Магістерська кваліфікаційна робота на тему:

«*Інформаційна технологія виявлення шкідливого програмного забезпечення*»

Виконав:

ст. групи КН-17м

Паламарчук В.Л.

Науковий керівник:

PhD, професор Савчук Т.О.

Інформаційна технологія виявлення шкідливого програмного забезпечення

- **Мета дослідження** – підвищення ефективності виявлення шкідливого програмного забезпечення за допомогою машинного навчання на основі статичного та динамічного аналізу.

- **Об’єкт дослідження** – процес виявлення шкідливого програмного забезпечення.
- **Предмет дослідження –** інформаційні технології виявлення шкідливого програмного.

Інформаційна технологія виявлення шкідливого програмного забезпечення

- Широке розповсюдження шкідливого програмного забезпечення на мобільних платформах заважає користувачам та ставить під загрозу їх безпеку. Нове шкідливе ПЗ створюється дуже швидкими темпами: по суті, щоб уникнути механізму виявлення шкідливого ПЗ на основі підпису достатньо застосувати звичайну обфускацію програмного коду.

Інформаційна технологія виявлення шкідливого програмного забезпечення

- У даному досліджені представлені підходи до виявлення шкідливого ПЗ на основі машинного навчання до виявлення шкідливих програм, що базуються на статичному й динамічному аналізі. Швидкий розвиток технік обфускації програмного коду суттєво ускладнює своєчасне виявлення шкідливого програмного забезпечення та ставить під загрозу безпеку користувача.

Інформаційна технологія виявлення шкідливого програмного забезпечення

Порівняльна таблиця сучасних антивірусних засобів для Android OS

Характеристика / Аналоги	ESET Mobile Security & Antivirus	Avast Antivirus	AVG AntiVirus
Обов'язкова прив'язка до Інтернету	присутня	присутня	присутня
Зрозумілий інтерфейс	відсутній	присутній	відсутній
Наявність серверної взаємодії	відсутня	відсутня	Частково присутня
Навантаження на систему	Високе	Високе	Середнє
Машинне навчання	відсутнє	відсутнє	відсутнє

Постановка задачі

Нехай є набір відомого програмного забезпечення:

$$\mathbf{S} = < \boldsymbol{M}, \boldsymbol{T} >,$$

де M – множина шкідливого програмного забезпечення, а T – множина довіреного програмного забезпечення.

Кожен об'єкт $o_i \in M$ або $o_i \in T$ має набір атрибутів:

$$\mathbf{O} = \{\boldsymbol{o_j} =< \boldsymbol{a_{j1}}, \dots, \boldsymbol{a_{jk}}, \boldsymbol{k} = \boldsymbol{k(j)} >\}.$$

Для кожного об'єкту набір атрибутів може відрізнятись.

Користувач формулює своє початкове представлення про інформаційну потребу у вигляді вхідного програмного забезпечення:

$$\boldsymbol{b_0} = \{\boldsymbol{b_{01}}, \dots, \boldsymbol{b_{0m}}\},$$

яке задає множину необхідних атрибутів об'єктів для пошуку.

Функція пошуку A здійснює інформаційний пошук у наборі S по запиту b_0:

$$\mathrm{A}(\boldsymbol{b_0}, \boldsymbol{S}) = \boldsymbol{\delta} \subset \boldsymbol{O}.$$

Результатом пошуку є множина δ об'єктів пошуку з набору O.

Користувач оцінює результати роботи пошуку на відповідність інформаційної потреби:

$$\boldsymbol{E}(\boldsymbol{b_o}, \boldsymbol{\delta}) = \boldsymbol{\delta'} \subseteq \boldsymbol{\delta}.$$

Після оцінки результату атрибути b_0 та сам об'єкт додаються до відповідних наборів M або T.

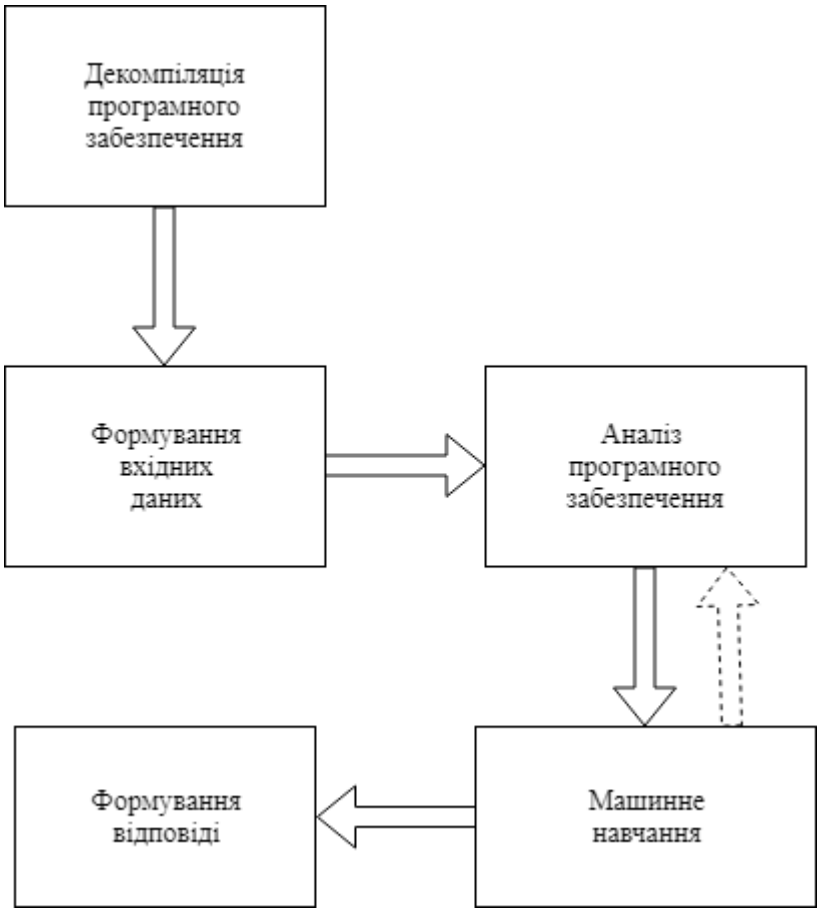
Таким чином, для розв'язку задачі виявлення шкідливого програмного забезпечення необхідно побудувати функцію $\mathrm{A}(b_0, S)$;

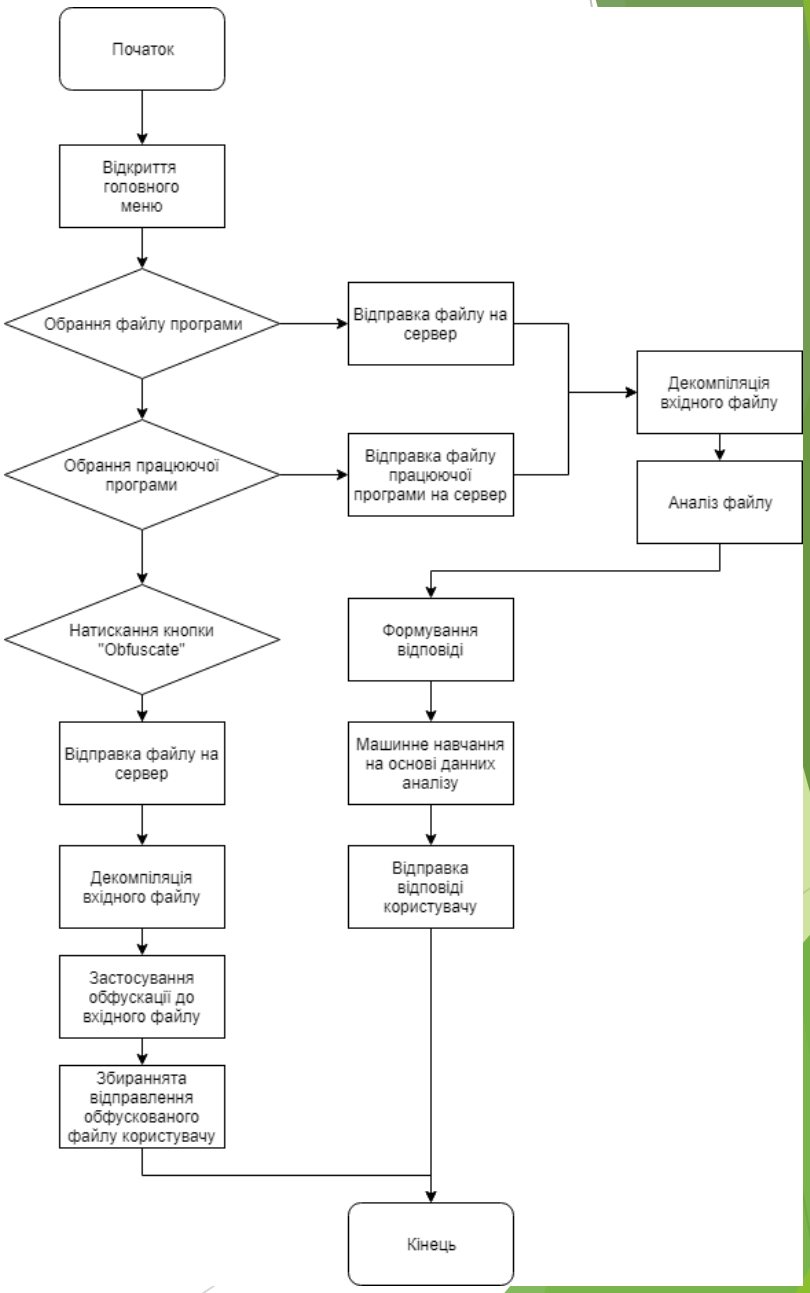
Аналіз програмного забезпечення припиняється коли множини δ' та δ, будуть збігатись.

Точність виявлення визначається відповідно до традиційного визначення точності:

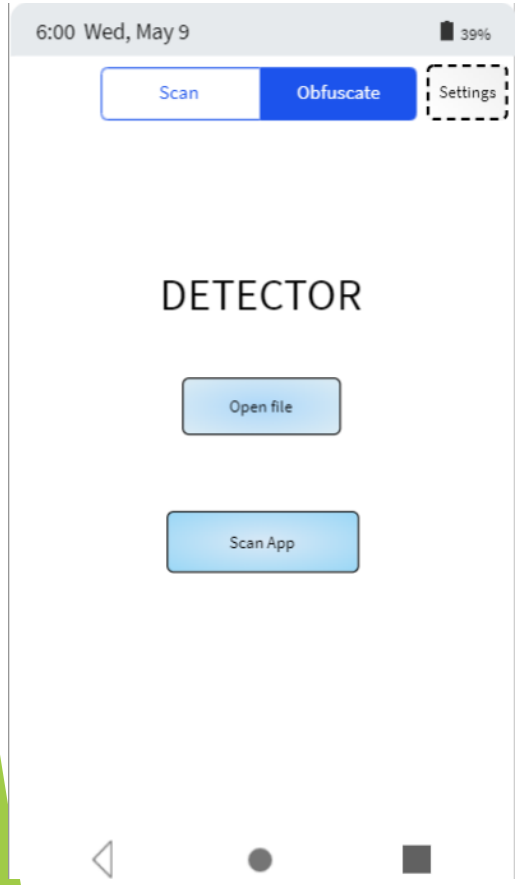
$$\frac{|\boldsymbol{\delta'}|}{|\boldsymbol{\delta}|}.$$

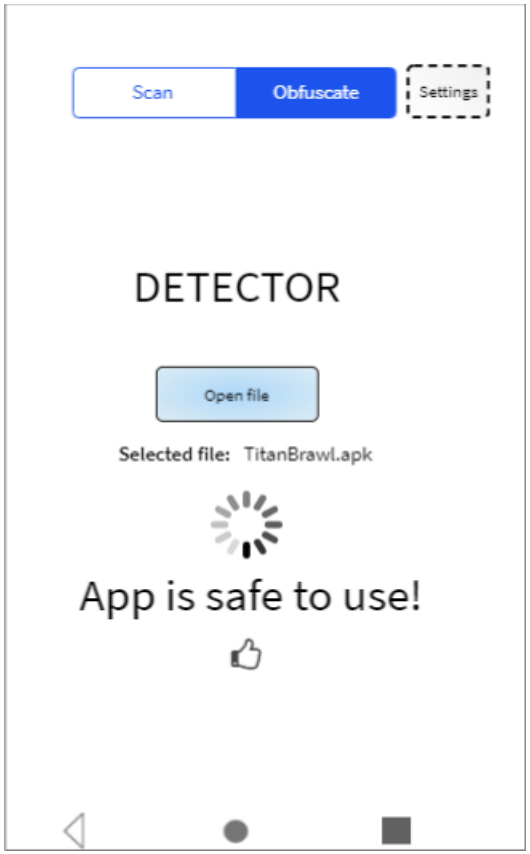
Інформаційна технологія виявлення шкідливого програмного забезпечення





Результати роботи програми





Інформаційна технологія виявлення шкідливого програмного забезпечення

	Швидкість виявлення шкідливого ПЗ	Ефективність виявлення шкідливого ПЗ	Навантаження на пристрій користувача
ESET Mobile Security & Antivirus	3.5 с	94%	33%
Avast Antivirus	2.8 с	96%	45%
AVG AntiVirus	3.0 с	94%	43%
DETECTOR	2.3 с	97%	3%

Висновки

- проведено аналіз сучасного рівня розвитку інформаційних технологій виявлення шкідливого програмного забезпечення;
- **визначено доцільність та** сформовано задачу розробки інформаційної технології виявлення шкідливого програмного забезпечення;
- Розроблено удосконалений алгоритм виявлення шкідливого ПЗ з використанням машинного навчання на основі динамічного та статичного аналізу;
- спроектовано та розроблено програмне забезпечення що реалізує інформаційну технологію.

АПРОБАЦІЇ ТА ПУБЛІКАЦІЇ

Наукові результати проведених досліджень апробовані на науково-технічній конференції у м.Влоцлавек, Польща.

Результати досліджень опубліковані у вигляді тез доповіді у збірнику праць та матеріалів конференції, оформлено статтю з результатими досліджень, а також оформлено заявку авторським рішенням комп'ютерної програми.

Дякую за увагу!