсифікації цифрового аудіо (ЦА). Більшість з них заснована на аналізі особливостей технічного пристрою, на якому сигнал було створено, та відносяться до програмно-технічних методів пасивного захисту інформації. Проте відомо, що переважними для використання є програмні методи пасивного захисту, які не потребують додаткової інформації для проведення перевірки цілісності сигналу. Відомі також методи виявлення фальсифікації ЦА, що базуються на аналізі матриці нульових сингулярних чисел блоків (МНСЧБ), двовимірного горизонтального представлення цифрового аудіо сигналу. До області застосування цих методів відносяться аудіо сигнали, що збережені у форматі без втрат інформації.

У зв'язку з цим задача виявлення фальсифікації цифрового аудіо, збереженого у форматі MPEG, є актуальною, але невирішеною в повному обсязі, проблемою.

ІІ. Мета роботи

Метою дослідження є процес виявлення та локалізації фальсифікації цифрового аудіо, збереженого у форматі MPEG.

ІІІ. Алгоритм виявлення та локалізації фальсифікації цифрового аудіо

Алгоритм MPEG орієнтований на кодування високоякісного стерео звуку, та забезпечує велику кількість допоміжних властивостей для частот дискретизації.

В основі стиснення звуку в MPEG лежить принцип квантування. Однак, квантовані величини беруться не з звукових симплів, а з чисел (званих сигналами), які виділяються з частотної області звуку. Той факт, що коефіцієнт стиснення (або бітова швидкість) відомий кодеру, означає, що кодер в кожен момент часу знає, скільки біт можна призначити квантованому сигналу. Отже важливою частиною кодера є адаптивний алгоритм призначення бітів.

Цей алгоритм використовує відому бітову швидкість і частотний спектр самих останніх аудіосимплів для визначення розміру квантування сигналу так, щоб шум квантування (різниця між вихідним сигналом і його квантованим варіантом) був нечутний (тобто, він має знаходитися нижче порога маскування).

Стандарт MPEG включає квантування відповідних коефіцієнтів дискретного косинусного перетворення [31]. У зв'язку з цим розглянутий вище метод виявлення та локалізації фальсифікації цифрового зображення (ЦЗ) може бути адаптований для аналізу ЦА, що зберігаються у форматі з втратою інформації.

Алгоритм виявлення та локалізації фальсифікації цифрового аудіо:

а) розбити вектор ЦА на m підблоків сигналу;

б) для і–го ПБС, $i = \overline{1,m}$: