

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ
ІНФОРМАЦІЇ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ
ІНФОРМАЦІЇ

ДИПЛОМНА РОБОТА

на тему

«Програмний комплекс оцінювання наслідків витоку службової
інформації у сфері оборони»

Виконав: студент БІ-443 Петренко С. А.

Керівник: Заріцький О.В.

Київ-2019

Постановка задачі

- Мета роботи - програмна реалізація для оцінки наслідків витоку службової інформації у сфері оборони
- Об'єкт дослідження - службова інформація у сфері оборони
- Предмет дослідження - методи та алгоритми створення програмного забезпечення для реалізації оцінки наслідків витоку службової інформації у сфері оборони
- Методи - використання різних мов програмування для реалізації оцінки ризиків витоку інформації

Постановка задачі

Виходячи з мети, завданням даної дипломної роботи є:

- провести аналіз методів захисту службової інформації, їх переваги та недоліки
- обґрунтувати вибір та дослідити метод програмної реалізації оцінення шкоди національній безпеці у разі витоку службової інформації.
- створення блок-схеми алгоритму.
- програмна реалізація методу оцінення шкоди національній безпеці у разі витоку службової інформації.
- експеримент програмної реалізації витоку службової інформації у сфері оборони.

Новизна

Вперше запропонована програмна реалізація, що має інтуїтивно зрозумілий інтерфейс, в якому реалізована оцінка витоку службової інформації у сфері оборони, а також є можливість вибору варіантів протидії витоку і запобігання його у майбутньому.

Практична цінність

Програмний комплекс може використовуватись у реальних практичних системах захисту інформації, за допомогою даного програмного продукту можлива оцінка витоку інформації і протидія цьому витоку у майбутньому.

Вперше розроблена програма, яка може використовуватись у сфері оборони, як практичний захист від витоку інформації у сфері оборони.

Актуальність

- Наша країна знаходиться у стані війни, тому питання оцінки витоку службової інформації у сфері оборони – стоїть дуже гостро.
- Виходячи з цього можна вважати, що тема створення програми для реалізації оцінки наслідків витоку інформації є дуже важлива в даний період часу.

Службова інформація

До службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Порівняльний аналіз методів оцінки наслідків витоку службової інформації

- Метод аналізу і оцінки величини можливої шкоди національній безпеці у сфері охорони службової інформації
- Метод нечіткої класифікації відомостей, що становлять службову інформацію за встановленими критеріями
- Метод оцінювання важливості відомостей за визначеними сферами службової інформації

Алгоритм роботи програми



Рис.1.1. Блок-схема алгоритму роботи

Блок 1 – введення початкових даних експертної оцінки (СРСД, порушення (події), відомостей, що оцінюються (стаття ЗВДТ та її СС));

Блок 2 – визначення об'єкту ($O_{N,i,j}$) відомостей, його «питома вага» (Q), ідентифікація СЧО (ВВСЧО (k));

Блок 3 – формування та визначення «ваги» переліку X відомостей, що становлять ДТ, які забезпечують функціонування об'єкту $O_{N,i,j}$ і наявні в РСО СРСД;

Блок 4 – розрахунок ефективності функціонування СОДТ ($K^{СОДТ}$) та рівня зниження функціонування СЧО (ρ);

Блок 5 – розрахунок прогнозованої (бальної) величини можливої ЕШ ($W_{ек}$) та ІТН ($W_{ін}$), його опис та категорія тяжкості для національної безпеки;

Блок 6 – введення дати засекречування відомостей за рішенням ДЕТ та дати інформування про виникнення щодо них подій Р або В зі звіту про стан забезпечення ОДТ в РСО СРСД;

Блок 7 – визначення кількості років зберігання та охорони цих відомостей (T_{ϕ});

Алгоритм роботи

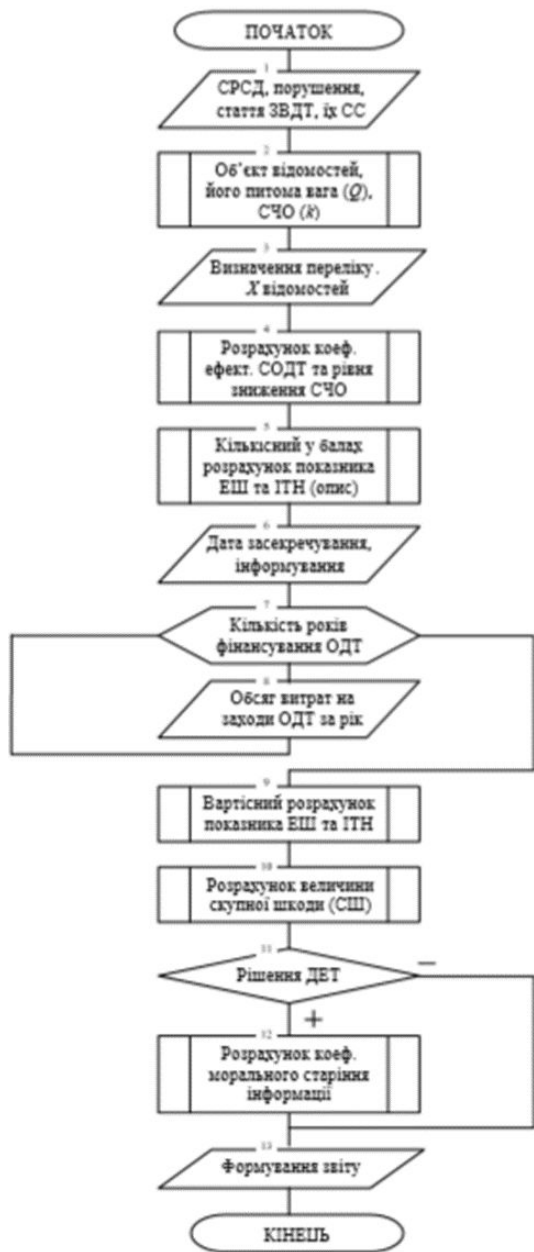


Рис.1.1. Блок-схема алгоритму роботи

Блок 8 – введення фінансової бухгалтерської звітності щодо величини витрат на забезпечення заходів ОДТ за кожен визначений рік у блоці 7;

Блок 9 – вартісний розрахунок величини ЕШ ($C_{W_{ек}}$) та шкоди від ІТН ($C_{W_{ін}}$) національній безпеці України у разі витоку ДТ;

Блок 10 – розрахунок СШ (C_W) національній безпеці України у разі витоку ДТ;

Блок 11 – прийняття рішення ДЕТ щодо застосування коефіцієнту морального старіння (K_c) інформації у зв'язку з необхідністю розсекречування цих відомостей або втрати їх актуальності чи важливості;

Блок 12 – розрахунок коефіцієнту морального старіння (K_c);

Блок 13 – автоматизоване формування звіту з результатами та відомостями експертного оцінювання. Важливою властивістю розробленого алгоритму є масовість, або можливість застосування до різних вхідних даних. Необхідною умовою, яка задовольняє алгоритм, є детермінованість, або визначеність.

Програмна реалізація

Система АОШ національній безпеці держави у сфері ОДТ

Ідентифікація порушення/відомостей, що становлять ДТ

Назва установи

Стаття ЗВДТ Гриф П. Кваліфікація порушення

Зміст відомостей: Сфера: --

Кількісний розрахунок показника ЕШ та ІТН (в балах)

Шкода за ступенем секретності ()

Показник ЕШ

Показник ІТН

Категорія тяжкості: -- Пункт

Опис ІТН

Об'єкт відомостей

Номер об'єкта Допустиме значення

Питома вага об'єкта --

Коефіцієнт СЧО --

Опис об'єкта

Дата засекречення № рішення

Дата інформування № рішення

Строк дії рішення --

Фактичний термін зберігання --

Можливий коефіцієнт старіння --

Перелік відомостей, що забезпечують об'єкт ДТ

Стаття	Гриф	Стаття	Гриф	Коефіцієнт ефективності СОДТ
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	0

Рівень зниження ефективності СЧО

Зміст відомостей:

Вартісний розрахунок показника ЕШ та ІТН

Фінансування заходів на ОДТ за 1 рік тис. грн.

Коефіцієнт захищеності відомостей --

Загальні витрати (до порушення) --

Обґрунтовані витрати (після порушення) --

Розмір економічної шкоди (ЕШ) --

Розмір шкоди від ІТН --

Розрахунок величини СШ

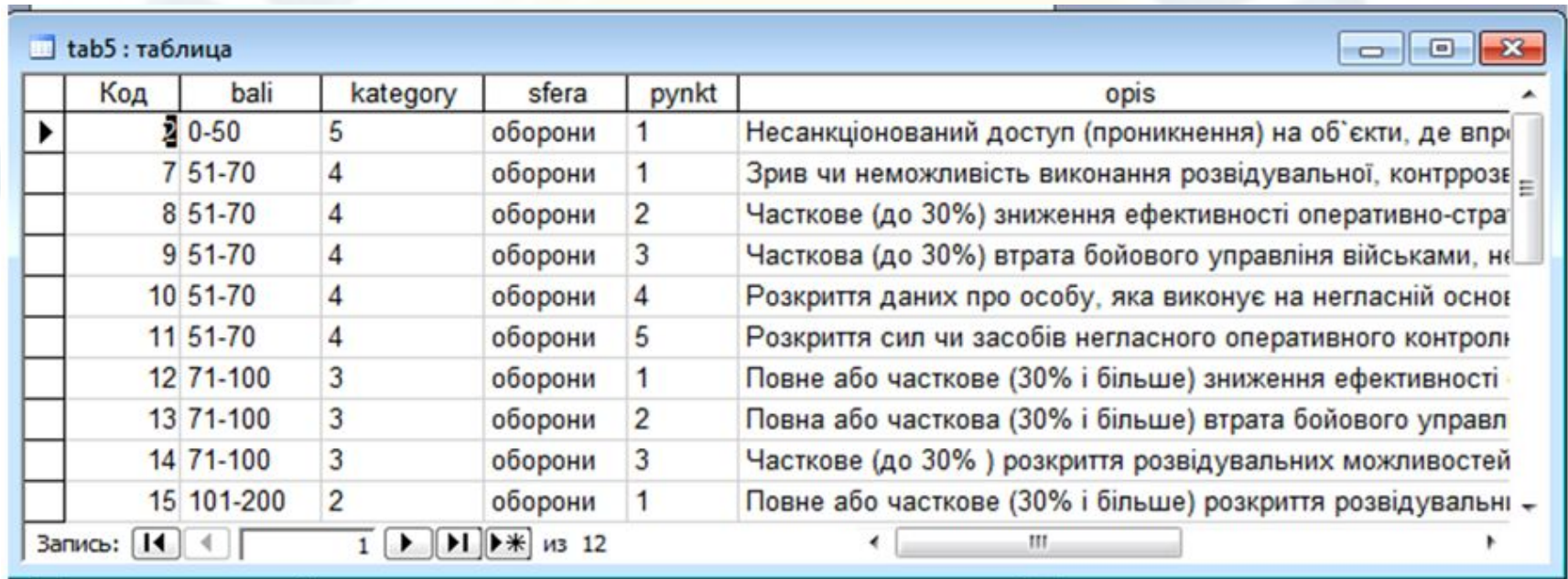
Дозвіл ДЕСПТ на розрахунок коефіцієнта старіння відомостей

Дата № рішення

Сукупна шкода: --

Рис.1.2. Інтерфейс програми

Приклад роботи створеної програми




Код	bali	category	sfera	punkt	opis
2	0-50	5	оборони	1	Несанкціонований доступ (проникнення) на об'єкти, де впр
7	51-70	4	оборони	1	Зрив чи неможливість виконання розвідувальної, контррозв
8	51-70	4	оборони	2	Часткове (до 30%) зниження ефективності оперативно-стра
9	51-70	4	оборони	3	Часткова (до 30%) втрата бойового управління військами, не
10	51-70	4	оборони	4	Розкриття даних про особу, яка виконує на негласній основ
11	51-70	4	оборони	5	Розкриття сил чи засобів негласного оперативного контролю
12	71-100	3	оборони	1	Повне або часткове (30% і більше) зниження ефективності
13	71-100	3	оборони	2	Повна або часткова (30% і більше) втрата бойового управл
14	71-100	3	оборони	3	Часткове (до 30%) розкриття розвідувальних можливостей
15	101-200	2	оборони	1	Повне або часткове (30% і більше) розкриття розвідувальні

Рис.1.3. Інтерфейс програми

ВИСНОВОК

- ✓ проведено аналіз методів захисту службової інформації, їх переваги та недоліки
- ✓ обгрунтовано вибір та досліджено метод програмної реалізації оцінення шкоди національній безпеці у разі витоку службової інформації.
- ✓ створено програмна реалізація методу оцінення шкоди національній безпеці у разі витоку службової інформації.
- ✓ зроблений експеримент програмної реалізації витоку службової інформації у сфері оборони.



**Доповідь
закінчено**

**Дякую за
увагу**