$$T_n^t = \left\{ \left\{ M_k^t \right\}_{k=1}^{k=K} \right\}_{0+t*\Delta t_a} \quad (1)$$

де M_k^t – амплітуда k-ої частотної складової діапазону n в момент часу t; K - кількість частотних складових; Δt_a – дискретний зсув вікна аналізу аудіосигналу в часі.

В ході експериментів було встановлено, що цей алгоритм є досить чутливим до масштабування сигналу, викликаного змінами швидкості відтворення. Для збільшення стійкості до масштабування запропоновано модифікований алгоритм, в якому обчислення амплітуди спектра модуляції засноване на швидкому перетворення Мелліна:

$$T_\omega = |D_\omega(t,c)| \quad (2)$$

Використання швидкого перетворення Мелліна для генерації вектора ознак дозволило збільшити стійкість алгоритму до масштабування сигналу в часі в 2.5 рази в порівнянні з вихідним методом.

VI. Висновки

Експериментально встановлено, що існуючі методи не забезпечують надійну ідентифікацію акустичних сигналів, стислих у часі і, таким чином непридатні для моніторингу радіо- і телевізійних передач. Представлений новий метод ідентифікації акустичних сигналів, заснований на аналізі спектру модуляції в частотних діапазонах. З метою підвищення стійкості алгоритму до масштабування сигналу в часі для обчислення параметрів спектра модуляції запропоновано використовувати перетворення Мелліна і його модифікований варіант, заснований на дискретному косинусному перетворенні. Запропонований алгоритм має високу стійкість до зміни масштабу аудіосигналів і дозволяє здійснювати надійну ідентифікацію аудіовізуальних матеріалів, що мають аудіоканал.

Список використаних джерел

1. Wold E., Blum T., Keislar D., Wheaton J. Content-Based Classification, Search, and Retrieval of Audio // IEEE Multimedia. – 1996.- Vol. 3, No.3.- P. 27-36.
2. Cano P., Batlle E., Mayer H., Neuschmied H. obust sound modeling for song detection in broadcast audio // Proc. AES 112th Int. Conv. – 2002. - Munich (Germany).
3. Neuschmied H., Mayer H., Batlle E. Content-based identification of audio titles on the internet //Proc. International Conference on Web Delivering of Music.- 2001.
4. Rabiner L. R. A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition // Proc. of the IEEE. – 1989.- Vol.77, No.2.- P. 257-286 .
5. Haitsma J., Kalker T. A Highly Robust Audio Fingerprinting System// Proc. of the 3rd Int. Symposium on Music Information Retrieval. – 2002. - P. 144-148.
6. Sd Jin Soo Seo, Haitsma J., Kalker T. Linear speed-change resilient audio fingerprinting // Proc. IEEE Benelux Workshop on Model based Processing and Coding of Audio. – 2002. – Leuven (Belgium).
7. С.В.Билобров. Метод идентификации аудиоматериалов на основании анализа спектра модуляции сигнала // Вісник Донецького університету, Сер.А: Природничі науки.-2005.-Вип.2.- С.387-391.
8. Picone J. Signal modeling techniques in speech recognition // Proc. of the ICASSP. – 1993. - Vol. 81. No. 9. - P. 1215–1247.
Greenberg S., Kingsbury B. The Modulation Spectrogram: in Pursuit of an Invariant Representation of Speech // ICASSP.- 1997.- P. 1647-1650.
9. Пат. US2007055500 США, МКИ G10L 21. Extraction and matching of characteristic fingerprints from audio signals: Пат. US2007055500 США, МКИ G10L 21 / S.Bilobrov; SIVI. - № 219385; Заявл. 01.11.05; Опубл. 08.03.07, НКИ 704/217. - 13с.

УДК 683.1

ЗАХИСТ ДОКУМЕНТІВ НА ОСНОВІ СЕМАНТИЧНОГО АНАЛІЗУ

Якименко І.З.[1)], Ящук В.Ф.[2)]

Тернопільський національний економічний університет

[1)] к.т.н; [2)] магістрант

I. Постановка проблеми

При проектуванні та використанні документів на основі автоматизованої системи управління визначальну роль в наш час відіграє захист даних від несанкціонованого доступу [1], особливо в епоху широкого запровадженням електронного документообігу та визнанням цифрових підписів, які

мають юридичну силу. Тим більше , на відміну від паперових, електронні документи є більш вразливими на різноманітні спотворення тому, що вони передаються по незахищеним каналам зв'язку, таких як мережа Інтернет, що не дає гарантії щодо забезпечення необхідного рівня захисту від атак [2].

Перед існуючими системами документообігу, які впроваджені на підприємствах, ставляться актуальні задачі семантичного аналізу, оскільки суть інформації, яка відображється в цих документах, визначається їх семантикою. Впровадження електронного документообігу, як всередині підприємства, так і між окремими підприємствами визначили особливу актуальність задач семантичного контролю документів [3].

II. Мета роботи

У зв'язку з цим, метою роботи є проведення аналізу та досліджень сучасних систем захисту документообігу, етапів проектування, на основі чого привести пропозиції щодо покращення безпеки з використанням семантичного аналізу.

III. Етапи проектування систем захисту документів на основі семантичного контролю документів

Інформаційна безпека в автоматизованих системах документообігу (АСДО) є визначальною функцією, яка повинна реалізуватися в системі. Тому, для забезпечення захисту документів необхідно розрізняти наступні функціональні підсистеми, а саме – контролю документів та захисту документів, які забезпечать виконання цих функцій.

При аналізі контролю документів необхідним є те щоб виконуватися наступні важливі контролюючі функції - засобів проектування, коректності документа, загальний контроль документа, типу документа, що проектується та термінів проектування документа.

Іншою важливою підсистемою системи документообігу є підсистема захисту документів. До найбільш поширених типів засобів захисту АСДО можна віднести: захист документів у процесі їх проектування, функціонування та зберігання. На етапі проектування чи виготовлення підсистем даного типу необхідним є також врахування даних про загрози, які можуть виникати. До найбільш поширених загроз, які можуть бути по відношенню до документу, слід віднести: заміна суті опису управляючої дії, значень параметрів документів, несанкціоноване створення документу, впровадження в документ компонент чи фрагментів, які повністю або частково суперечать початковій меті проектування документів, використання несертифікованих засобів для проектування документів та зміна технологічних етапів проектування документу.

При реалізації засобів захисту необхідним є те, що кожний окремий елемент засобів захисту функціонує за певною стратегією, тобто – розпізнає дію атаки на документ, чи на АСДО в цілому, здійснює протидію атаці, або нейтралізує дію атаки на об'єкт атаки, яким є документ, формує елементи, які постійно знаходяться в технологічному циклі і завдяки яким успішне втручання в документ відповідною атакою стає неможливим, або модифікує компоненти технологічного процесу таким чином, щоб реалізація уже розпізнаної атаки була неможливою при її повторенні [2, 4].

Такий підхід орієнтований на протидію атаці зі сторони зловмисника, дозволяє уникнути загроз щодо несанкціонованого спотворення документу.

Найбільш перспективними з огляду на забезпечення необхідного рівня безпеки інформації документів є методи на основі семантичного аналізу, які включають наступні фактори: наявність системи інтерпретації та правил використання цієї системи, гомоморфізм між правилами використання системи інтерпретації та правилами побудови документів, які передбачається інтерпретувати, семантична несуперечність системи документів і системи інтерпретації [3].

Крім того, семантичний захист документів ґрунтється на підходах, які коротко можна охарактеризувати таким чином – семантичне завантаження самих носіїв семантики додатковими умовами, носіїв історії функціонування документообігу, зовнішнього середовища, для якого призначені документи, семантична генерація загроз, проектування документів, які вміщають засоби протидії можливим атакам, що формуються на основі загроз.

IV. Висновки

Проведені дослідження та аналіз сучасних систем захисту документообігу, етапів проектування, на основі чого було встановлено, що найбільш перспективними з огляду на забезпечення необхідного рівня безпеки є методи на основі семантичного аналізу

Список використаних джерел

1. Якименко І.З. Теоретичні основи зменшення часової та апаратної складності систем захисту інформаційних потоків на основі еліптичних кривих з використанням теоретико-числового базису Радемахера-Крестенсона. //І.З. Якименко, М.М. Касянчук/Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі». – №694.– 2012. – с. 118–125.
2. Andrew P. Moore Attack Modeling for Information Security and Survivability. //Andrew P. Moore, Robert J. Ellison, Richard C. Linger. / Technical Note CMU/SEI-2001-TN-001, 2001.
3. Сакович В. Высшая математика. Математическое программирование./В. Сакович , Н. Холод , А. Кузнецов — М., 2001. — 352 с.
4. Соколов В. Защита от компьютерного терроризма. — СПб, 2002. — 496 с.
5. Corbin J. The art of distributed applications. Programming Tech. for Remote Procedure Calls. Berlin. Springer Verlag, 1992. — 305 p.
6. Гуйванюк Н. В. та ін. Семантична структура тексту: Навч.-метод. посіб./ Гуйванюк Н. В., Гнатчук О. С., Нечипорук М. В.; Чернів. нац. ун-т ім. Ю. Федьковича. — Чернівці: Рута, 2000. — 131 с