Дипломний проект на тему:
«Система підтримки прийняття рішень при оцінюванні ризиків інформаційної безпеки підприємства »

Виконано студентом групи БС-16 сп. Ратніков Н.О.
Науковий керівник: к.т.н., доцент., каф. ЗІ Куперштейн Л.М.

МЕТА ТА ЗАДАЧИ ДИПЛОМНОІ РОБОТИ

Метою дипломної роботи є підвищення інформаційної безпеки підприємства за рахунок розробки та впровадження засобу оцінки ризику інформаційної безпеки

Для досягнення мети необхідно виконати такі задачі:

- Проаналізовати літературні джерела з інформаційної безпеки.
- Розглянути методики оцінки ризиків інформаційної безпеки (ІБ).
- Провести аналіз програмних засобів для оцінки ризиків ІБ.
- Проаналізовати структуру підприємства.
- Розглянути основні загрози ІБ на підприємстві.
- Розробити ієрархічну модель оцінки ризиків ІБ.
- Розробити програмний засіб для оцінки ризиків ІБ.

Техніко економічне обґрунтування

Дивлячись на те що в даний час на ринку є велика кількість ПЗ, користувач придбає те що є більш дешевим, але не уступить по параметрам дорожчим програмним засобам. Тому необхідно оцінити конкурентоспроможність розроблюваного виробу.

Конкурентоспроможність можна оцінити за формулою:

$$К = \frac{I_{т.п.}}{I_{е.п.}}$$

Техніко економічне обґрунтування

Показник	Варіанти		Коефіцієнт вагомості параметра
	Базовий (товар-конкурент)	Новий (інноваційне рішення)	
Нормативний параметр: Ліцензія	+	+	0,1
Технічний параметр: Трудомісткість	Середня	Висока	0,5
Економічні параметри: Ціна	11356,4 грн.	8548,2 грн.	0,3
Експлуатаційні витрати	10500 грн./рік	6751,29 грн./рік	0,1

$$K = \frac{1{,}904}{0{,}7} = 2{,}72$$

А отже, К>1 то інноваційне рішення вважається більш конкурентоспроможним, ніж товар-конкурент, обраний за базу для порівняння

Економічне обґрунтування доцільності розробки

Витрати на розробку продукту: 8290,2 грн.

Собівартість ПЗ: 2580,23 грн.

Чистий прибуток виробника: 19362,96 грн.

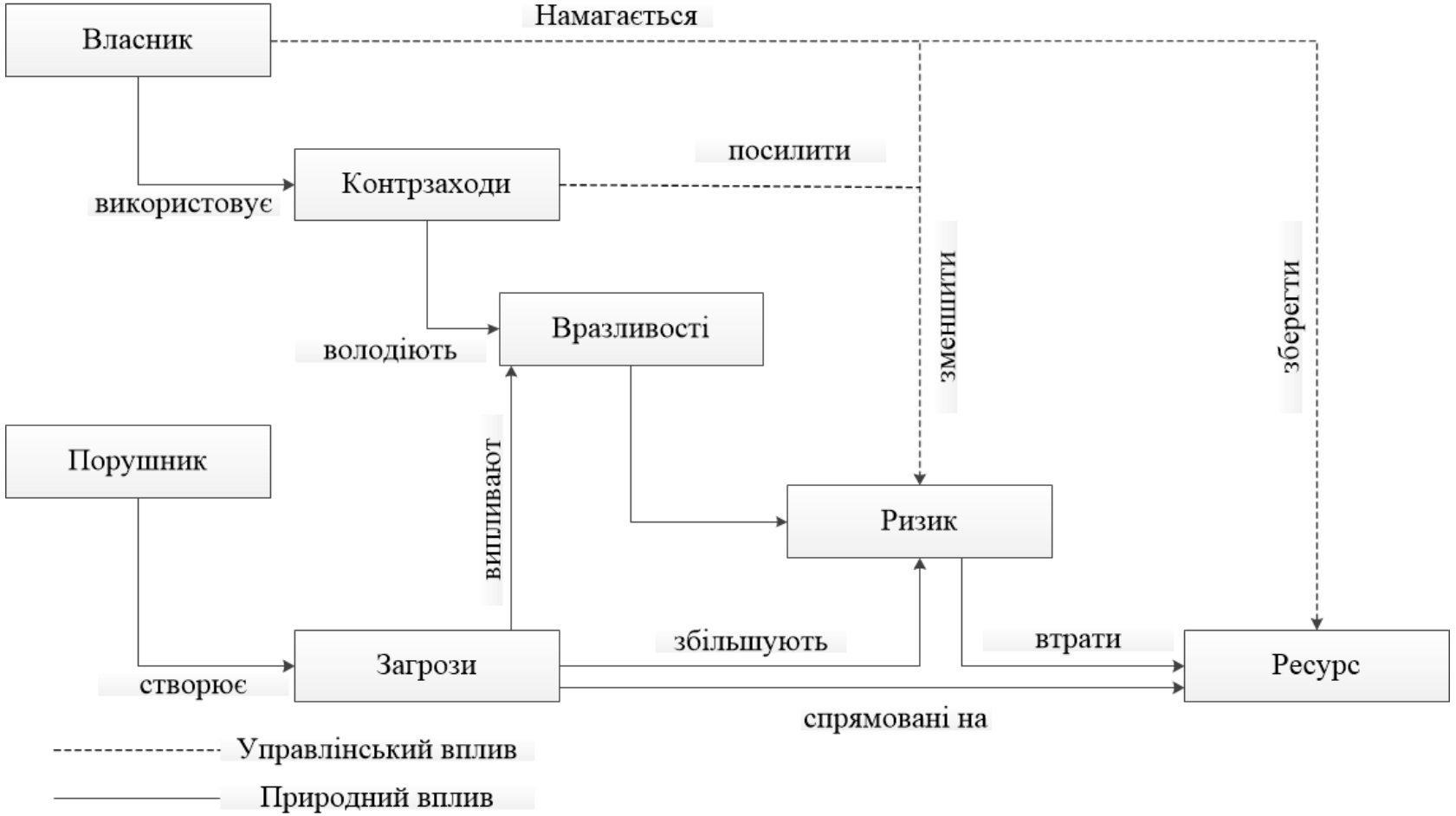
Експлуатаційні витрати: 6751,29 грн.

Річний економічний ефект: 5613,3 грн.

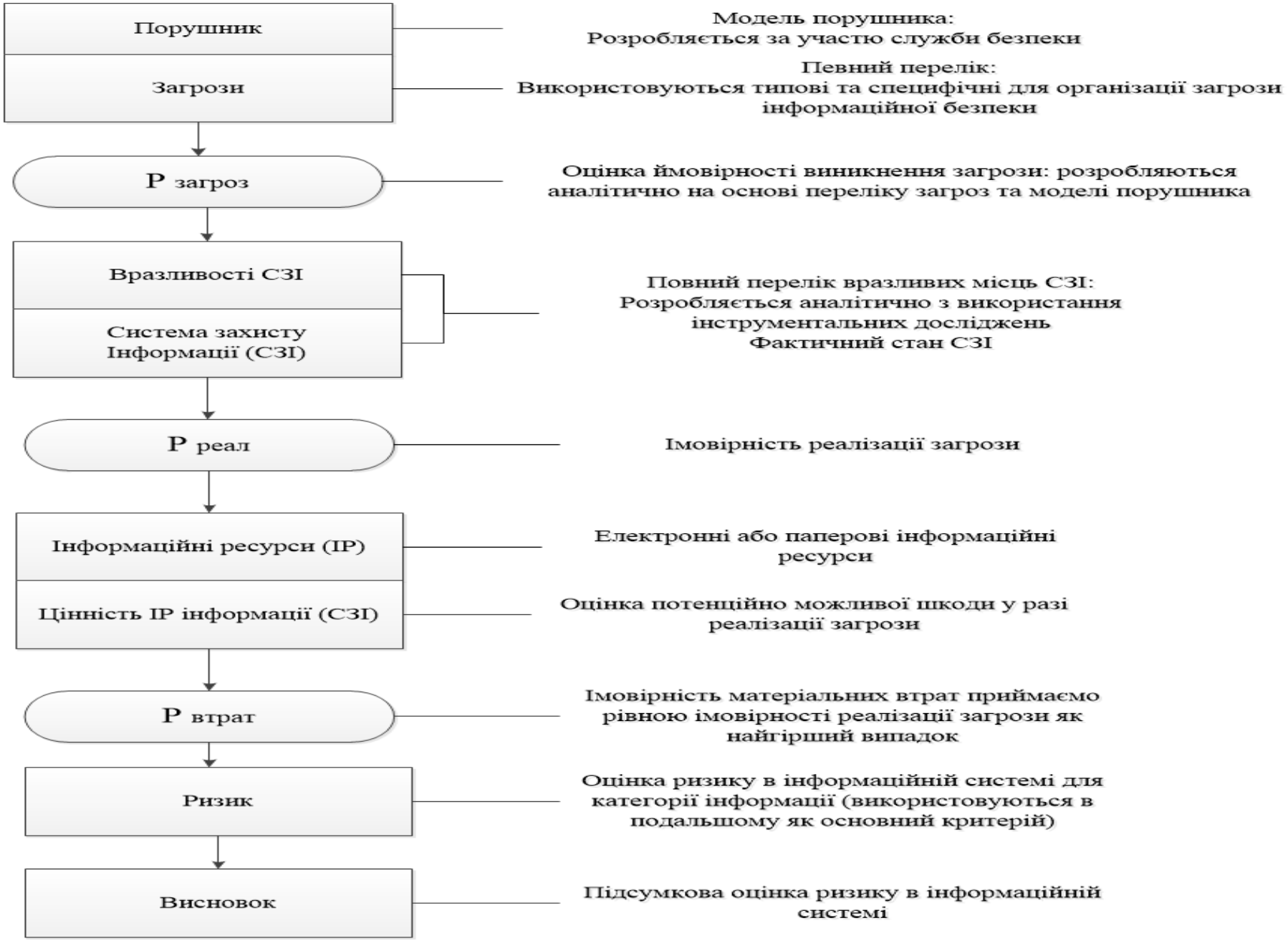
Термін окупності: 0,15.

Тобто розробка такого ПЗ окупить себе за 0,15 року. Ці результати свідчать про доцільність розробки нового продукту та її ефективність.

Модель системи безпеки підприємства в інформаційній сфері



Алгоритм оцінювання інформаційних ризиків



Методи оцінки ризиків

Методи оцінки	Кількісні методи	Якісні методи
Переваги	– Дозволяють чисельно оцінити необхідні параметри. – Реалізують аналіз витрат і прибутку при виборі захисту. – Надають більш точне відображення шуканих значень.	– Дозволяють визначити області критичних рівнів в короткий час і без значних витрат. – Дозволяють оцінювати відносно легко і дешево.
Недоліки	– Кількісні заходи залежать від обсягу і точності використовуваної шкали виміру. – Результати оцінки можуть бути неточними і вводити в оману. – Повинні бути доповнені якісним описом. – Оцінка, що проводиться із застосуванням цих методів, як правило, дорожче, вимагає більшого досвіду і сучасного інструментарію.	– Чи не дозволяють визначити ймовірності і результати з використанням числових коефіцієнтів. – Аналіз витрат і вигод при виборі – захисту складніший. – Отримані результати носять загальний, наближений характер.

Характеристики існуючий засобів аналізу ризиків

	RA2 art of risk	Risk Advisor	RiskWatch	CRAMM	Авангард Аналіз	ГРИФ Ф	технологія аналізу ризиків
Простота використання	+	+	+	+/-	+/-	+	+
метод отримання даних	пряма оцінка ймовірності.	пряма оцінка ймовірності.	пряма оцінка ймовірності.	пряма оцінка ймовірності.	пряма оцінка ймовірності.	пряма оцінка ймовірності	Метод аналізу ієрархій
Можливість підстроювання роботи	-	-	-	є профіль роботи	може виконати експерт	-	+
Використовуваний стандарт по ІБ	ISO 17799	ISO 17799	ISO 17799	ISO 17799	ГОСТ К 15408	ISO 17799	BSI
Облік загроз для ресурсів	+	+	+	+	+	+	+
Облік загроз для служб	+	-	+	+	+	+	+

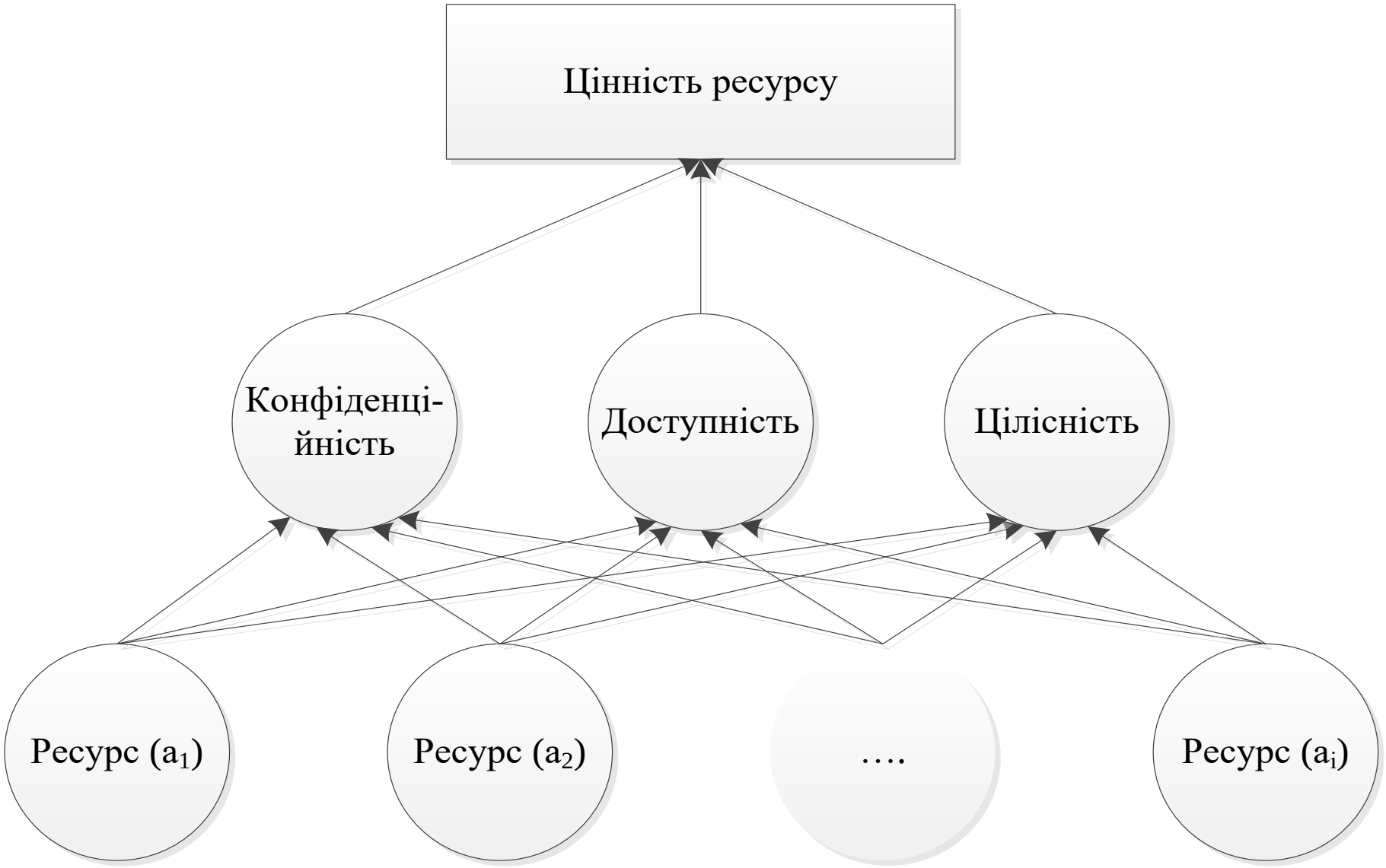
Типові інформаційні ресурси підприємства

Групи	Види
Сервіси	– Інтернет; – інші мережі загального призначення; – телефонія; – Служби групового створення гіпертексту.
Дані	– звіти по виробництву; – контракти, акти, накази; – фінансові звіти; – база працівників; – база клієнтів;
Програмне забезпечення	– операційна система; – програмне забезпечення; – бухгалтерські додатки; – офісні додатки; – антивірусні додатки;
Апаратні засоби	– комутатор; – маршрутизатор; – робоча станція; – модем; – сервер;
Кадрові ресурси	– Персонал

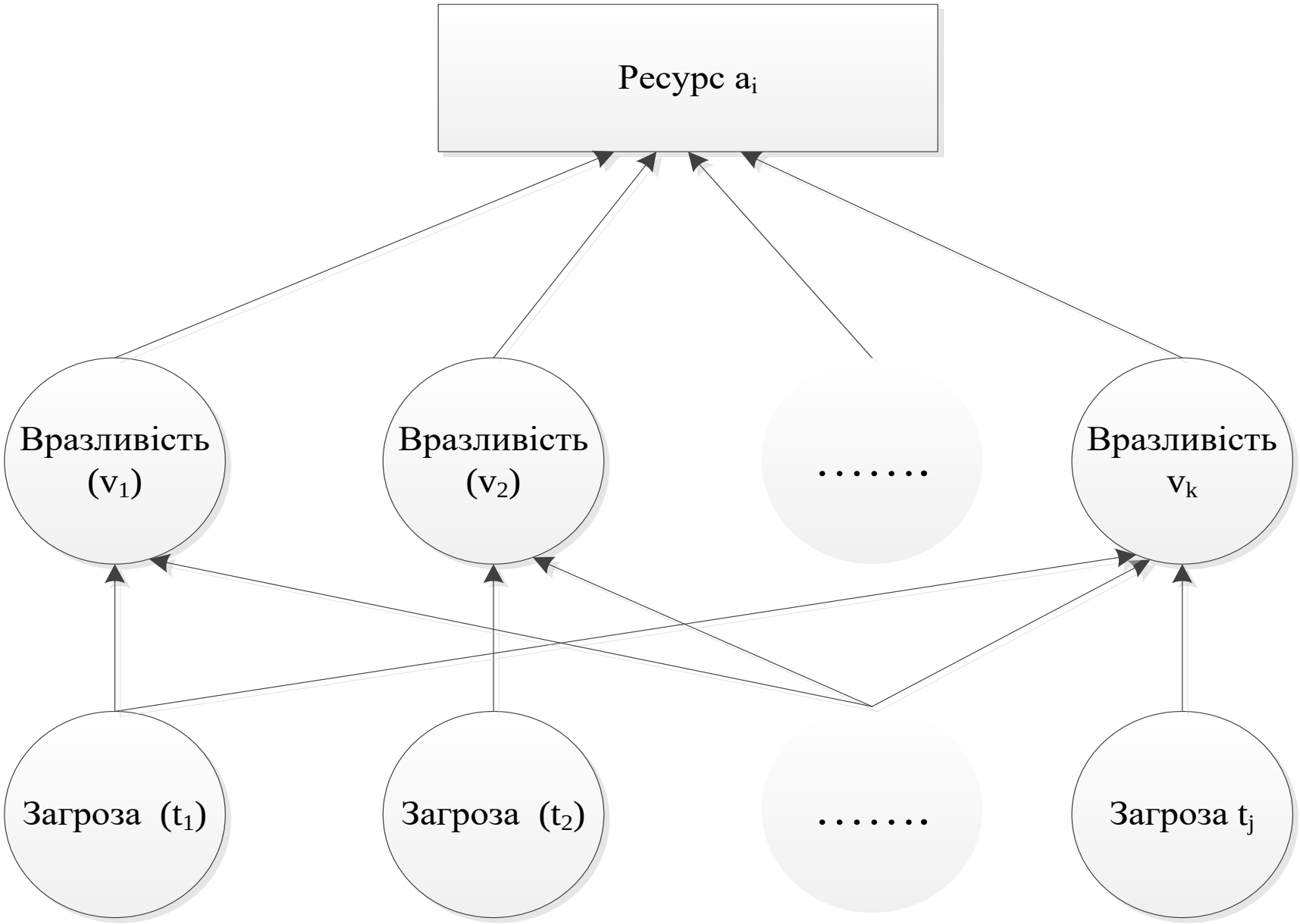
Приклад загроз і вразливостей по певному ресурсу

	Вразливість	Загроза, яка використовує вразливість
РЕСУРСИ КОНТРОЛЮ ДОСТУПУ		
1	Неправильне розмежування доступу в мережах	Обхід механізмів контролю системи або додатки
2	Відсутня або некоректна політика контролю доступу	Несанкціоновані підключення до мереж
3	Відсутність механізмів ідентифікації і автентифікації	Втрата або пошкодження інформації
4	Відсутність захисту мобільного ком. обладнання	Привласнення чужого призначеного для користувача ідентифікатора
5	Відсутність політик чистих столів і чистих екранів	Використання програмного забезпечення неавторизованими користувачами
6	Відсутність “виходу з системи”, коли покидається робоча станція	Несанкціонований доступ до інформації

Загальна ієрархічна модель цінності ресурсу



Загальна ієрархічна модель загроз та вразливостей



Модель розрахунку ризику інформаційної безпеки

$$R_{ijk} = \left(a_i \cdot \sqrt{t_{ij} \cdot v_{ik}}\right)^{1/2}$$

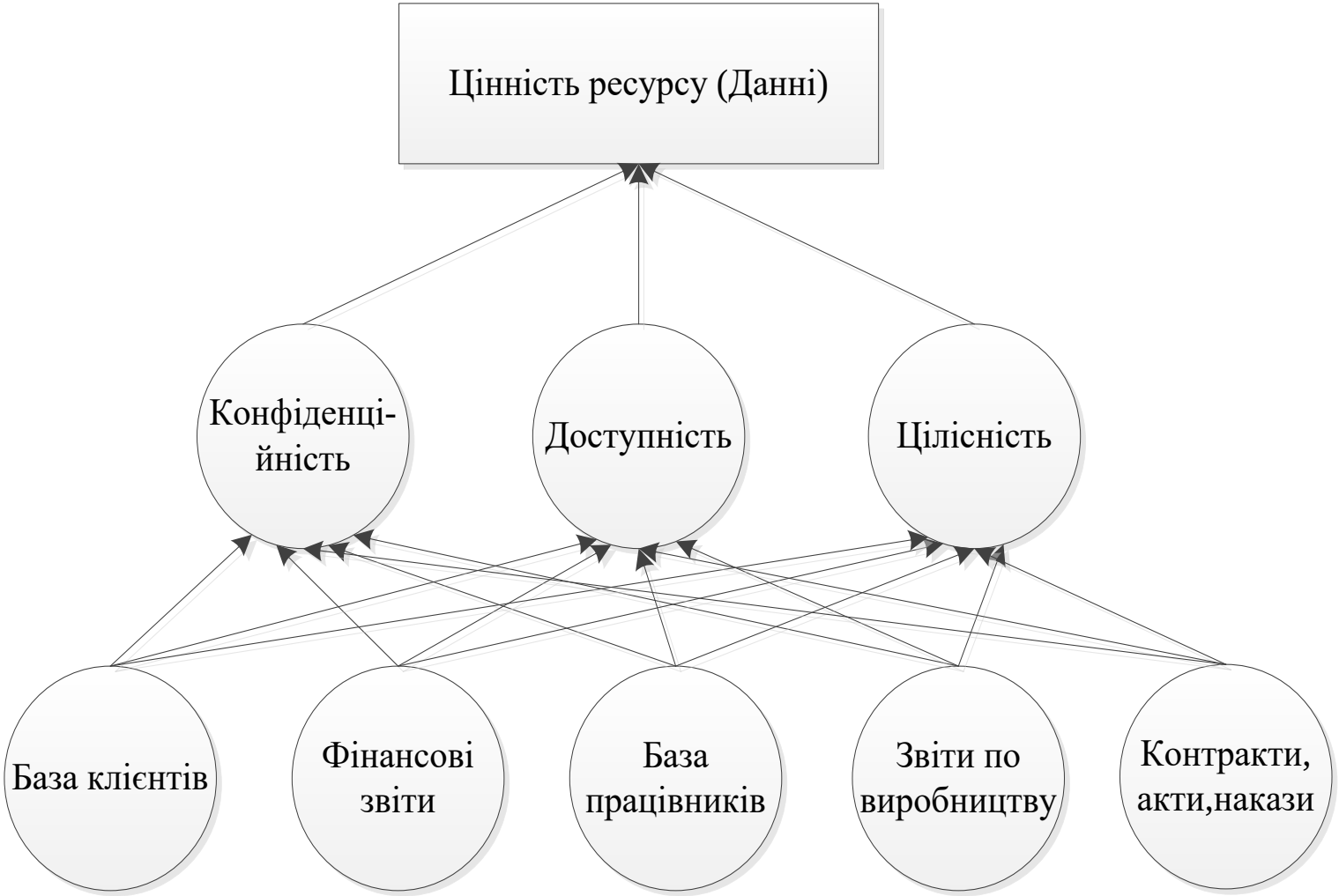
$$T = \{t_1, t_2, \ldots . t_j\}$$

$$A = \{a_1, a_2, \ldots . a_i\}$$

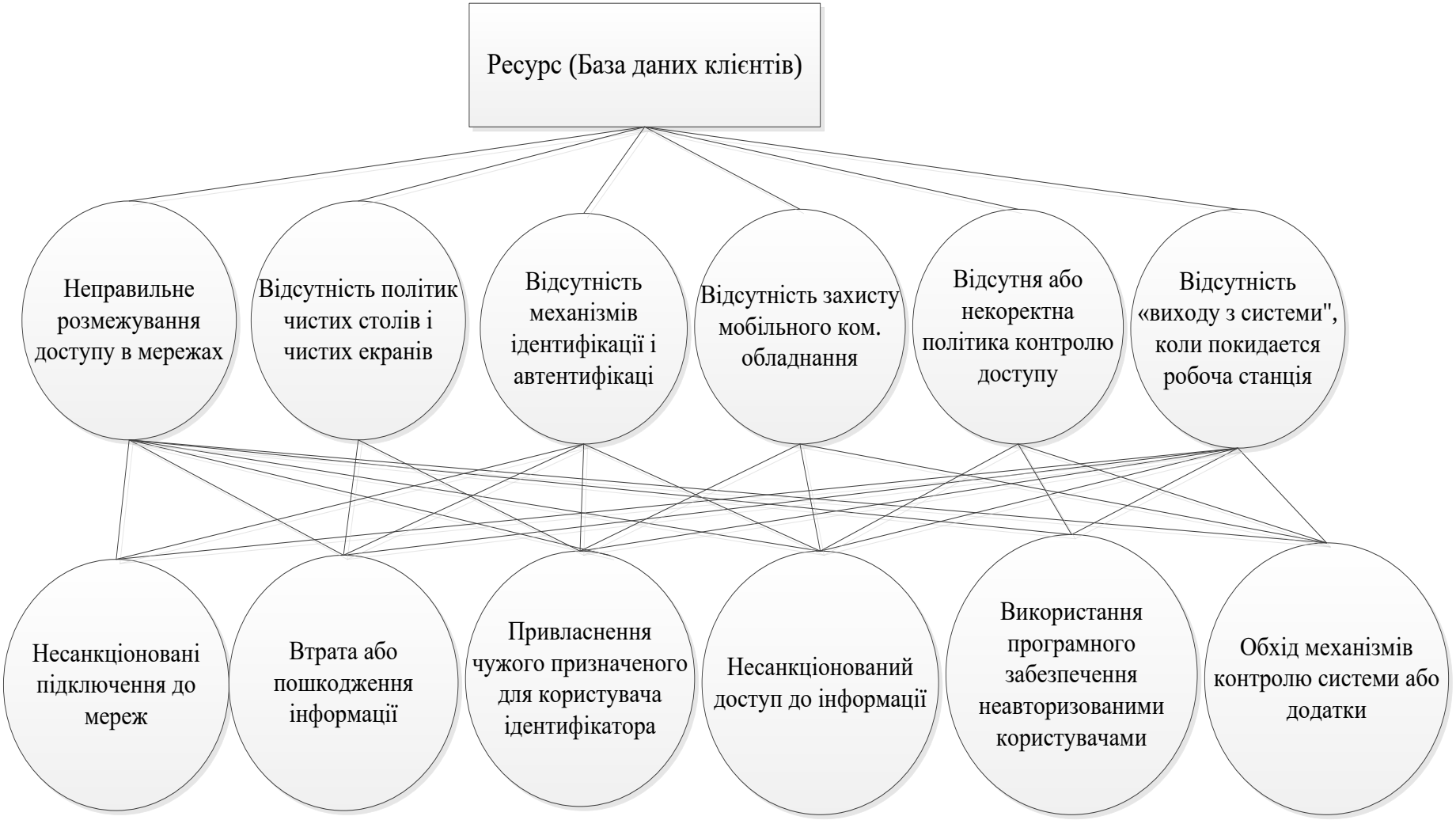
$$V = \{v_1, v_2, \ldots . v_k\}$$

Де Rijk величина ризику ресурсу A_i (i = 1,2, ..., m) можливою загрозою T_j (j = 1,2, ..., n) через вразливість V_k (K = 1, 2, .. ., h);
A_i цінність ресурсу A_i;
T_{ij} ступінь небезпеки загрози T_j для ресурсу A_i;
V_{ik} ступінь небезпеки вразливості V_k для ресурсу A_i, які можуть призвести до реалізації загрози T_j.

Ієрархічна модель цінності ресурсу групи «данні»



Ієрархічна модель загроз та вразливостей ресурсу «База клієнтів»



Результати розрахунку

Аспекти оцінки ризику	Вага певного критерія
Ресурси (A_i)	1. База клієнтів (0,317) 2. База працівників (0,260) 3. Фінансові звіти (0,180) 4. Звіти по виробництву (0,180) 5. Контракти, акти, накази (0,122) 6. Рекламні звіти (0,121)
Вразливості (V_i)	1. Неправильне розмежування доступу в мережах (0,278) 2. Відсутня або некоректна політика контролю доступу (0,248) 3. Відсутність механізмів ідентифікації і автентифікації (0,163) 4. Відсутність захисту мобільного ком. Обладнання (0,158) 5. Відсутність політик чистих столів і чистих екранів (0,154) 6. Відсутність «виходу з системи", коли покидається робоча станція (0,121)
Загрози (T_i)	1. Обхід механізмів контролю системи або додатки (0,401) 2. Несанкціоновані підключення до мереж (0,182) 3. Втрата або пошкодження інформації (0,182) 4. Привласнення чужого призначеного для користувача ідентифікатора (0,132) 5. Використання програмного забезпечення неавторизованими користувачами (0,045) 6. Несанкціонований доступ до інформації (0,055)

Результати розрахунку ризику інформаційної безпеки

Ресурси	Загрози	Вразливості						Результат ризику R	
		V_1	V_2	V_3	V_4	V_5	V_6		
A_1=0,317	T_1	0,1282	0,1288	0,1230	0,1732	0,1514	0,1332		
	T_2	0,1472	0,2087	0,1977	0,2197	0,1455	0,1673	0,2391	Мак.
	T_3	0,1507	0,1661	0,2290	0,2135	0,2273	0,1938	0,1282	Мін
	T_4	0,1306	0,1552	0,1739	0,1582	0,1452	0,2075	0,1784	Сер.
	T_5	0,1283	0,1499	0,1286	0,1397	0,1314	0,1439		
	T_6	0,1285	0,1416	0,1341	0,1904	0,1665	0,1335		

Структурна схема програмного засобу

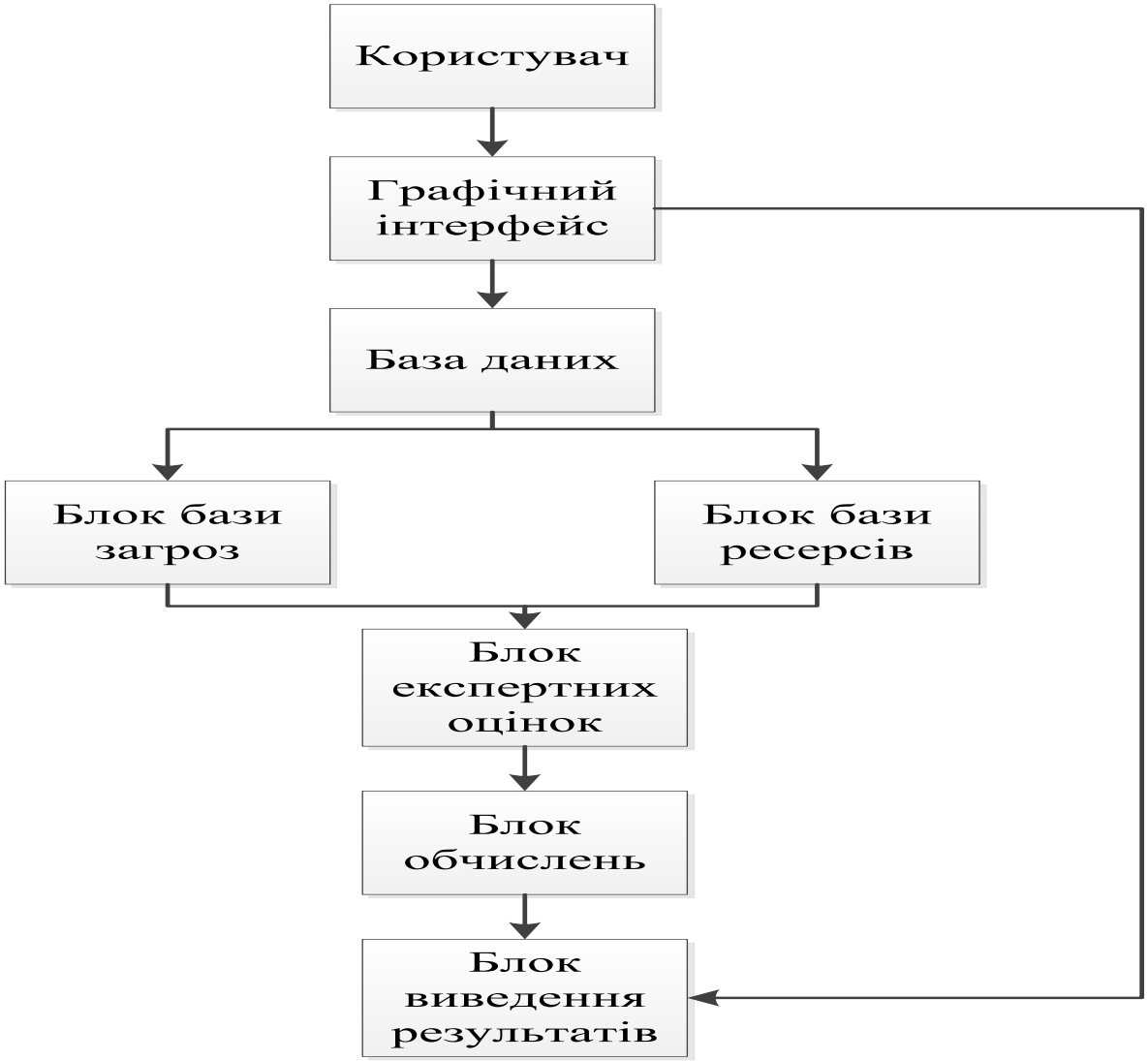
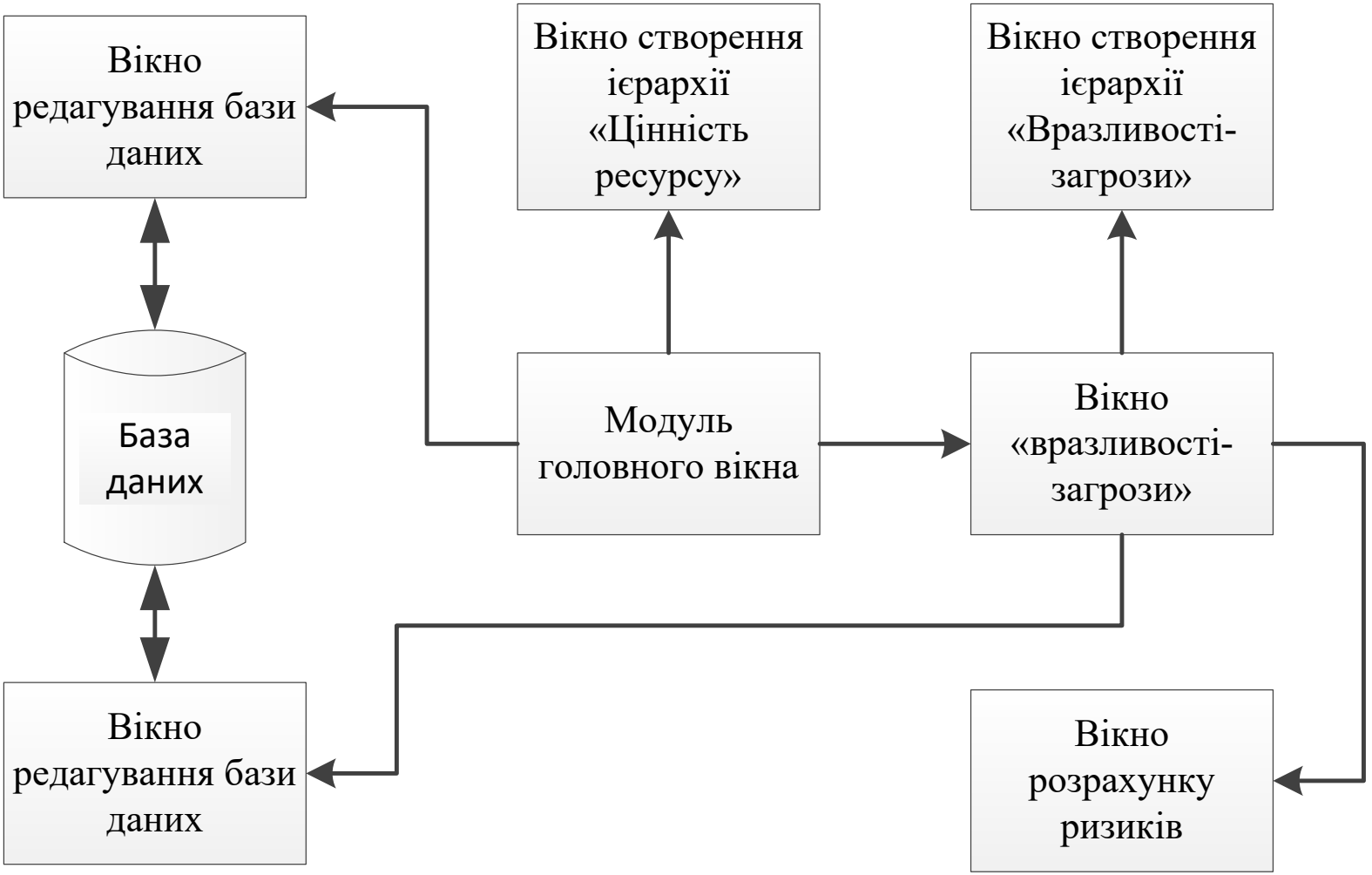
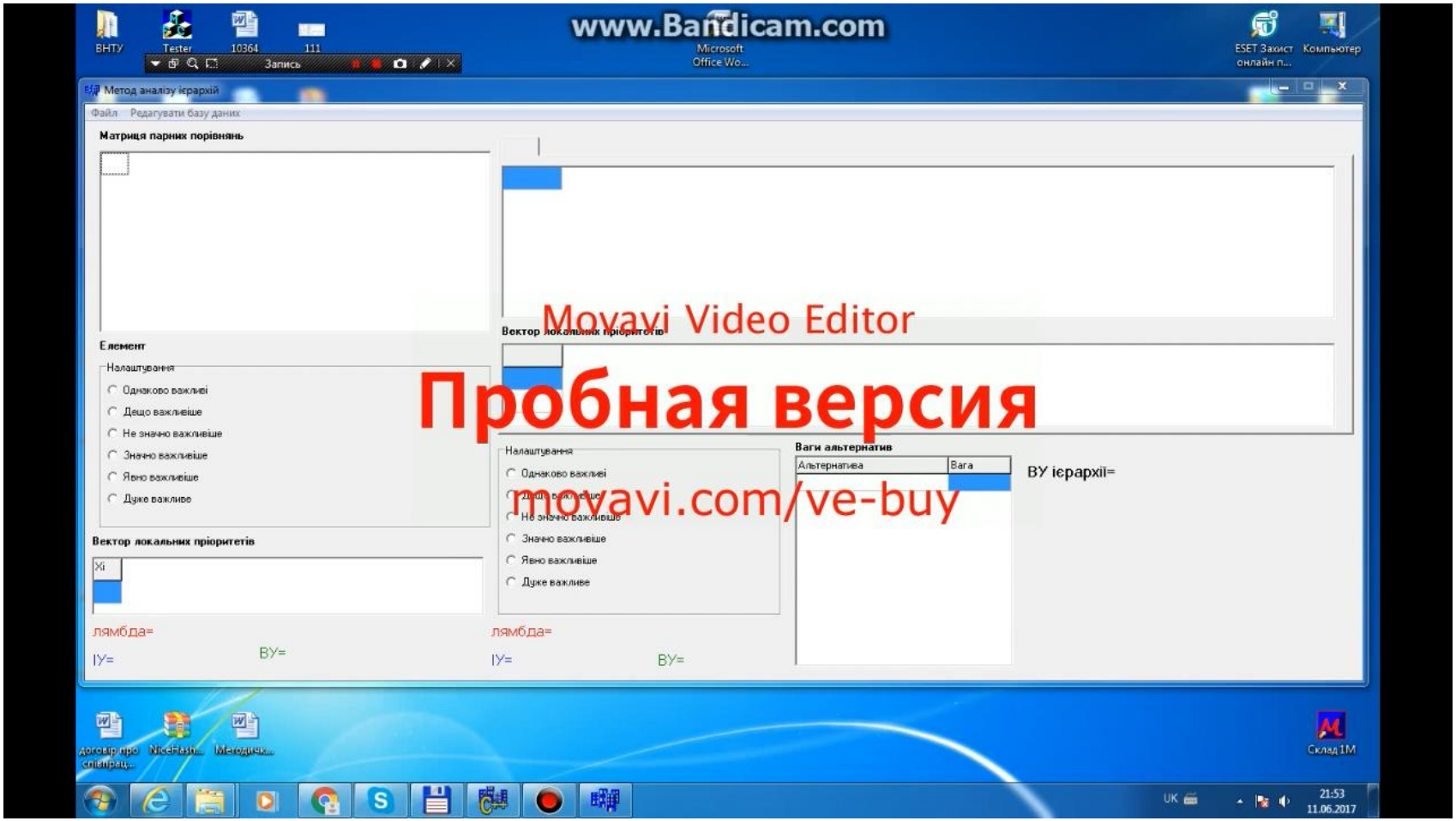


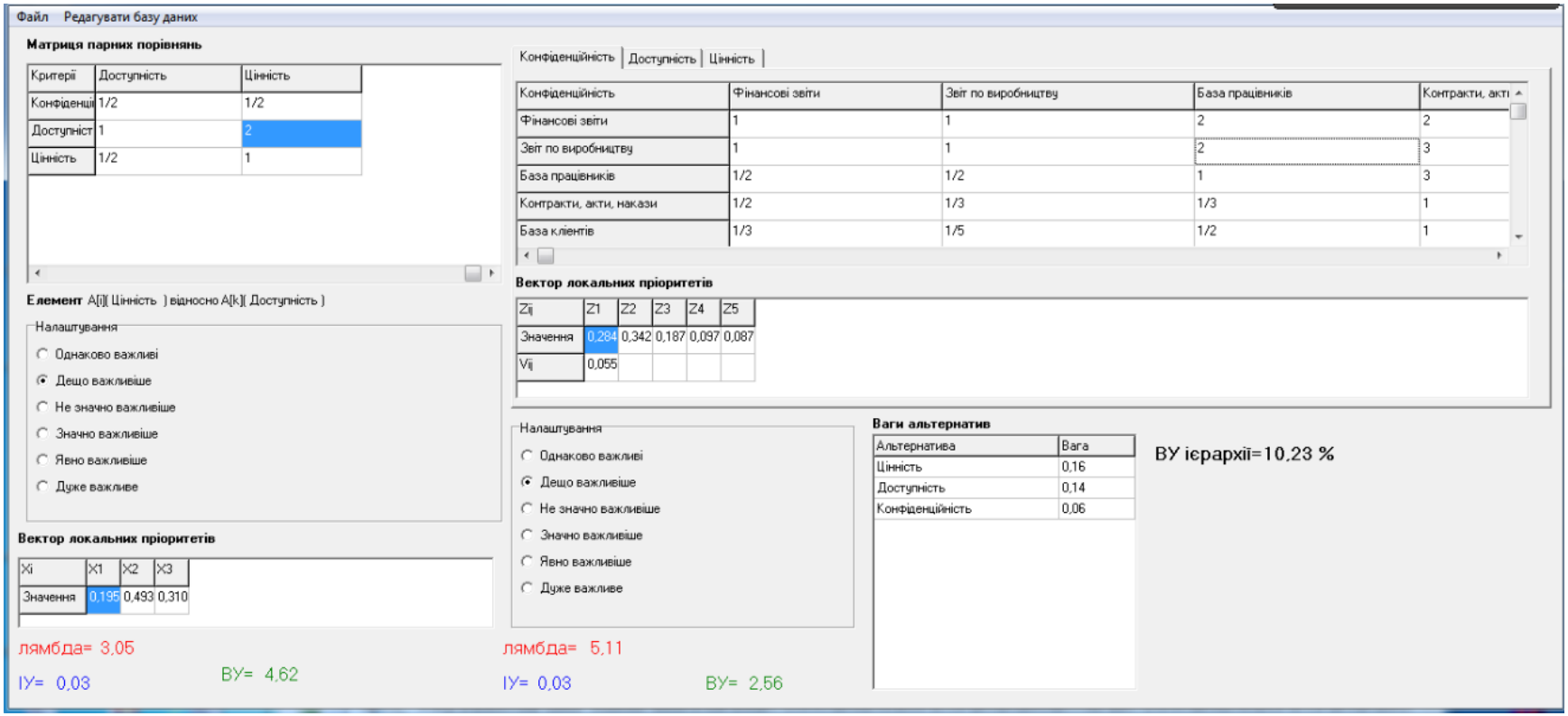
Схема інтерфейсових модулів програмного засобу



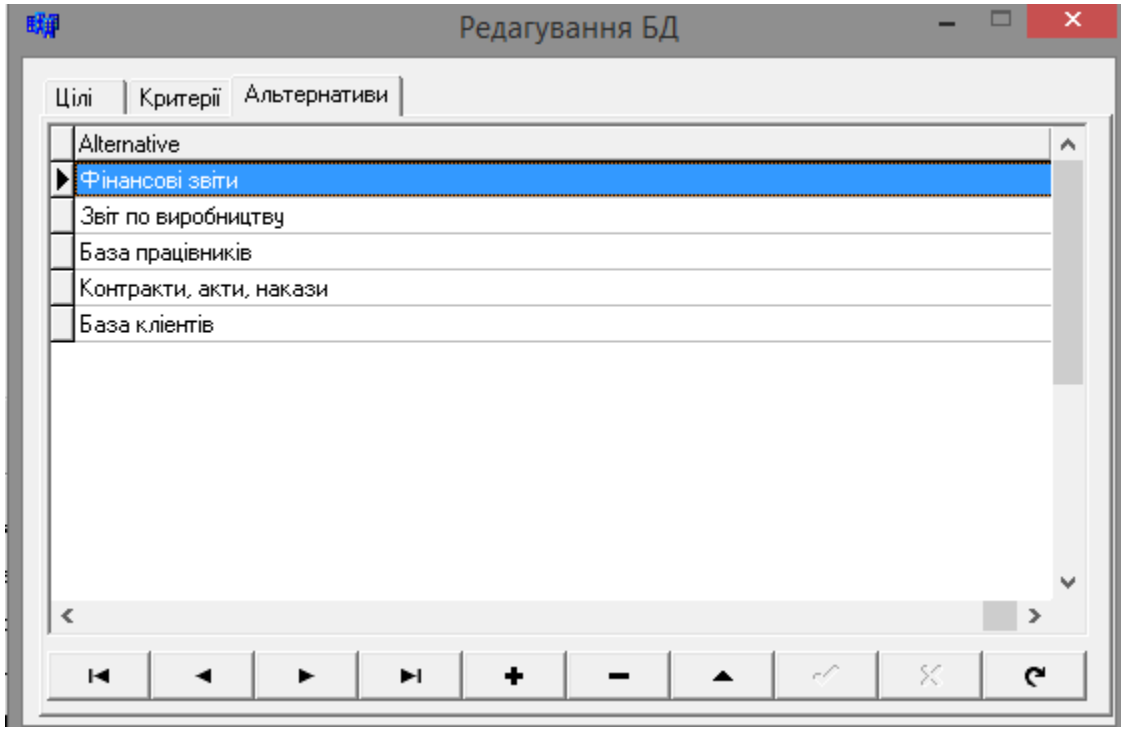
Працездатність програмного засобу



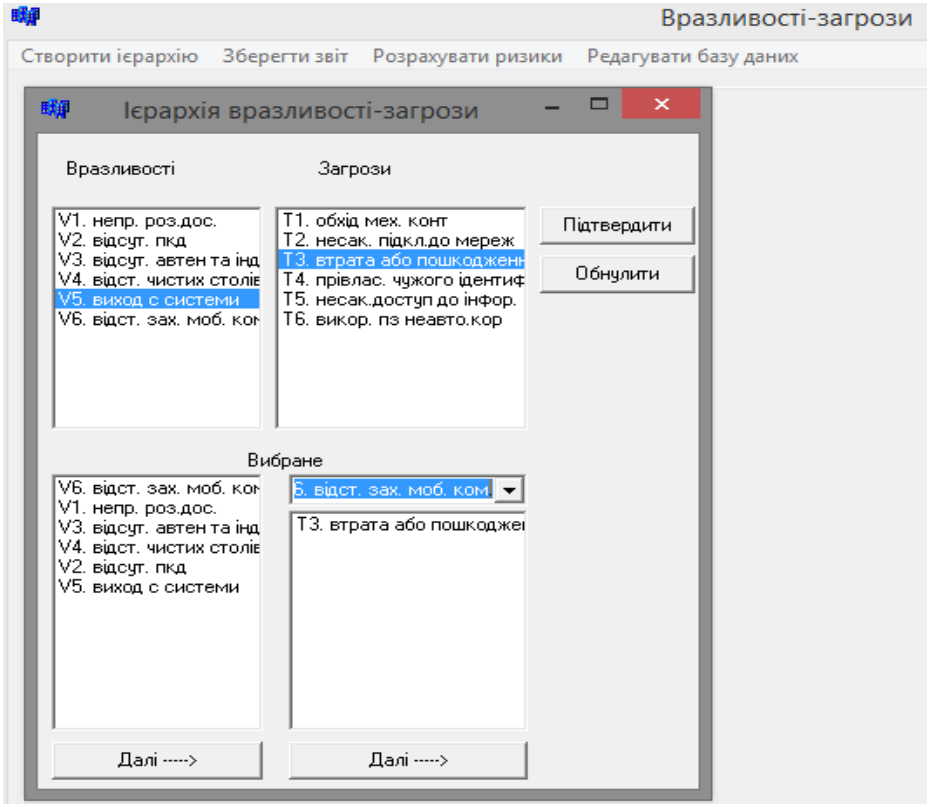
Екранна форма головного вікна програми



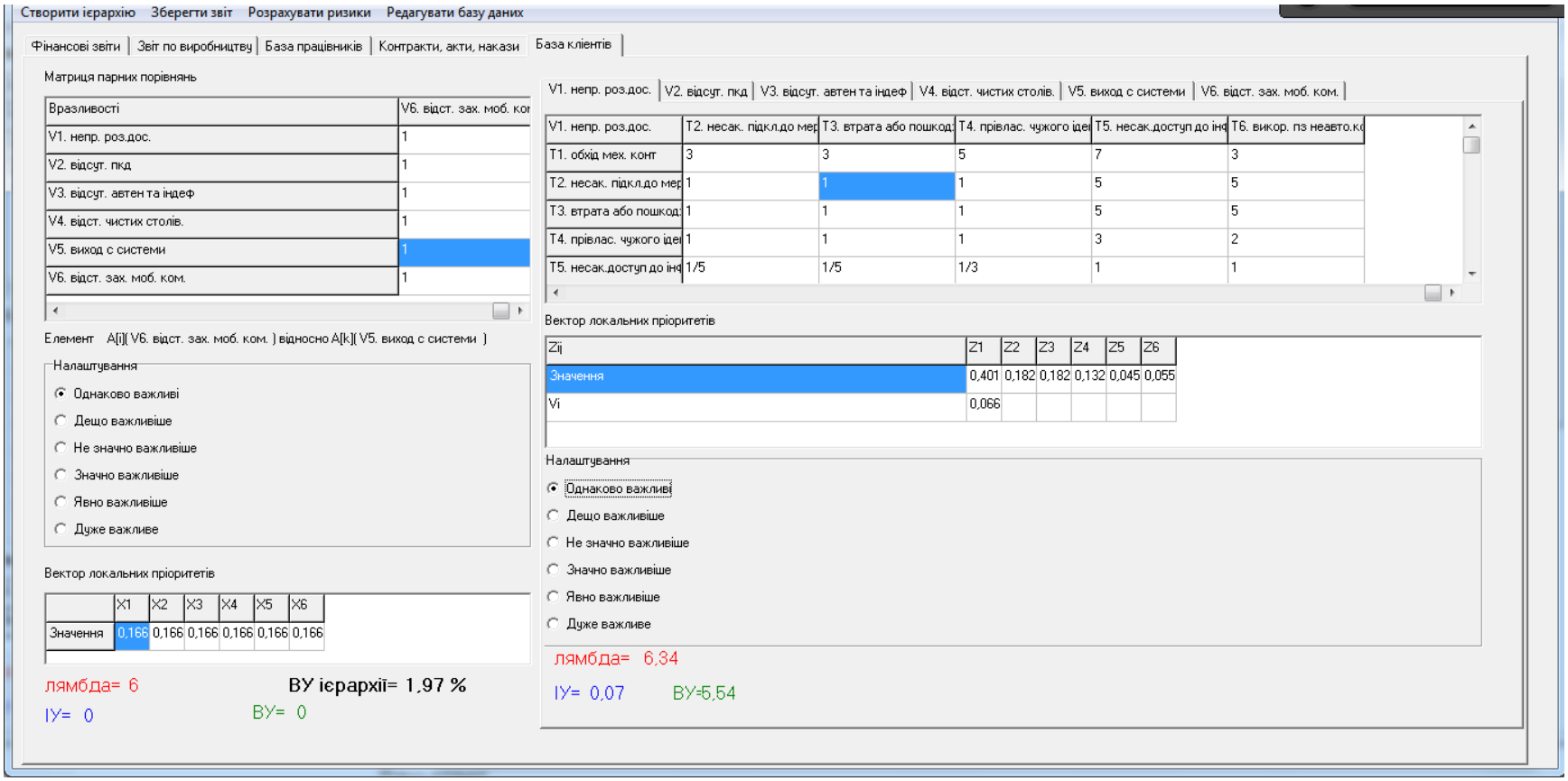
Зображення можливості редагування БД



Створення нової ієрархії



Обчислення даних загроз та вразливостей ієрархії



ВИСНОВКИ

Розроблений програмний продукт може застосовуватися для оцінки ризиків інформаційній безпеці організацій усіх сфер діяльності, так як він характеризує інформаційну систему з боку розрахунку оцінки ризиків інформаційної безпеки і відповідно може бути конкретизован під конкретну організацію.

Дякую за увагу