Використання імунних мереж для виявлення атак на ресурси розподілених інформаційних систем

Дипломна робота на здобуття кваліфікації бакалавра системного аналізу

Король Олександр Олександрович,КА-34

Керівник д.т.н., професор кафедри ММСА

Данилов Валерій Якович

Вступ

З кожним роком зростає кількість програм, разом з нею зростає і кількість вірусів.

Розробники антивірусів фізично не можуть встигнути за темпами появи нових вірусів.

У зв’язку з цим постає задача розробки алгоритму, який дасть змогу виявляти нові віруси.

Структура дослідження

Об’єкт дослідження – задача виявлення шкідливих програм.

Предмет дослідження – штучні імунні системи, зокрема штучні імунні мережі.

Мета дослідження – дослідження штучних імунних систем як одних з провідних методів виявлення шкідливих програм.

Завдання

Для досягнення мети поставлено наступні завдання:

1. Провести аналіз існуючих методів, що використовуються для вирішення задач виявлення шкідливих програм.
2. Розробити програмний додаток, який реалізує роботу імунної мережі.
3. Провести дослідження.

Негативний відбір

- В імунній системі таке розпізнавання забезпечується Т-лімфоцитами і іншими клітинами, що мають на своїй поверхні рецептори, здатні виявляти чужорідні білки (антигени). Рецептори створюються на основі псевдовипадкогвого генетично зумовленого процесу перегрупування в ході освіти Т-клітин. Потрапляючи в тимус, Т-клітини піддаються цензуруваню, званому негативним відбором, при цьому клітини, які вступили в реакцію з власними білками, знищуються, а решта (що не утворюють з ними зв'язків) отримують можливість покинути тимус. Потім ці Т-клітини циркулюють по всьому організму і виконують функцію захисту від чужорідних антигенів.

- Аналогічно діє алгоритм негативного відбору, випадковим чином створюючи детектори і видаляючи ті з них, які розпізнають своє, так що залишаються детектори, які можуть виявляти будь-яке не своє.

Імунна мережа

- Імунна система являє собою комплекс клітин, молекули і органів, яка довела свою здатність виконувати деяку кількість завдань, таких як розпізнавання шаблонів, навчання, придбання пам'яті, генерація різноманітності, терпимості шуму, узагальнення, розподілене виявлення і оптимізація.

Алгоритм виявлення вірусу

Спочатку задаються два типи файлів(віруси і чисті файли). Ми обираємо файл який буде перевірятись і порівнюємо його з чистими файлами та з вірусами виявляючи відсоток співпадання.

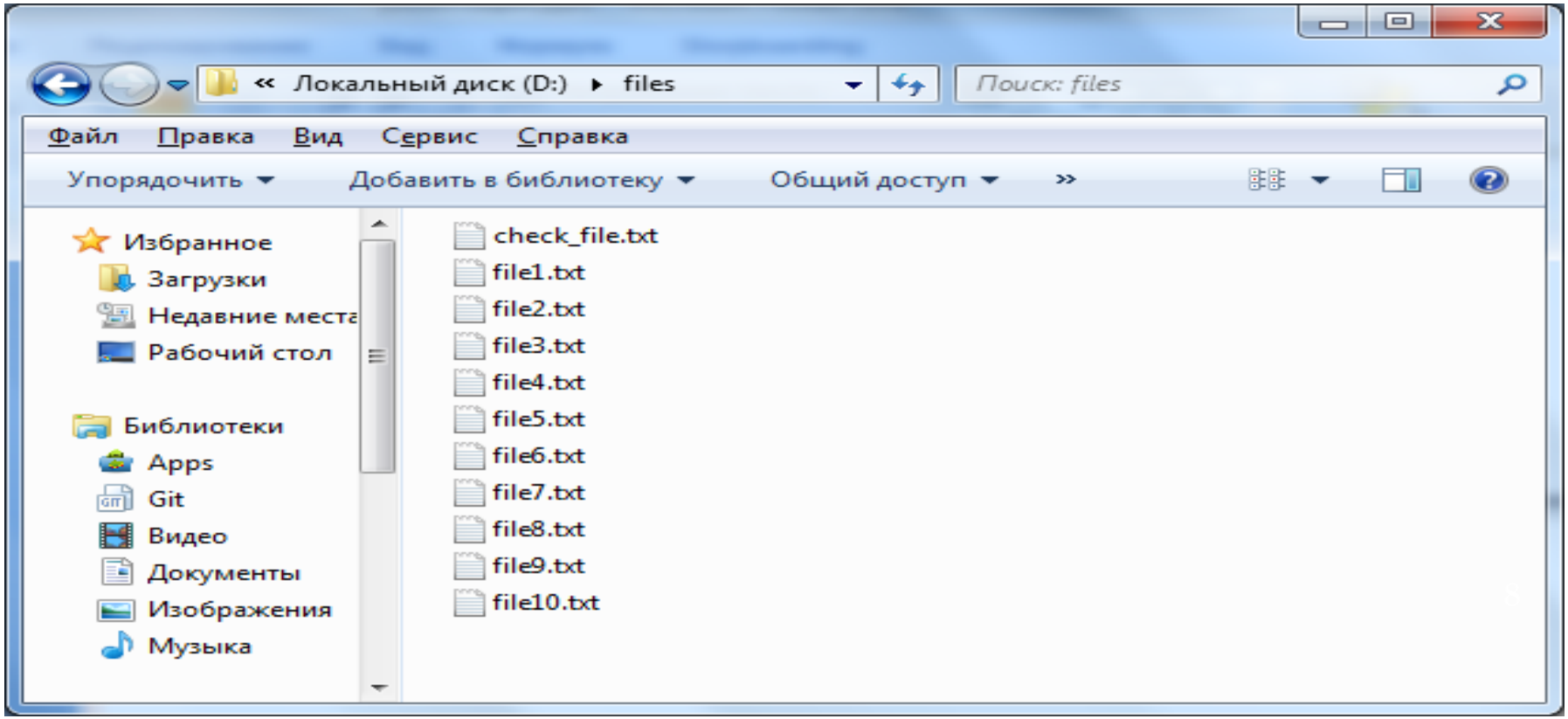
В залежності від того на скільки відсотків файл співпадає з вірусами/чистими файлами він відправляється в одну або іншу папку.

Якщо відсоток відповідності з чистими файлами > 80%, а відповідність вірусам <20%,то файл вважається чистим, якщо ж відсоток відповідності вірусам >20%, файл відноситься до вірусів.

Приклад роботи програми при виявленні чистого файлу

Problems | Javadoc | Declaration | Console

```
<terminated> program [Java Application] C:\Program Files\Java\jdk1.8.0_101\bin\javaw.exe
File not infected, match with file = 90%
File added to files folder with name check_file.txt
```

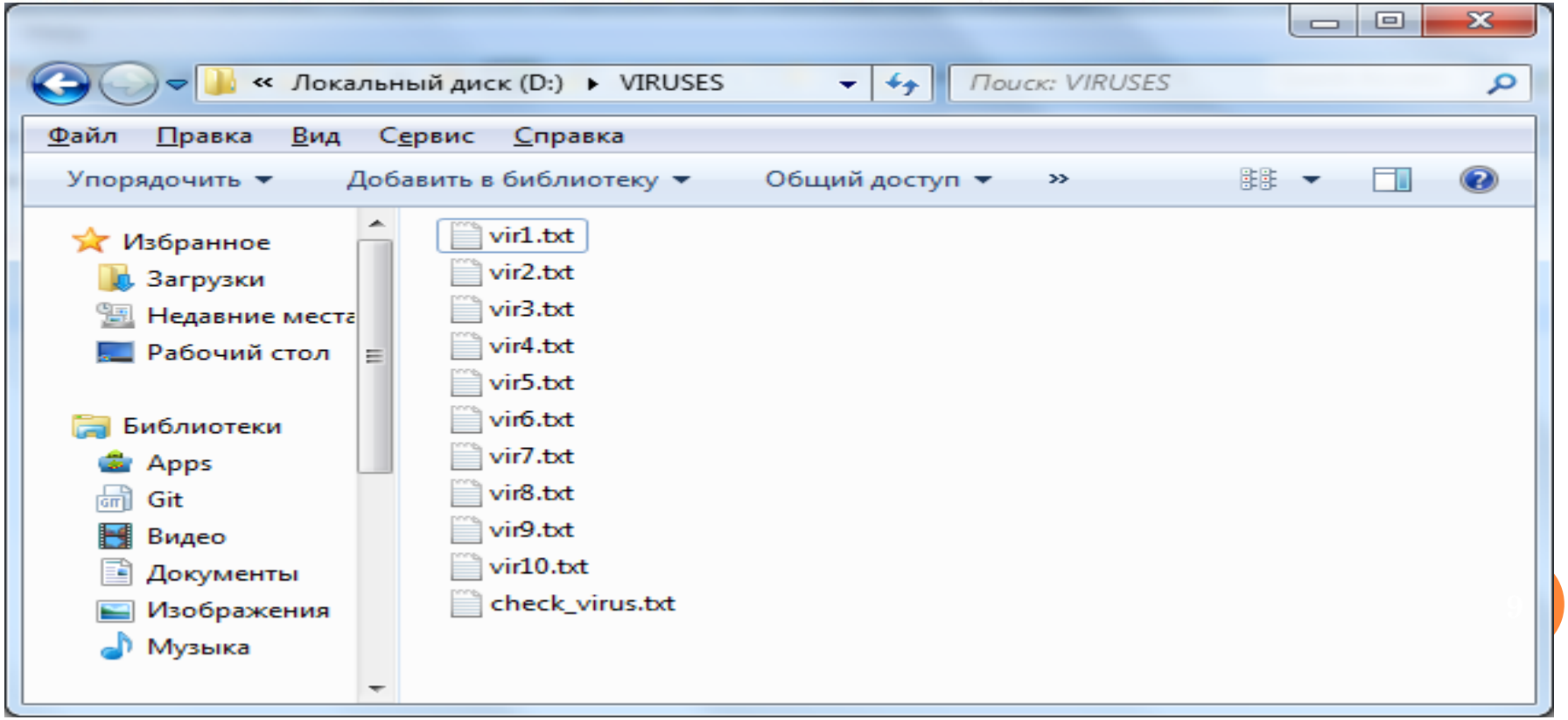


Приклад роботи програми при виявленні вірусу

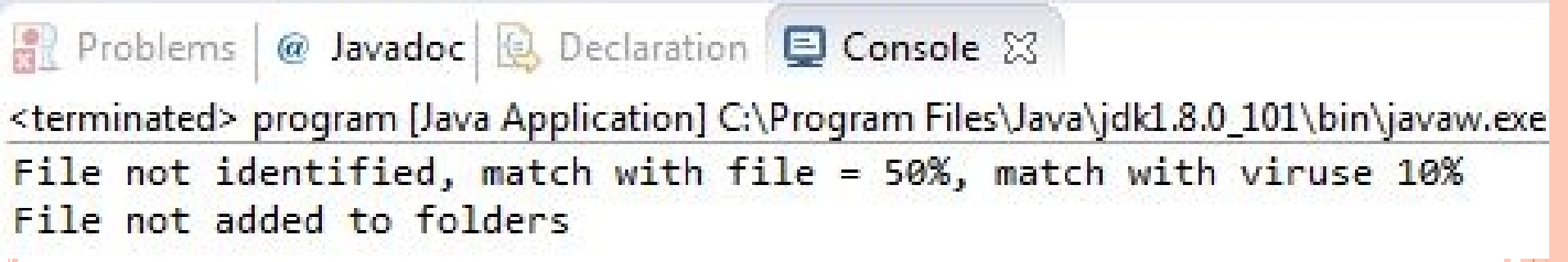
Problems @ Javadoc Declaration Console

<terminated> program [Java Application] C:\Program Files\Java\jdk1.8.0_101\bin\javaw.exe

```
File infected, match with viruses = 30%
File added to viruses folder with name check_virus.txt
```



Приклад роботи програми при недостатній кількості збігів



- Оскільки файл не співпадає достатньо для прийняття рішення ні з чистими фалами, ні з вірусами, ми не можемо віднести його до файлів або вірусів. Дана ситуація виникла у зв'язку з недостатньою кількістю програм та вірусів для перевірки.

Висновки

- Представлений розв’язок є легким для розуміння, простим у реалізіції та досить точним, також точність підвищується з часом і залежить від кількості контрольних файлів.
- Основним недоліком програми є швидкодія, оскільки для порівняння з багатьма фалами витрачається багато часу.

Дякую за увагу