References

1. Why Keccak is so cool and why it was chosen as the new SHA-3. [Electronic resource] - Access mode: https://habrahabr.ru/ post / 168707
2. Keccak hash function and Sponge design as a universal crypto-primitive. [Electronic resource] - Access mode: https://www.pgpru.com/biblioteka/statji/keccaksponge.
3. Schneier B. Applied cryptography. Protocols, algorithms, source texts in C language. / B. Schneier. - Moscow: Triumph, 2009. - 806 p.

УДК 004.056

ПРОЕКТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ПРОСОЧУВАННЯ ІНФОРМАЦІЇ В ПЕРЕДАНОМУ ПОТОЦІ ДАНИХ

Божко Н.В. [1], Моргун Ю.А.[2]

Коледж Миколаївського національного університету імені В.О.Сухомлинського

[1] викладач; [2] студент

I. Постановка проблеми

Комерційний інтерес на сьогодні є метою несанкціонованого збору інформації. На жаль в нашій країні на теперішній момент не досить належний рівень інформаційної безпеки корпоративних мереж. Фактичний та потенційно можливий матеріальний збиток компаній досить високий від прихованого просочування інформації.

Системи безпеки в основному повинні обмежувати допуск користувачів до інформаційних ресурсів, визначати їх повноваження, вміти розпізнавати несанкціоновані вторгнення в мережеву інфраструктуру, прогнозувати аварійні ситуації та усувати їх наслідки часткової втрати або тривалого блокування ресурсів.

Для того щоб важлива інформація надійно була захищена, вкрай необхідно забезпечити її цілісність даних та конфіденційність.

II. Мета роботи

Метою дослідження є проектування системи виявлення просочування інформації в переданому потоці даних у вигляді програмного модуля виявлення текстових областей в графічних файлах для вирішення завдань запобігання просочування конфіденційної інформації.

III. Розробка та використання системи

На підставі вищесказаного, було прийняте рішення створити програмний модуль, який мав би можливість виявлення в графічних файлах передачу текстових областей. За допомогою даного модуля стане можливим поліпшення комплексного захисту автоматизованої корпоративної системи, її інформаційної безпеки та запобігання несанкціонованого поширення конфіденційної інформації в графічних файлах.

Функції розробленого модуля: аналіз графічних файлів, виявлення текстових областей, які відповідають заданим критеріям; вивід звіту про досліджені графічні файли; виділення потенційно «небезпечних» зображень.

Підсистема виводить звіт про дослідження графічних файлів, результати дослідження залежать від заданих критеріїв.

Програмний модуль знаходить текстові області в графічних файлах, які можуть містити в собі конфіденційну інформацію та повідомляє про них для подальшого їх дослідження іншими модулями системи захисту.

Перевагою даного модуля є швидке знаходження необхідних текстових областей. Це дозволяє передавати на подальше дослідження системи захисту для розпізнавання образів на предмет наявності конфіденційної інформації тільки ті файли, в яких містяться дозволені текстові області. Це допомагає пришвидшити оброблення графічної інформації, додає властивість комплексності в цілому всієї системи.

В основу розробки блок-схеми алгоритму роботи системи взяті існуючі алгоритми виявлення текстових областей, а саме алгоритм «Швидке і ефективне текстове виявлення» (рис.1).

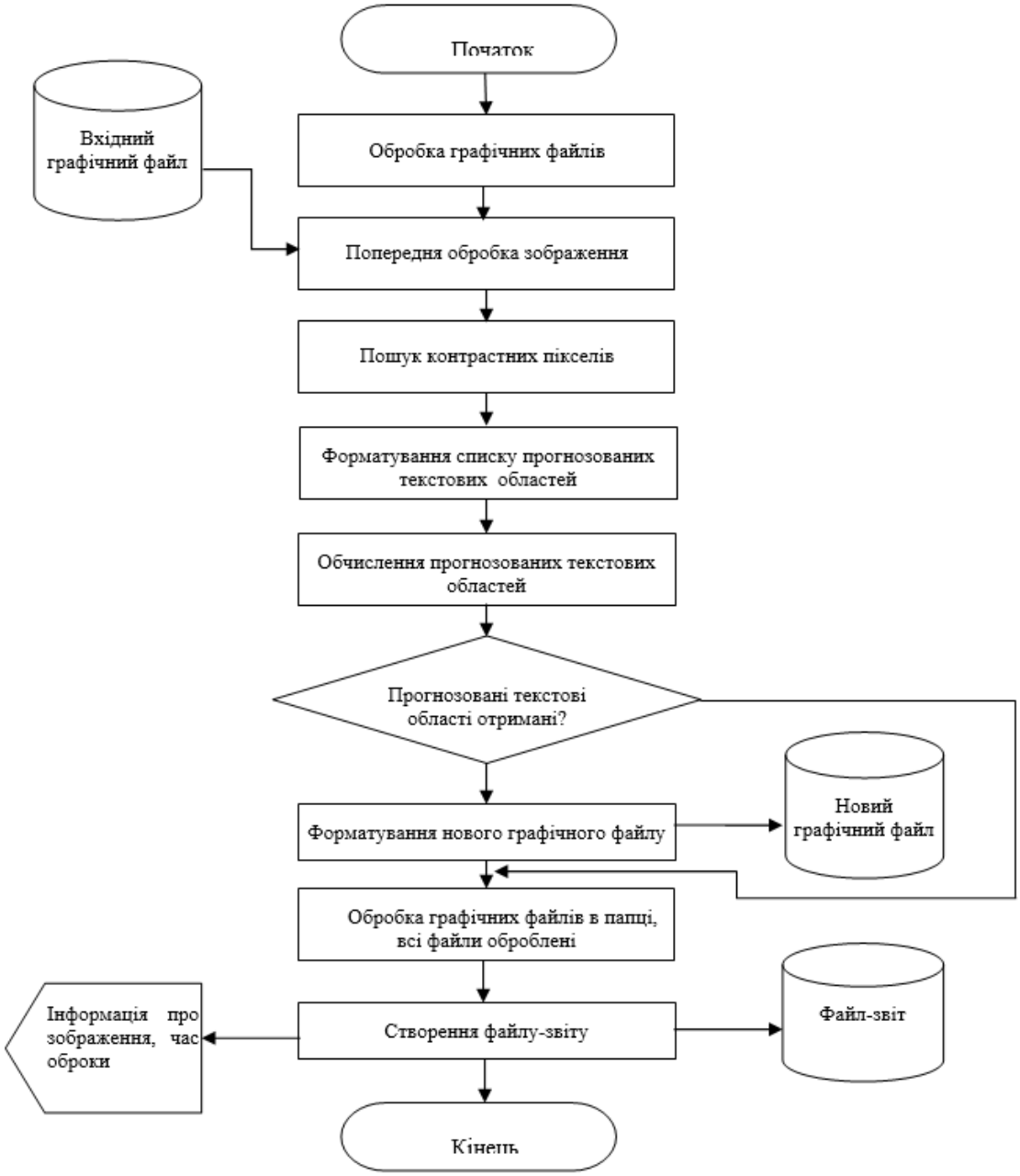

Рисунок 1 - Блок-схема розробленого алгоритму

Висновок

У роботі було спроектовано програмний модуль виявлення текстових областей в графічних файлах. На основі проведених досліджень були отримані ефективні результати роботи алгоритму і програмного модуля.

У зв'язку з цим його можна використовувати в системах захисту для виявлення і запобігання просочування конфіденційної інформації в графічних файлах.

Список використаних джерел

1. Буточнов О.М., Гончар Г.В., Дерев'янко С.М., Короленко М.П. Захист інформації в комунікаційній мережі зв'язку ЄДАПС. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 37 – 58.
2. Рустэм Хайретдинов. Практика внедрения систем защиты от утечек конфиденциальной информации – М.: СЛОВО - СІМС, 2012. - 284с.