Вінницький національний технічний університет
Інститут інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Дипломний проект на тему:
“Програмний засіб для адаптивного керування системою захисту інформації підприємства”

Доповідач: ст. групи БС-11сп
Рибалкін І.М.
Керівник: ас. каф. ЗІ
Дмитришин О.В.

Мета і задачі дослідження

Актуальність дипломного проекту полягає в своєчасному оцінюванні рівня забезпечення цілісності, доступності та конфіденційності інформації на підприємстві і керуванні ризиками.

Метою дипломного проекту є підвищення рівня захищеності інформації в комп'ютерних системах шляхом керування ризиками.

Завданням дипломного проекту є*:*

- аналіз методів оцінювання рівня захисту інформаційних ресурсів;
- варіантний аналіз вибору методів оцінювання рівня безпеки підприємства;
- розробка програмного засобу для оцінювання рівня інформаційної безпеки підприємства;
- тестування розробленого програмного засобу.

Техніко-економічне обгрунтування

Таблиця 1 - Аналіз систем для оцінювання рівня захисту

Назва методу	Область застосування	Переваги	Недоліки
1	2	3	4
CRAMM	Застосовується для забезпечення інформаційної безпеки безперервності бізнесу.	1)може використовуватися на всіх стадіях проведення аудита безпеки інформаційних систем; 2)в основі ПЗ лежить об'ємна база знань по контрзаходам.	1) потрібен висококваліфікований аудит; 2) неможливо внести доповнення в базу знань.
Risk-Watch	Застосовується для орієнтації на точну кількісну оцінку співвідношення втрат від загроз безпеки і витрат на створення системи захисту	1) допомогає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту.	1) метод підходить, якщо потрібно провести аналіз ризиків на програмно-технічному рівні захисту, без урахування організаційних та адміністративних чинників; 2) програмне забезпечення Risk-Watch існує тільки англійською мовою.
COBRA	Застосовується для найпростішого варіанту оцінювання інформаційних ризиків будь-якої компанії.	1) використовується автоматизований режим оцінювання ризиків; 2) до складу входять інструменти для проведення огляду безпеки розроблені експертними системами.	1) метод не враховує комплексний підхід до інформаційної безпеки.

Основні загрози і вразливості

ЗАГРОЗИ:

- загрози конфіденційності (несанкціонованого одержання) інформації всіма потенційними і можливими каналами її витоку особливо каналами побічних електромагнітних випромінювань і наводок, таємними каналами зв'язку в імпортному обладнанні та розвідувальними закладними пристроями;
- загрози цілісності (несанкціонованої зміни) інформації;

загрози доступності інформації (несанкціонованого або випадкового обмеження) та ресурсів самої інформаційної системи;

- загрози спостереження роботи інформаційних систем (порушення процедур ідентифікації і автентифікації та процедур контролю доступу і дій користувачів.

ВРАЗЛИВОСТІ:

1. Легкість спостереження за каналами та перехоплення інформації;
2. Відсутність політики безпеки;
3. Складність конфігурування засобів захисту;
4. Помилки при конфігуруванні хоста або ресурсів управління доступом;
5. Роль та важливість адміністрування системи;
6. Слабка автентифікація.
7. Можливість легкого спостереження за даними, що передаються;
8. Можливість легкого маскування під інших користувачів;
9. Слабкий захист на рівні хостів.

Вибір схеми оцінювання рівня ІБ та методу оцінки стійкості системи захисту

В результаті виконання дипломного проекту був проведений огляд трьох схем оцінювання рівня ІБ:

-Простої;
-Поліноміальної;
-Пуассонівської.

Базовою моделю обрана проста схема оцінювання, оскільки вона є основою для побудови інших ймовірнісних моделей, зокрема і тих, котрі широко використовуються у дослідженні переліку загроз інформаційної безпеки.

Методи оцінки стійкості системи захисту:

- метод «чорної шухляди»;
- метод «білої шухляди».

Обрано метод «чорної шухляди» він припускає відсутність у тестуючої сторони яких-небудь спеціальних знань про конфігурацію і внутрішню структуру об'єкта. При цьому проти об'єкта реалізуються усі відомі типи атак і перевіряється стійкість системи захисту у відношенні цих атак.

Вибір схеми оцінювання рівня ІБ та методу оцінки стійкості системи захисту

Визначення ризику, пов’язаного з порушенням цілісності, для і-того інформаційного ресурсу, визначатимемо так:

$$\widetilde{R}_{цi} = \widetilde{P}^{ц}_{ami} \sum_{j=1}^{p_i} C_{ij},$$

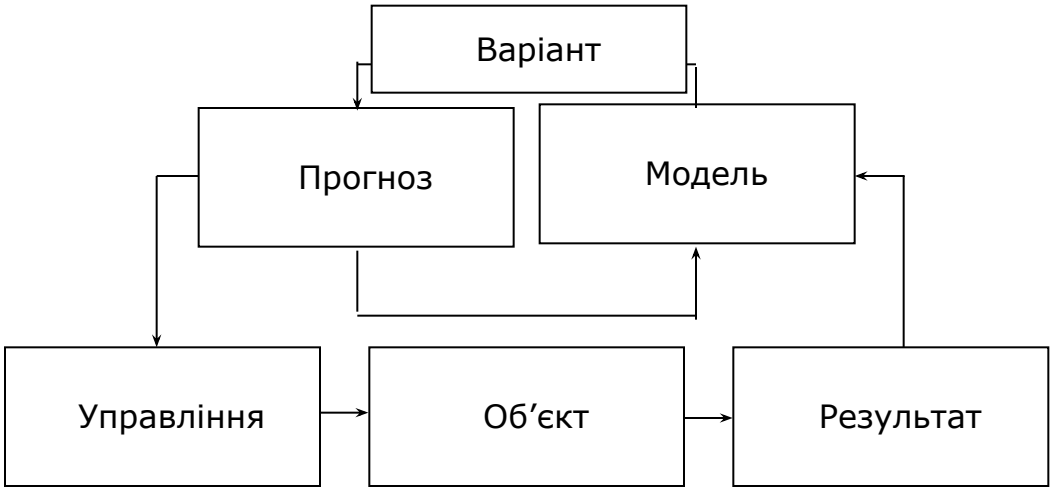
Аналогічним чином формалізуємо ризик, пов'язаний з порушенням доступності для і-того інформаційного ресурсу:

$$\widetilde{R}_{дi} = \widetilde{P}^{д}_{ami} \cdot \sum_{j=1}^{k_i} w_{ij},$$

Для визначення ризику, пов’язаного з порушенням конфіденційності, для і-того інформаційного ресурсу, використаємо запропонований підхід:

$$\widetilde{R}_{кi} = \widetilde{P}^{к}_{ami} \sum_{j=1}^{S_i} C^{/}_{ij}.$$

Структура адаптивного управління системою захисту підприємства



Адаптивне управління системою захисту полягає в зміні параметрів і структури системи залежно від змін внутрішніх і зовнішніх умов діяльності підприємства.

Модель процесу оцінювання рівня інформаційної безпеки підприємства

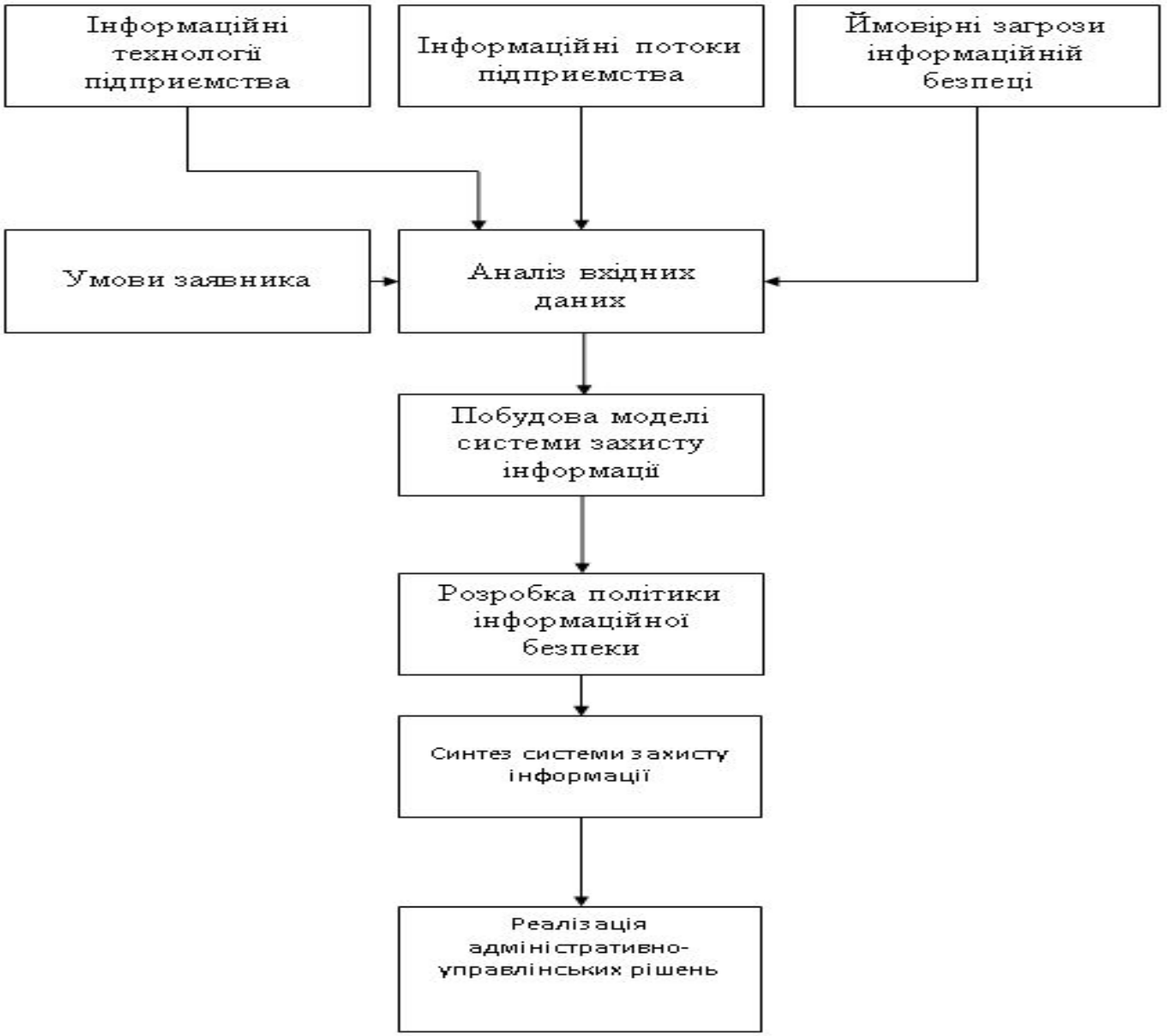


Схема роботи програмного засобу

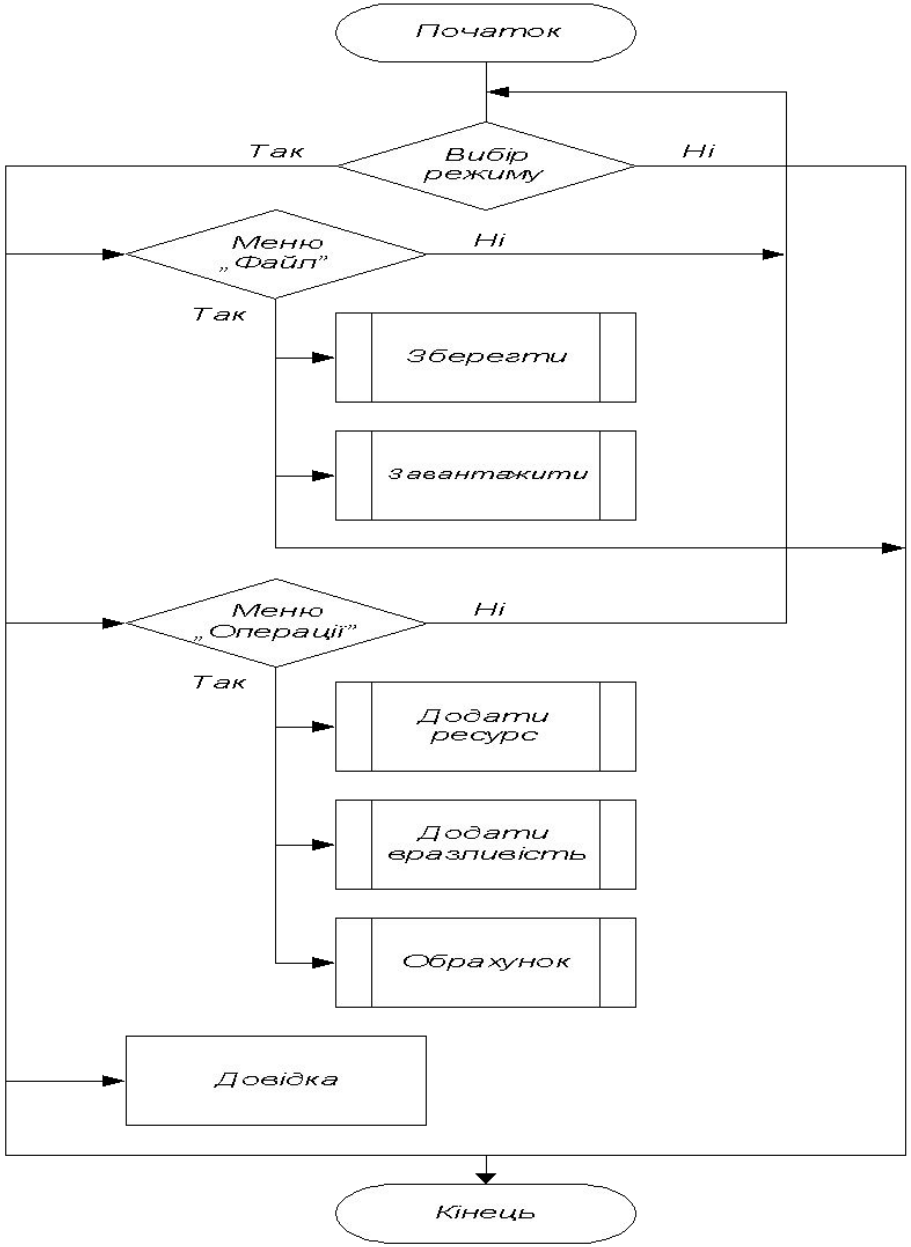
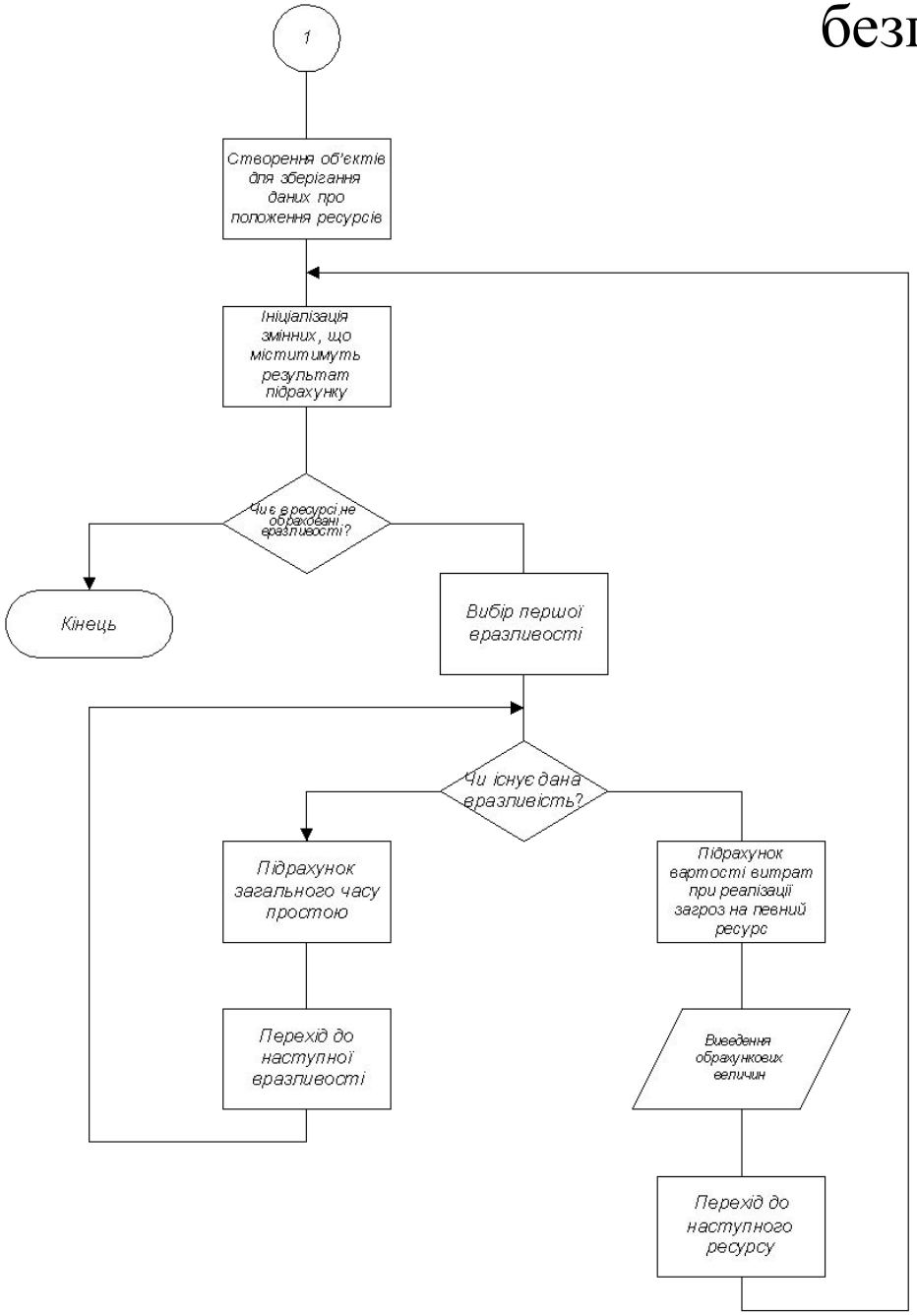
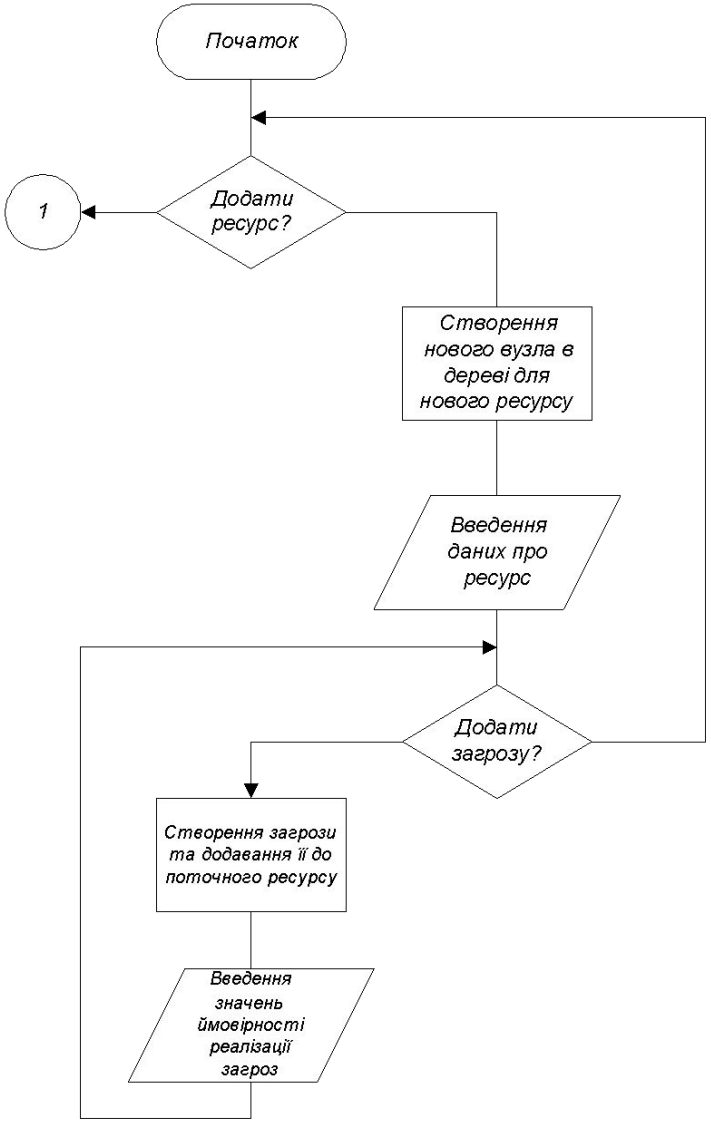


Схема роботи програми обчислення рівня інформаційної безпеки





Фрагменти інтерфейсу

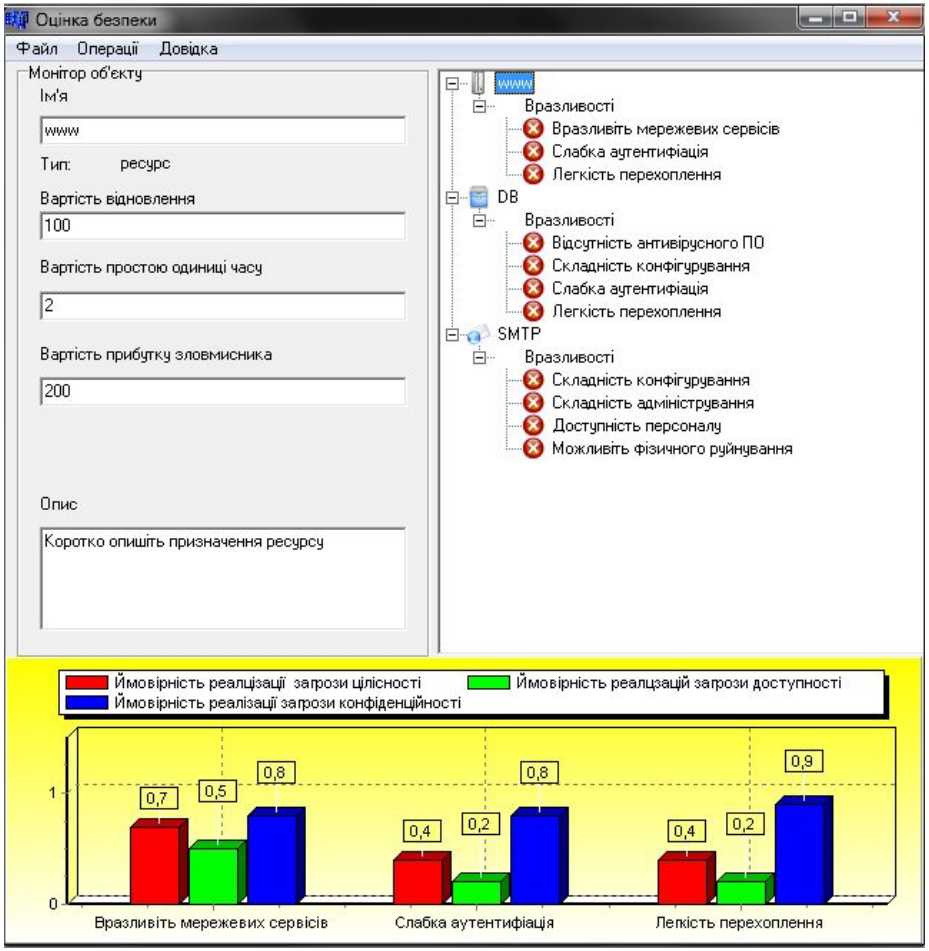


Рисунок 1 – Вигляд головного вікна програми та обрахування вразливостей

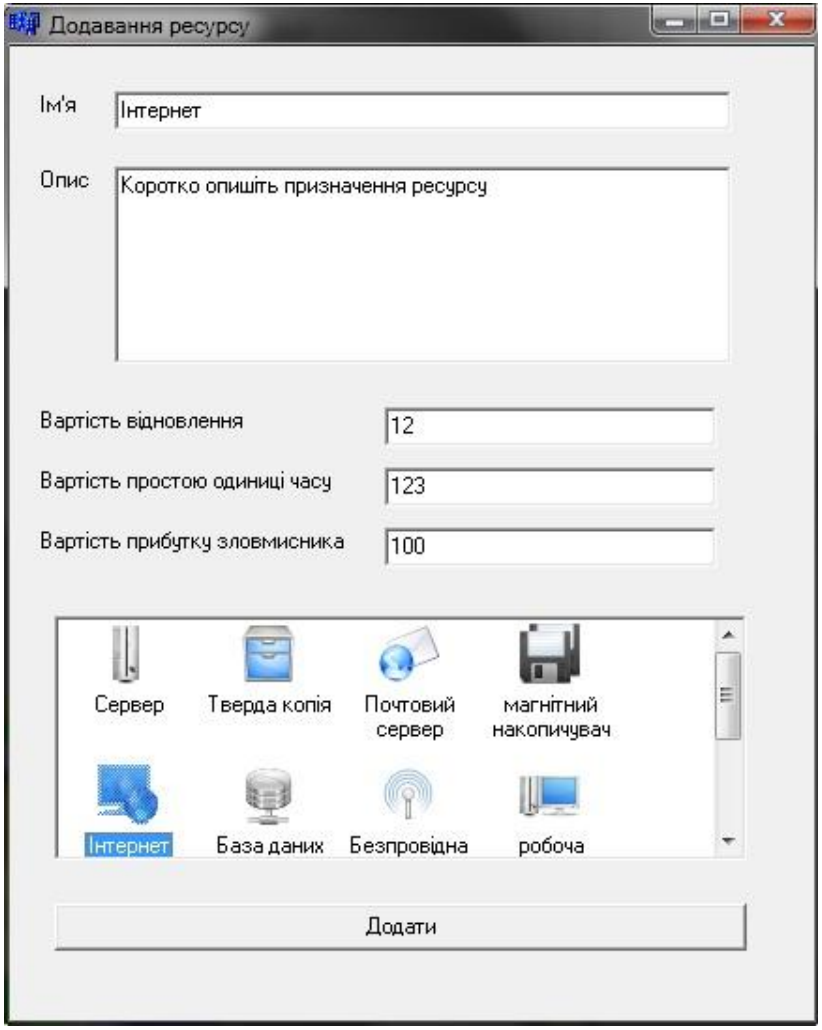


Рисунок 2 – Вигляд вікна додавання ресурсу

Фрагменти інтерфейсу

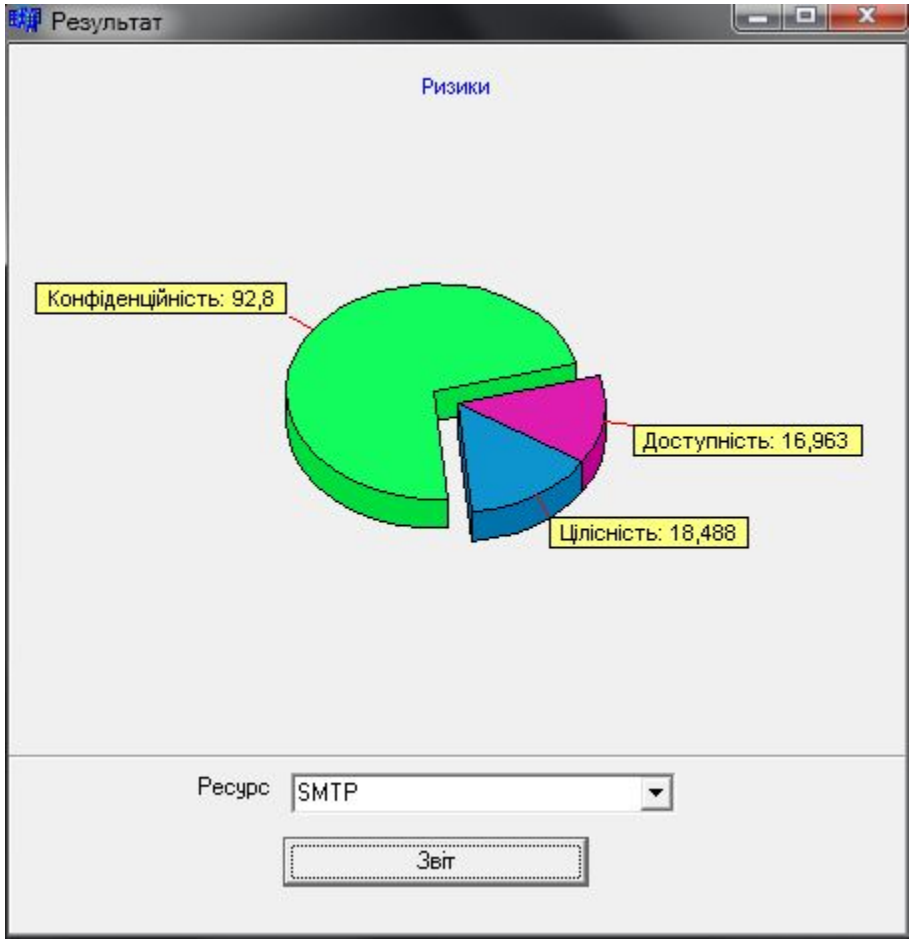


Рисунок 3 – Результат розрахунку ризику для поштового протоколу SMTP

Економічна частина

Ціна продукту – 2910 грн

Термін окупності - 0,77 років

Прибуток – 19071,14 грн

Р[illegible] 24684,78 [illegible]

Охорона праці

п/п	Фактори виробничого середовища і трудового процесу	Нормативне значення	Фактичне значення
1	Шум (дБА екв.)	50	70
2	Ультразвук, кГц:	20	20
3	Мікроклімат у приміщенні:		
	- температура повітря, °С	22-25	20-30
	- швидкість руху повітря, м/с	0,1	0,1
	- відносна вологість повітря, %	40-60	40-60
4	Робоча поза:	Вільна	Вільна
	-перебування в нахиленому положенні до 30 ^{0}	25	25
	-дрібні стереотипні рухи кистей і пальців рук	До 20 000	До 20 000
	- нахили тулуба, разів	до 100	до 100
	- переміщення в просторі, км (переходи, обумовлені технологічним процесом)	До 1 км за зміну	До 1 км за зміну

Висновки

В ході виконання дипломного проекту було створено програмний засіб для адаптивного керування системою захисту інформації. Виконана розробка відповідає завданню на дипломний проект.

Було проведене дослідження існуючих програмних продуктів для визначення можливих аналогів, та здійснено техніко-економічне обґрунтування доцільності розробки нового програмного продукту.

Проаналізовані основні методи оцінювання ризиків та встановлено, що вони не враховують можливість оцінювання рівня захищеності інформації підприємства в залежності від змін ймовірностей здійснення загроз. Проте підхід на основі адаптивного оцінювання захищеності інформації дозволяє ефективно керувати системою захисту інформації підприємства.

На основі математичної моделі оцінювання рівня захисту підприємства розроблено програмний засіб, що дозволяє виконувати адаптивне керування системою захисту підприємства. Для виявлення помилок і забезпечення стабільної роботи програмного засобу проведено тестування програмного додатку. В результаті роботи розроблено програмний засіб, в якому реалізовано оцінювання рівня інформаційної безпеки підприємства.

Визначено економічні витрати на розробку нового продукту, в том числі на виготовлення одного примірника продукції. Здійснено аналіз ринку та встановлено можливий рівень попиту на нову розробку. Визначено собівартість та номінальну вартість одного примірника програмного продукту. Розраховано приблизний термін окупності розробки програмного продукту.

Визначено норми гігієни праці програміста. Розроблено основні вимоги до організації робочого місця розробника програми. Визначені параметри мікроклімату. Розглянуті інженерно-технічні заходи захисту працівників та комплексних систем від дії вражаючих факторів в надзвичайних ситуаціях.

Дана розробка призначена для оцінювання рівня інформаційної безпеки підприємства та адаптивного керування його системи захисту