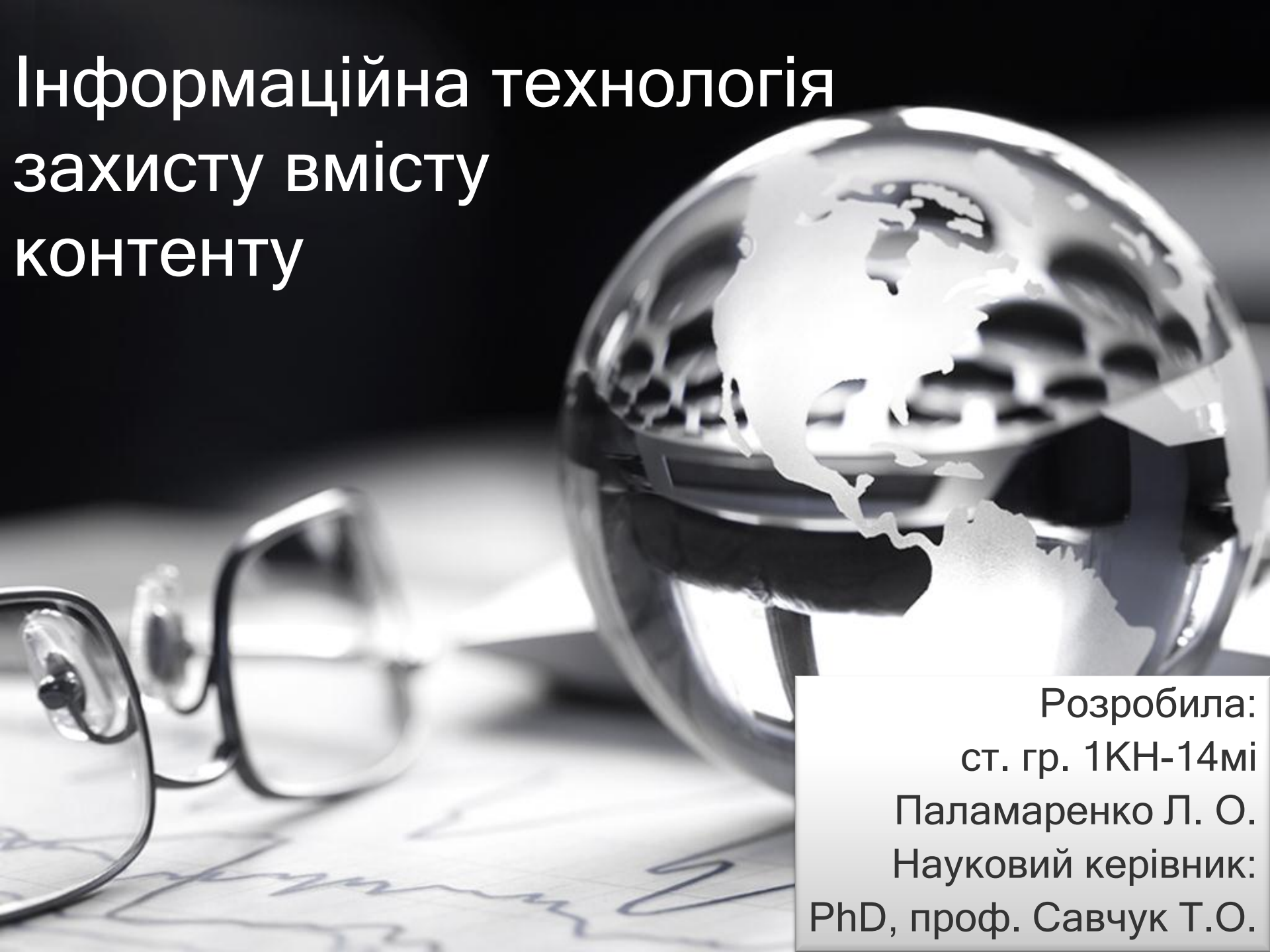
Інформаційна технологія захисту вмісту контенту



Розробила:
ст. гр. 1КН-14мі
Паламаренко Л. О.
Науковий керівник:
PhD, проф. Савчук Т.О.

Вступ

Актуальність розробки полягає в забезпеченні дотримання прав громадян та організацій через збереження інформації про їх особисте життя та діяльність, в тому числі конфіденційної, за допомогою інформаційної технології, яка дозволить прийняти рішення про наявний рівень захисту вмісту контенту та надати рекомендації щодо забезпечення необхідного рівня.

Метою дослідження в магістерській кваліфікаційній роботі є підвищення рівня захищеності вмісту контенту за рахунок впровадження інформаційної технології, яка базується на технічному аналізі програмного коду і діяльності IP-адрес.

Для досягнення поставленої мети необхідно розв'язати такі задачі:

- провести аналіз проблеми забезпечення захисту вмісту контенту;
- розглянути сучасні технології та методи захисту вмісту контенту;
- здійснити аналіз використання нечіткої логіки при прийнятті рішень в блокуванні адміністративної панелі;
- розробити інформаційну модель процесу забезпечення рівня захищеності вмісту контенту;
- розробити алгоритм захисту вмісту контенту;
- розробити удосконалений метод захисту вмісту контенту;
- розробити інформаційну технологію захисту вмісту контенту;
- провести моделювання та аналіз роботи процесу захисту вмісту контенту з використанням інформаційної технології.

Об'єкт дослідження – процес забезпечення захищеності вмісту контенту.

Предмет дослідження – технології захисту вмісту контенту.

Порівняльна характеристика існуючих сервісів захисту вмісту контенту

Назва сервісу / Функції	FalconStor FreeStor	Continuous Data Protector
Зручність інтерфейсу користувача	+	+
Можливість аналізу коду в мережі Інтернет	+	+
Можливість аналізу діяльності IP	-	+
Можливість завантажувати дані більше 1 Тб	-	+
Можливість аналізувати власний код	-	-
Можливість роботи за відсутності Інтернету	-	-

Постановка задачі

Нехай D (d_1, …, d_i) – якість проекту, де d_i – ступінь якості файлу, $i = \overline{1,3}$.

Значення параметра якості можна поділити на такі категорії:

d_1 - файл низької якості (підозрілий вміст);

d_2 - файл середньої якості (частково підозрілий вміст);

d_3 - файл високої якості (вміст без підозр).

Заданому набору параметрів файлу поставимо у відповідність один із показників d_j $(j = \overline{1, 3})$. Якщо файл з низькою якістю, то робота з ним буде заблокована у разі, коли зайва або некоректна інформація не буде виправлена.

Вектор змінних $X(x_1, \ldots, x_y)$ відображатиме параметри файлів для їх оцінювання, де x_y – кількісний параметр, $y = \overline{1,4}$.

В такому випадку x_1 – кількість символів в назві файлу відносно максимально заданого числа; x_2 – кількість закоментованих рядків коду; x_3 – кількість ключів, які використовуються; x_4 – середня кількість посилань для перелінковки.

Значення x_1 має діапазон значень від 10 – 15 %; x_2 – від 0.5 до 0.65 %; x_3 – від 28 до 32 %; x_4 – від 2.5 до 3.2 посилання/ст.

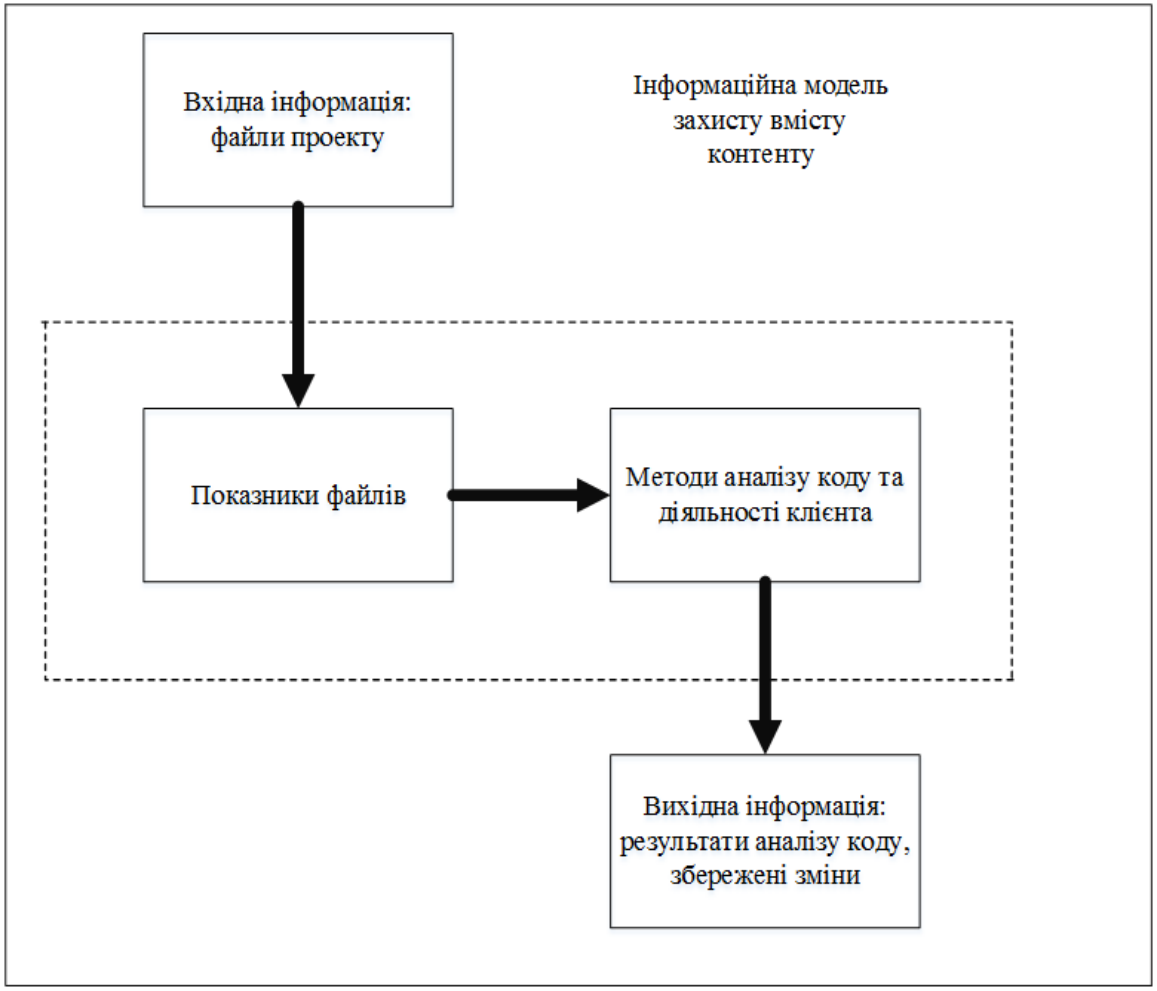
Тоді, з метою забезпечення захисту вмісту контенту слід проводити аналіз вектору параметрів файлів X, що дозволить оцінити рівень його захисту:

$$\mu^{d_j}(x_1, x_2, ..., x_n) = \bigvee_{p=1}^{k_j}\left[\bigwedge_{i=1}^{n}\mu^{a_i^{jp}}(x_j)\right],\ j=\overline{1,\ m}, \qquad (1.1)$$

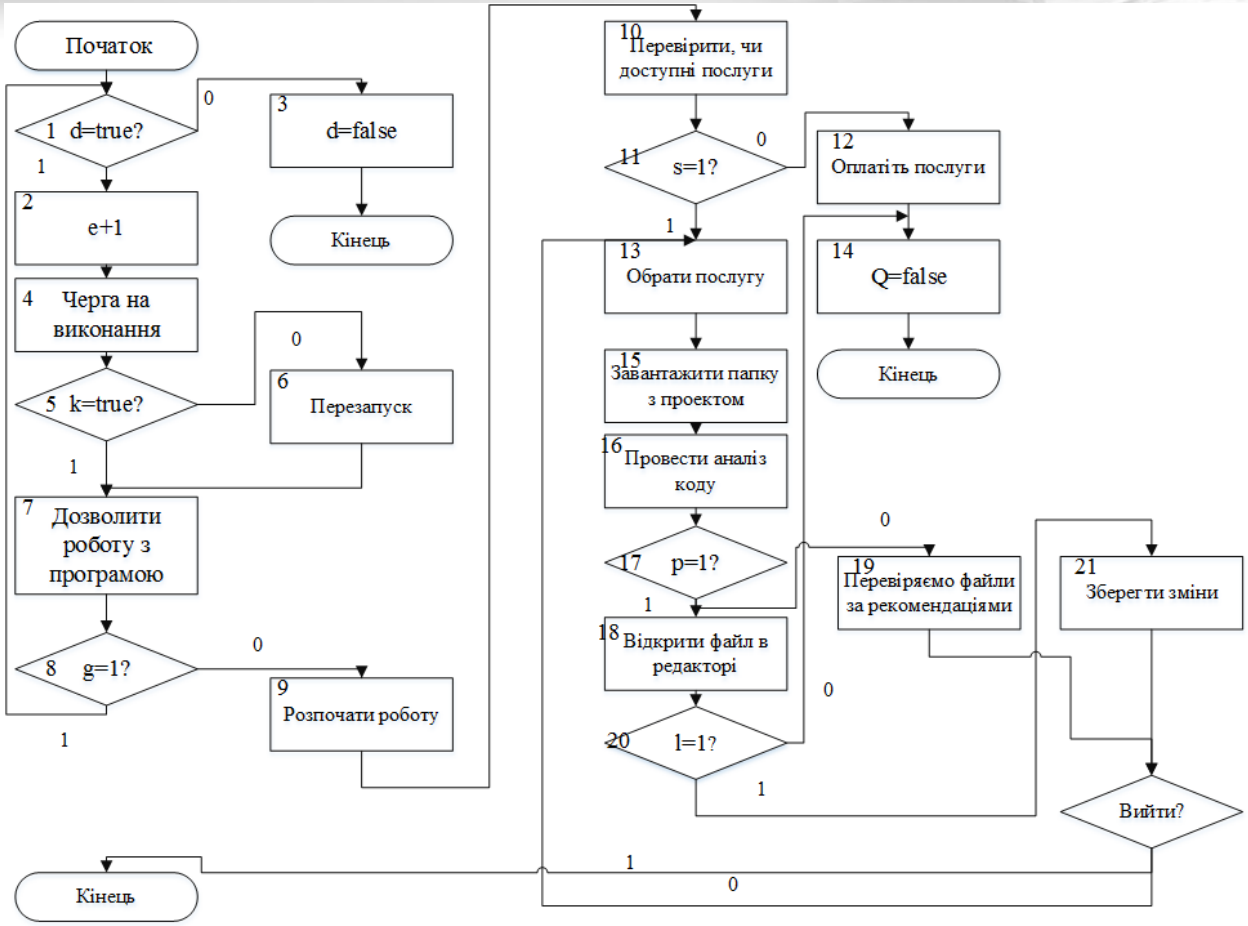
де $\mu^{a_i^{jp}}(x_i)$ – функція належності змінної $x_i \in [\underline{x}_i, \bar{x}_i]$ нечіткому терму a_i^{jp}, $i=\overline{1,\ n}$, $j=\overline{1,\ m}$, $p=\overline{1,\ k_j}$;

$\mu^{d_j}(x_1, x_2, ..., x_n)$ – функція належності вектора вхідних змінних $X=\{x_1, x_2, ..., x_n\}$ значенню вихідної змінної $y=d_j$, $j=\overline{1,\ m}$.

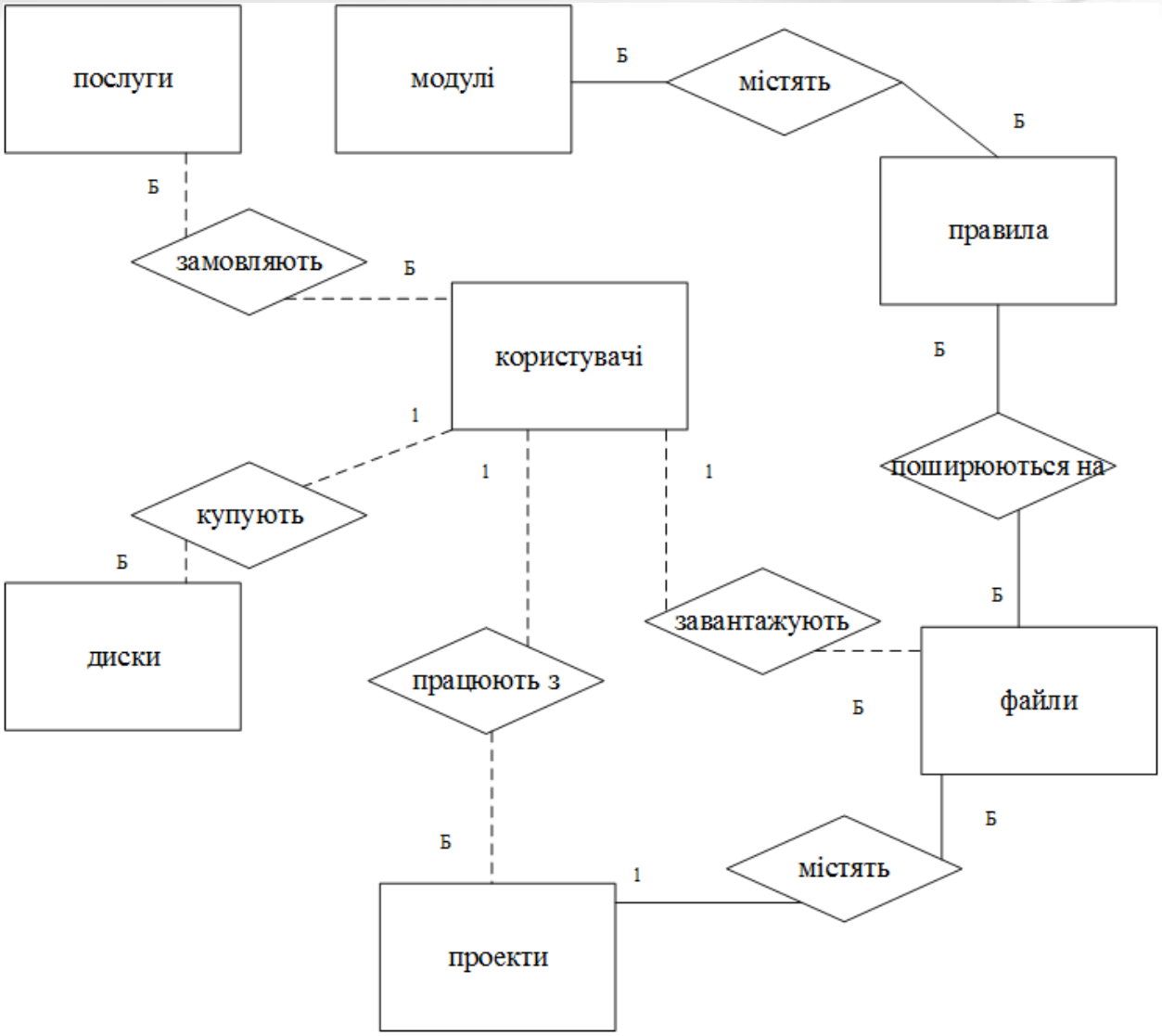
Схема інформаційної моделі захисту вмісту контенту



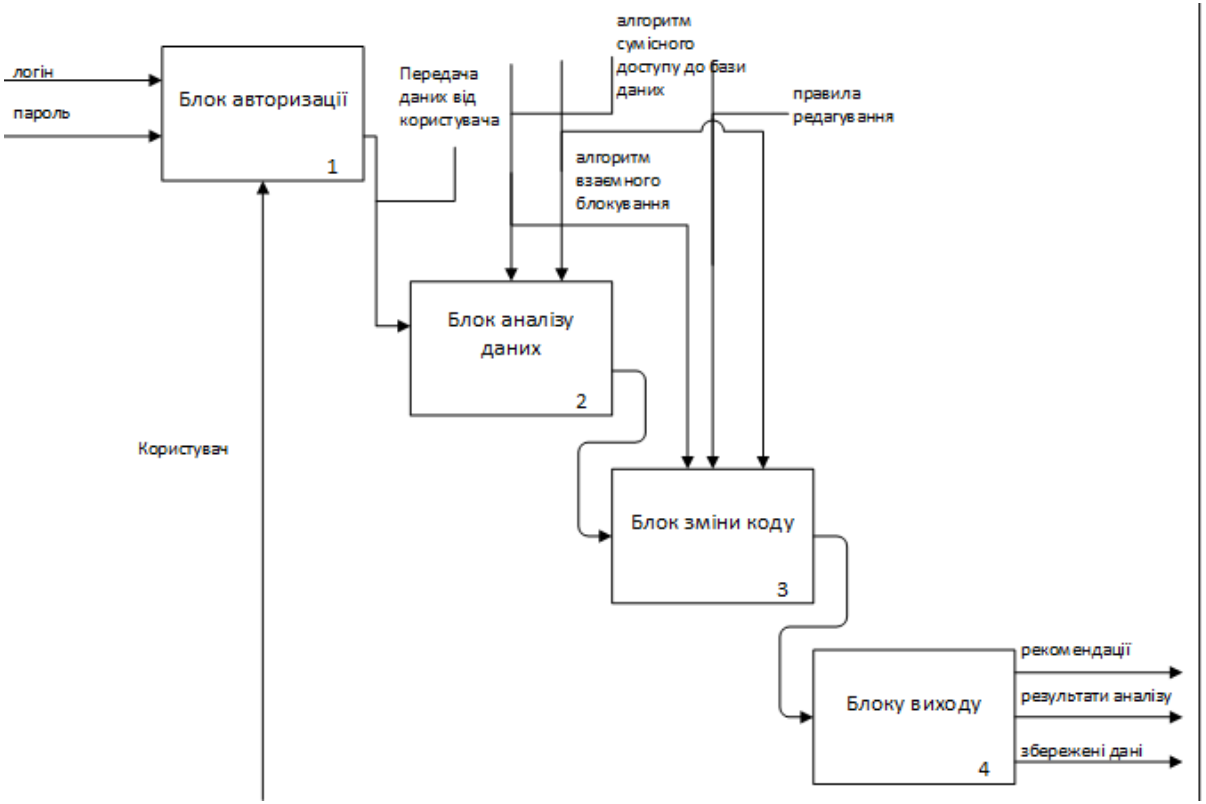
Удосконалений алгоритм захисту вмісту контенту

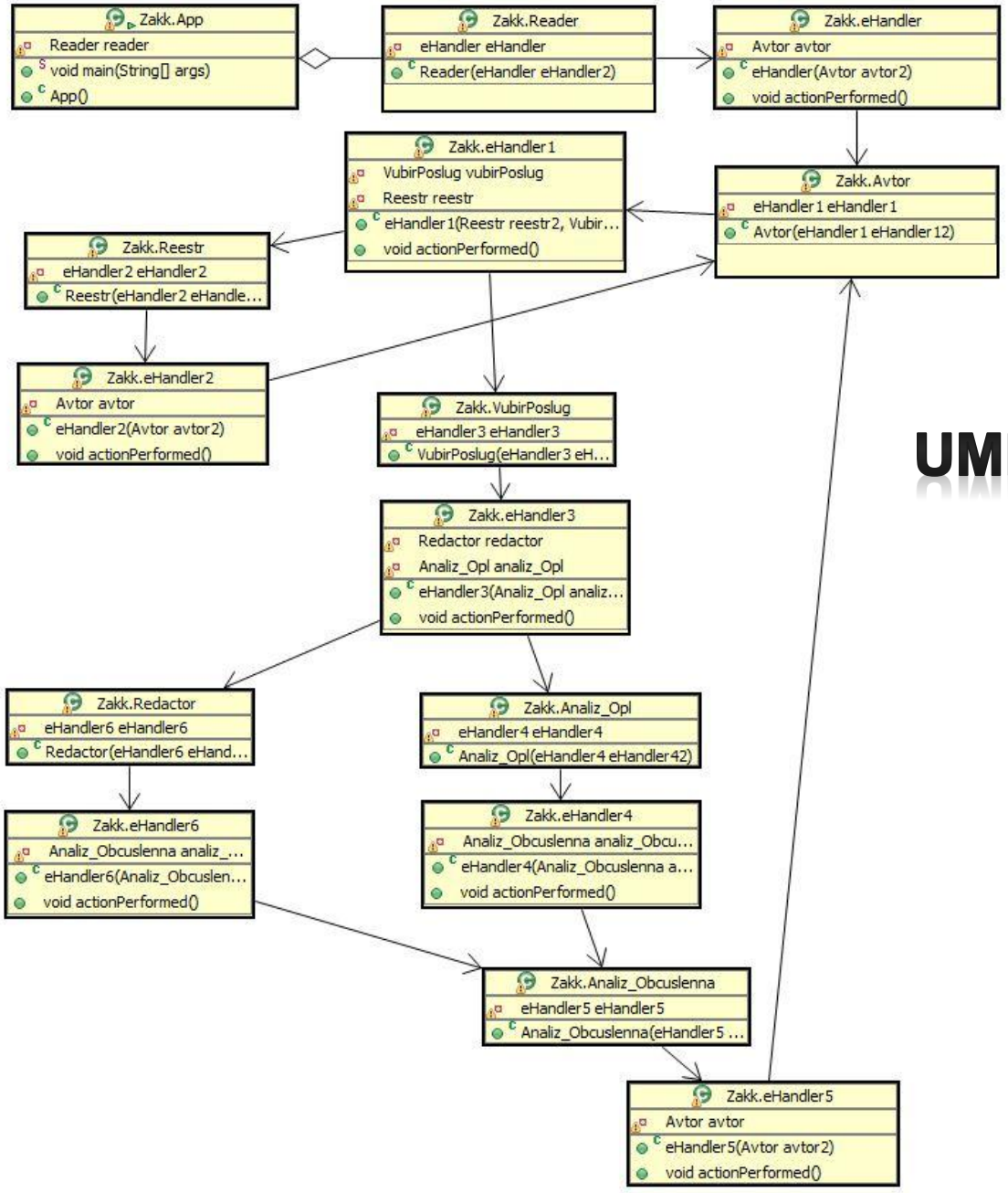


Концептуальна схема бази даних інформаційної технології захисту вмісту контенту



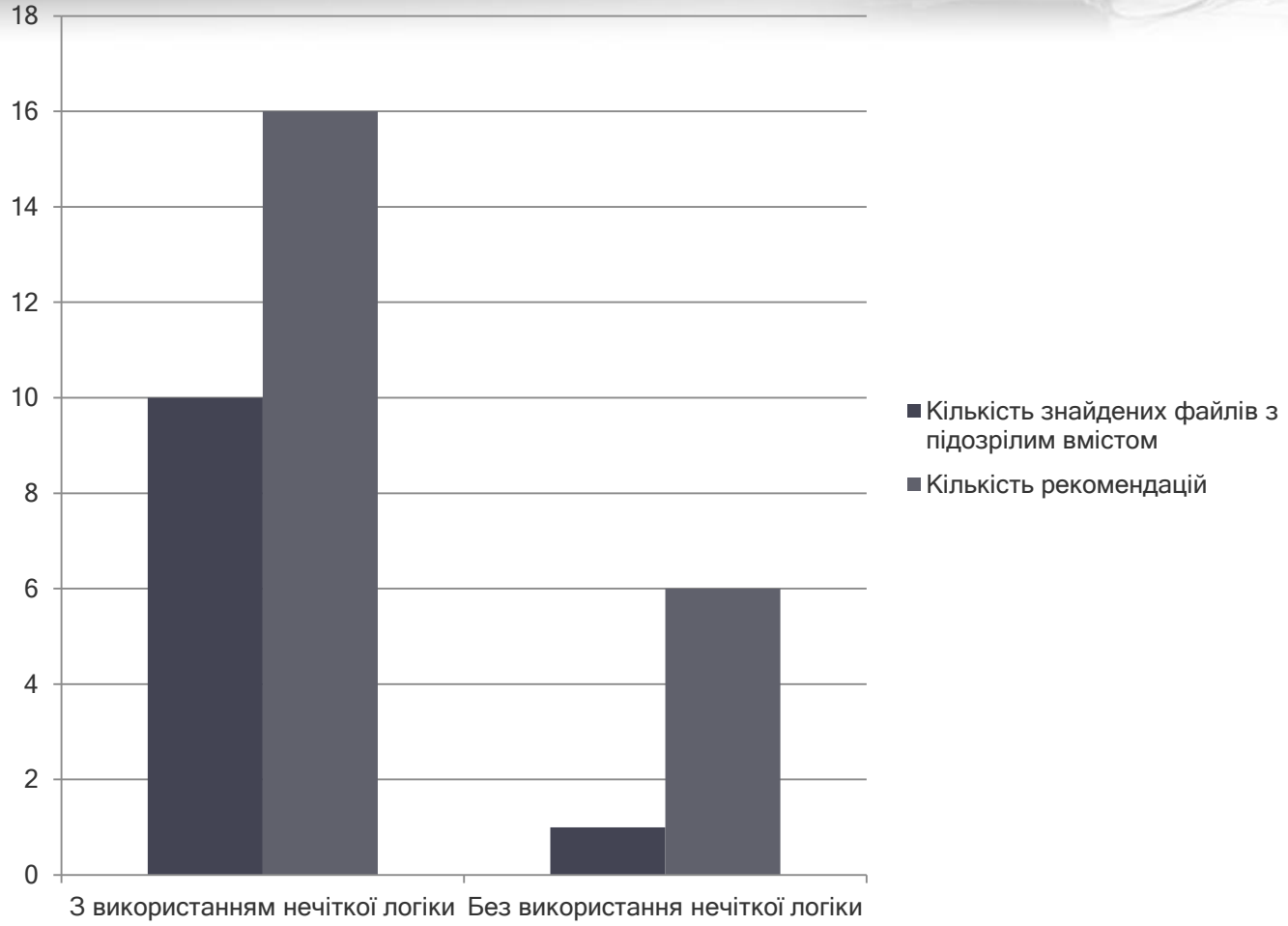
Структурна схема IDEF0 програмного засобу захисту вмісту контенту





UML_ДІАГРАМА КЛАСІВ

Результати аналізу роботи інформаційної технології захисту вмісту контенту



Результати роботи були апробовані на 1 міжнародній науковій конференції – «ІНТЕРНЕТ-ОСВІТА-НАУКА-2014» (м. Вінниця, Україна, 2014 р.), Всеукраїнській науково-практичній конференції молодих учених та студентів «Інтелектуальні технології в системному програмуванні» (м. Хмельницький, Україна, 2014 р.), та опубліковані у збірнику тез даної конференції; XLIII, XLIV науково-технічній конференції професорсько-викладацького складу, співробітників та студентів університету, співробітників та студентів Вінницького національного технічного університету (м. Вінниця, Україна, 2014 – 2015 рр.) та опубліковані у збірниках тез даних конференцій.

Висновки

Дана розробка в подальшому може використовуватись як додаткова система забезпечення захисту вмісту контенту, а також підвищити рівень захисту комп'ютера в мережі.

В результаті виконання магістерської кваліфікаційної роботи було здобуто наступні наукові та практичні результати:

Виходячи з аналізу сучасного стану розвитку технологій захисту вмісту контенту встановлено, що доцільним для забезпечення достатнього рівня захищеності є використання засобів інтелектуального аналізу даних. З урахуванням недоліків існуючих технологій і сервісів, зроблено висновок про актуальність і доцільність розробки інформаційної технології захисту вмісту контенту.

Запропоновано інформаційну модель захисту вмісту контенту, що передбачає аналіз вектору параметрів файлів X, з метою оцінювання рівня захисту вмісту контенту. При цьому, вхідною інформацією є файли, а вихідною – висновок, який включає множину файлів, які відповідають вимогам користувача щодо рівня захищеності, а також рекомендації стосовно підтримки заданого рівня захищеності.
Удосконалено алгоритм захисту вмісту контенту, що дозволило підвищити рівень захищеності, та, за рахунок використання нечіткої логіки, підвищити інформативність користувачів.

Висновки

- Розроблено структуру і UML-діаграму взаємодії класів інформаційної технології захисту вмісту контенту, які відображають процеси авторизації, реєстрації, завантаження програмного коду, аналізу і редагування його коду, формування рекомендацій.
- Розроблено реляційну базу даних користувачів інформаційної технології, які замовляють послуги. Описані структури даних призначені для зберігання інформації, надання швидкого доступу до неї та фільтрації файлів

  за рахунок використання теорії нечітких множин.
- Розроблено програмний засіб, що реалізує інформаційну технологію захисту вмісту контенту, і надає можливість збільшити рівень захищеності за рахунок використання удосконаленого алгоритму та нечіткої логіки.
- Результати дослідження, отримані під час виконання магістерської кваліфікаційної роботи, підтверджують підвищення рівня захищеності за рахунок збільшення кількості файлів з підозрілим вмістом і надання більшої кількості рекомендацій для забезпечення повного захисту на внутрішньому і зовнішньому рівнях.

У ході виконання економічної частини кваліфікаційної роботи на основі розрахунків було доведено, що новий програмний продукт є економічно доцільним, оскільки витрати на розробку вказаного засобу з використанням відповідної інформаційної технології становлять 68525,3 грн. Показник абсолютної ефективності вкладених інвестицій $E_{абс}$ = 70868 грн, відносної – 40%, а термін окупності інвестицій становить 2,5 роки.

Дякую за увагу!