Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи

Магістр
(освітній ступінь)

на тему: **Методи та засоби оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень**

Виконав: студент 6 курсу, групи СІм-62
спеціальності
123 «Комп'ютерна інженерія»
(шифр і назва спеціальності (напряму підготовки))
(підпис) Оксенюк В.Ю.
(прізвище та ініціали)

Керівник (підпис) Баран І.О.
(прізвище та ініціали)

Нормоконтроль (підпис) Тиш Є.В.
(прізвище та ініціали)

Рецензент (підпис) Гащин Н.Б.
(прізвище та ініціали)

м. Тернопіль – 2019

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет Комп'ютерно-інформаційних систем і програмної інженерії
Кафедра Комп'ютерних систем та мереж
Освітній ступінь магістр
Напрям підготовки 123 комп'ютерна інженерія
(шифр і назва)
Спеціальність 123 комп'ютерна інженерія
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри [illegible] Осухівська Г.М.
«30» 08 2018 р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Оксенюк Віталій Юрійович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Методи та засоби оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень

Керівник проекту (роботи) Баран Ігор Олегович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «27» 04 2018 року № [illegible]

2. Термін подання студентом проекту (роботи) 27.12.2018

3. Вихідні дані до проекту (роботи) Результати огляду методів та засобів оцінювання загроз і ризиків, результати досліджень ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень. Алгоритм для розв'язання задачі оцінки ризиків ІБ

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1) Аналіз предметної області дослідження. 2) Теоретичні дослідження. 3) Практичне застосування оцінювання загроз та ризиків для організації інформаційної безпеки. 4) Обґрунтування економічної ефективності. 5) Охорона праці та безпека в надзвичайних ситуаціях. 6) Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Методи та засоби оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень. Актуальність теми дослідження. Класифікація загроз для мобільних пристроїв. Огляд існуючих програмних продуктів, що реалізують функції оцінки ризиків та загроз ІБ. [illegible] ризиків [illegible] оцінки загроз та ризиків. [illegible] алгоритму оцінювання [illegible], що [illegible] основі [illegible]. Висновки

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Обґрунтування економічн. ефективн.	к.е.н., доц. Ткачій О.Б.	Ткачій	Ткачій
Безпека в НС	Стрічок В.С. ст.викл. каф. ОХ	Стрічок	Стрічок
Екологія	Ніс А.Р. доц. каф. ОХ		
Охорона праці	Осухова Г.М.	21.11	21.11

7. Дата видачі завдання 30.09.2019

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1.	Вступ, предмет та об'єкт дослідження	4.10.19	
2.	Теоретичні дослідження	20.10.19	
3.	Практичне дослідження організації праці	6.11.19	
	та розробка дій організації праці		
	працівників		
4.	Обґрунтування економічної ефективності	9.11.19	
5.	Охорона праці та безпека в надзвичайних	16.11.19	
	ситуаціях		
6.	Висновки	23.11.19	
7.	Попередній захист дипломної роботи	27.11.19	
8.	Захист дипломної роботи	23.12.19	

Студент _____ Оксенюк В.Ю.
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ Бурлі Н.О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи та засоби оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень // Дипломна робота за освітнім ступенем “Магістр”// Оксенюк Віталій Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно–інформаційних систем і програмної інженерії, кафедра комп’ютерних систем та мереж, група СІм–62 // Тернопіль, 2019 // с. – , рис. – *32*, табл. – *7*, аркушів А1 – *10* , бібліогр. – *35*.

Ключові слова: АНАЛІЗ РИЗИКІВ, ВРАЗЛИВІСТЬ, ЗАГРОЗА, ЗАХИСТ ІНФОРМАЦІЇ, МОБІЛЬНЕ БІЗНЕС-РІШЕННЯ, ОЦІНКА РИЗИКІВ, РИЗИК

Дипломна робота присвячена дослідженню методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень.

У першому розділі сформульовано та описано вирішувану проблему. Проаналізовано основані загрози та вразливості для мобільних пристроїв. Їх виявлення та усунення дозволить зменшити економічні втрати підприємства. Проведено докладний аналіз окремих існуючих програмних продуктів (ГРИФ, RiskWatch, CRAMM), що реалізують функції оцінки ризиків та загроз інформаційної безпеки. Визначено їх переваги та недоліки.

В другому розділі проведено теоретичний аналіз методів та підходів до оцінювання загроз та ризиків для організації інформаційної безпеки підприємства. Описано чотири види методів для кількісної оцінки ризику (статистичні, ймовірнісно-статистичні, теоретико-ймовірнісні, експертні). Для розв’язання задачі кількісної оцінки ризиків основна увага приділена ймовірнісно-статистичним та експертним методам. Запропоновано підхід до оцінки загроз та ризиків та сформульована математична модель задачі для оцінки загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень.

В третьому розділі запропоновано програмну реалізацію підходу до оцінки ризиків та загроз інформаційної безпеки. Розроблено і описано алгоритм для проведення поетапної оцінки загроз та ризиків. Описано архітектуру програмного

продукту, представлено діаграму класів розробленого продукту. Докладно описано основні сутності бази даних. Програмний засіб для оцінювання загроз та ризиків створено на платформі .NET у MS Visual Studio 2010 на мові C#. Результати проведеного порівняльного тестування розробки та програмного комплексу ГРИФ дозволяють стверджувати про можливість використання розробленого продукту для проведення практичного дослідження.

У четвертому розділі обґрунтовано економічну доцільність дослідження методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень шляхом розрахунку показників економічної ефективності, що дало змогу протягом приблизно двох років компенсувати витрати на використання запропонованих технічних рішень.

В п’ятому розділі описані важливі питання охорони праці, вплив радіації на працездатність населення та планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації.

Шостий розділ присвячений питанням статистики екології об’єктів природного середовища та методологічним основам обробки екологічної інформації на базі комп’ютерних технологій.

ABSTRACT

Methods and tools of threats and risks assessment for information security provide at mobile business use // Master thesis // Okseniuk Vitalii // Ternopil Ivan Puluj national technical university, Department of Computer Information Systems and Software Engineering, Department of Computer Systems and Networks Group SIm-62 // Ternopil, 2019 // p.- , fig. – *32*, table. – *7*, Sheets A1 - *10* , Ref. – *35*.

Keywords: INFORMATION SECURITY, MOBILE BUSINESS SOLUTION, RISK RISK ANALYSIS, RISK ASSESSMENT, SYSTEM VULNERABILITY, THREAT

The diploma thesis deals with the research of methods and means of threat and risk assessment for organization of information security when using mobile business decisions.

The first section formulates and describes the problem solved. Basic threats and vulnerabilities for mobile devices are analyzed. Their identification and elimination will reduce the economic losses of the enterprise. A detailed analysis of selected existing software products (GRIF, RiskWatch, CRAMM) that implements information security and risk assessment functions has been carried out. Their advantages and disadvantages are identified.

The second section provides a theoretical analysis of methods and approaches to assessing threats and risks to the organization of information security of the enterprise. Four types of methods for quantitative risk assessment are described (statistical, probabilistic, theoretical, probabilistic, expert). To address the problem of quantitative risk assessment, the focus is on probabilistic statistical and expert methods. An approach to threat and risk assessment is proposed and a mathematical model of the task for threat and risk assessment for the organization of IB when using mobile business decisions is formulated.

Section 3 proposes a programmatic implementation of an approach to assessing information security risks and threats. An algorithm for gradual assessment of threats and risks has been developed and described. The architecture of the software is described, and a class diagram of the developed product is presented. The basic essence

of the database is described in detail. The threat and risk assessment software was created using the .NET platform in MS Visual Studio 2010 in C #. The results of the comparative testing of the GRIF development and software complex allow us to confirm the possibility of using the developed product for practical research.

The fourth section substantiates the economic feasibility of investigating threat and risk assessment methods and tools for the organization of information security when using mobile business decisions by calculating cost-effectiveness indicators, which made it possible to offset the costs of using the proposed technical solutions for approximately two years.

The fifth section describes important safety issues, the impact of radiation on the performance of the population, and the planning of civil protection measures at the facility in the event of an emergency.

The sixth section is devoted to the environmental statistics of environmental objects and the methodological bases of computer-based environmental information processing.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

CLR – Common Language Runtime;

GUI – Graphical user interface;

HCI – Human-Computer Interaction;

IEEE – Institute of Electrical and Electronics Engineers;

ISO – International Organization for Standardization;

ІБ – Інформаційна безпека;

ІС – Інформаційна система

ІТ – Інформаційні технології;

ПП – Програмний продукт;

ПС – Програмне середовище.

ПЗ – Програмне забезпечення

ВСТУП

Актуальність теми. На сучасному етапі розвитку інформаційних технологій грамотна організація інформаційної безпеки будь-якої компанії стає критично важливим стратегічним чинником її розвитку. Основна увага повинна приділятися вимогам і рекомендаціям відповідної нормативно-методичної бази в галузі захисту інформації. Разом з тим багато провідних компаній сьогодні використовують деякі додаткові ініціативи, спрямовані на забезпечення стійкості і стабільності функціонування корпоративних інформаційних систем для підтримки безперервності бізнесу в цілому.

Однією з таких ініціатив є використання мобільних пристроїв для ведення бізнесу. На даний час мобільні пристрої стали поширеним засобом доступу до інформації, додатків та ведення бізнесу, в той же час створюючи нові можливості загроз.

Незважаючи на постійно зростаючий ризик ІБ, підприємства все частіше переходять на використання мобільних пристроїв. Варто зазначити, що пов'язаний з мобільними пристроями ризик ІБ збільшується за рахунок їх зростаючої популярності, збільшення потужностей апаратної частини, функціональності операційних систем та додатків та особливої уваги до них з боку кіберзлочинців. Тому підвищення рівня захисту інформації, що циркулює в інформаційній системі підприємства з елементами мобільних технологій являє собою актуальну задачу.

Бізнес-процеси компаній поступово налаштовуються під все зростаючу мобільність співробітників. На сьогоднішній день виникла необхідність зробити рішення для забезпечення безпеки інтегрованою і невід'ємною частиною роботи з мобільними пристроями.

Зв’язок із науковими програмами, планами, темами. Магістерська робота виконана відповідно до наукової тематики Тернопільського національного технічного університету імені Івана Пулюя, кафедри комп’ютерних систем та мереж.

Мета роботи: підвищення рівня захисту інформації, що циркулює в інформаційній системі підприємства з використанням мобільних бізнес-рішень.

Об'єкт дослідження: процес налаштування системи захисту інформації підприємства.

Предмет дослідження: підходи та алгоритми оцінки загроз та ризиків інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень на підприємстві та в бізнесі.

В роботі поставлено та розв'язано **наступні задачі**:

– огляд існуючих методик та програмних продуктів оцінки ризиків,

– дослідження ризиків та загроз інформаційній безпеці при реалізації та використанні мобільних бізнес-рішень

– розробка додатку для розв'язання задачі оцінки ризиків на ПК за допомогою мови програмування C#, середовища розробки Visual Studio 2010 та СУБД MS SQL SERVER.

Наукова новизна отриманих результатів:

– побудовано модель оцінювання загроз та ризиків ІБ при реалізації мобільних бізнес-рішень;

– запропоновано підхід до оцінювання ризиків ІБ при реалізації та використанні бізнес-рішень;

– розроблено програмний засіб, який здатний вести список ресурсів, загроз, вразливостей, контрзаходів, користувачів системи та проводити оцінку ризиків для кожного ресурсу підприємства.

Методи дослідження: Метод теоретичного дослідження та експериментальний з використання персонального комп'ютера. Методологічну основу дослідження становлять фундаментальні положення комп'ютерної інженерії та комп'ютерних наук, наукові дослідження вітчизняних і зарубіжних компаній та вчених у сфері комп'ютеризованих систем.

Практичне значення одержаних результатів. Розроблений програмний продукт може застосовуватися для оцінки ризиків ІБ організацій усіх сфер діяльності, так як він характеризує ІС з боку ризиків і відповідно може бути конкретизована під конкретну організацію.

Публікації. Окремі результати дослідження доповідалися на VII науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (11-12 грудня 2019 р.) у вигляді тез:

1. Оксенюк В.Ю. Використання програмних засобів для оцінки та управління ризиками інформаційної безпеки. Інформаційні моделі, системи та технології: Праці VII наук.-техн. конф. (Тернопіль, 11-12 грудня 2019 р.) Тернопіль, 2019. С. 75.

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається з вступу, 6 розділів, висновків, списку використаної літератури та додатків. Обсяг роботи: пояснювальна записка – арк. формату А4, графічна частина – 10 аркушів формату А1.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕННЯ

1.1. Опис вирішуваної проблеми та формулювання задачі

На даний час мобільні пристрої стали поширеним засобом доступу до інформації, додатків та ведення бізнесу, в той же час створюючи нові можливості загроз.

Незважаючи на постійно зростаючий ризик ІБ, підприємства все частіше переходять на використання мобільних пристроїв. Варто зазначити, що пов'язаний з мобільними пристроями ризик ІБ збільшується за рахунок їх зростаючої популярності, збільшення потужностей апаратної частини, функціональності операційних систем та додатків та особливої уваги до них з боку кіберзлочинців.

Виникають нові напрямки мобільного кіберзлочинності, нові можливості для зловживання і неправомірного використання мобільних пристроїв і даних.

1.2. Аналіз загроз для мобільних пристроїв

На сьогоднішній день виникла необхідність зробити рішення для забезпечення безпеки інтегрованою і невід'ємною частиною роботи з мобільними пристроями [4].

До головних загроз для мобільних пристроїв можна віднести:

– атаки через Web-додатки та мережі. Як правило, запускаються шкідливими або скомпрометованими сайтами, а також використовують уразливості браузерів пристроїв. Такі мережі намагаються встановити зловмисне ПЗ або вкрасти конфіденційні дані, що проходять через браузер;

– шкідливе ПЗ. Аналоги класичних вірусів і троянських програм для мобільних пристроїв. Але на відміну від традиційних комп'ютерних вірусів, мобільні віруси використовують інші канали розповсюдження. Вони можуть

проникати на мобільні пристрої за допомогою MMS-повідомлення та змінних карт пам'яті, через Bluetooth з'єднання з іншого телефону, через інфрачервоне з'єднання, USB, WiFi, з персонального комп'ютера, через WEB-або WAP-сайти;

– атаки з використанням соціальної інженерії. Іншими словами, фішинг або прицільні атаки – являють собою психологічні прийоми з метою обману користувачів. Вони змушують користувача розкрити секретну інформацію або встановити зловмисне ПЗ;

– захоплення IT-ресурсів. Спроби використання мережі, пристрою та облікових даних користувача у зловмисних цілях – наприклад, розсилання спаму з інфікованих пристроїв, а також використання захоплених пристроїв для проведення атак "відмова в обслуговуванні";

– втрата даних. Раніше загроза втрати даних застосовувалася тільки для стандартних мобільних телефонів, але з розвитком мобільних пристроїв атаки зазнали смартфони і планшетні комп'ютери. Такі атаки можуть бути як навмисними, так і випадковими. Вони як і раніше залишаються найбільшою загрозою для мобільних пристроїв. В ході такої операції зловмисник викрадає секретну інформацію з пристрою або з мережі;

– загрози цілісності даних. Мета такого шахрайства – порушити роботу організації або отримати фінансову вигоду. Полягає в спробах зловмисників змінити або пошкодити персональні дані власника мобільного пристрою. Цілісність можна поділити на статичну (розуміється як незмінність інформаційних об'єктів) і динамічну (що відноситься до коректного виконання складних дій (транзакцій));

– загроза «відмова в обслуговуванні». Оскільки ресурси мобільних пристроїв сильно обмежені, на відміну від стандартного ПК, смартфони є більш вразливими до атак відмови в обслуговуванні. Мобільні оператори теж знаходяться в зоні ризику. Заражені вірусами телефони, які керуються зловмисниками віддалено, можуть використовуватися для атак «відмови в обслуговуванні» на мережі стільникових операторів, перевантажуючи їх;

– порушення зв'язку внаслідок впливу природних або штучних ненавмисних перешкод, виходу з ладу апаратури зв'язку, перевантаження мережі та ін. причин;

– навмисне порушення зв'язку, обумовлене застосуванням методів радіоелектронної протидії, викликають, блокування (глушіння) мобільних пристроїв;

– контроль місцезнаходження абонента;

– порушення безпеки мобільних транзакцій (m-транзакцій);

Класифікація загроз для мобільних пристроїв наведена на рис 1.1.

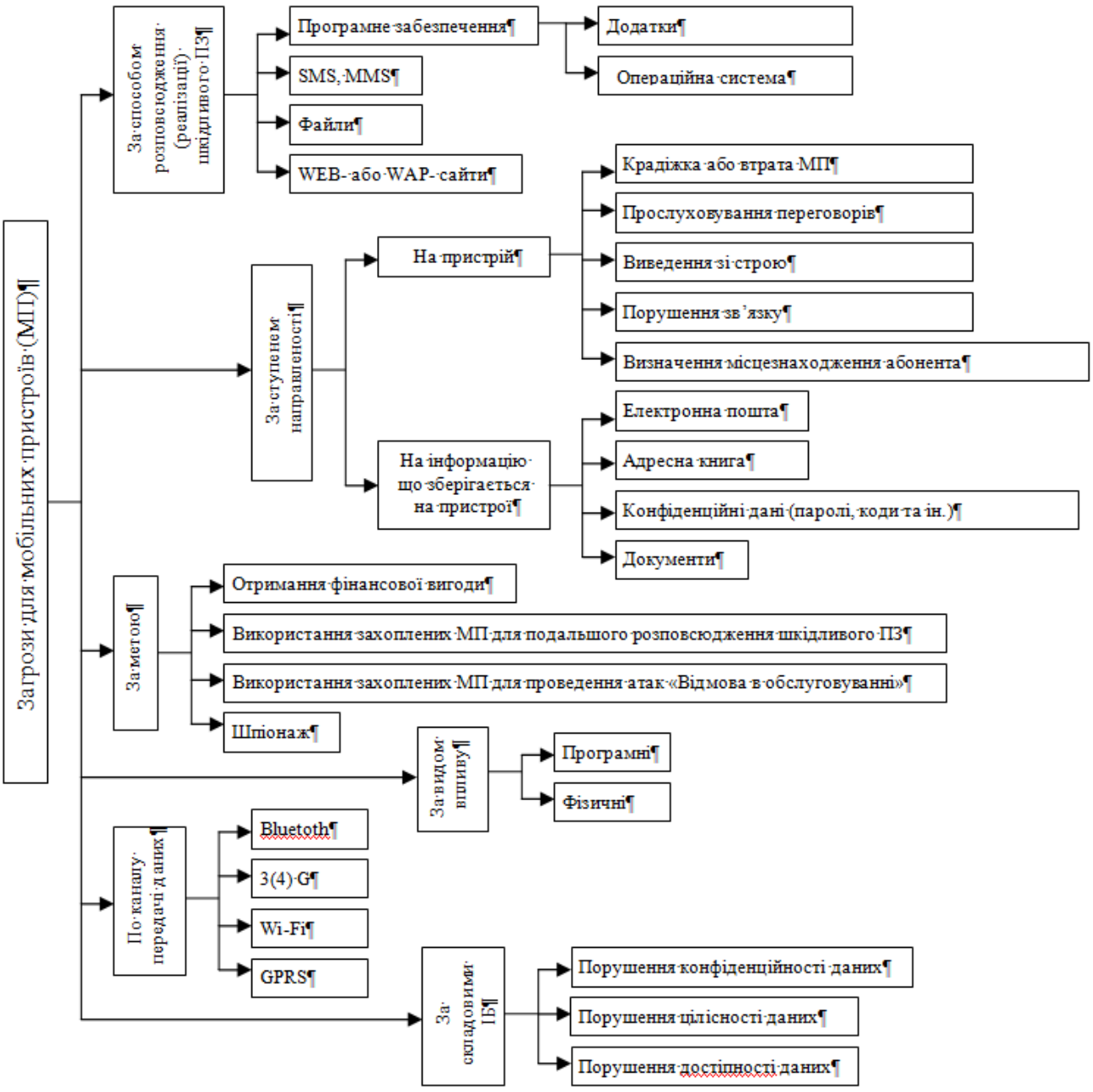


Рис 1.1. Класифікація загроз для мобільних пристроїв

Аналіз загроз показав, що основною загрозою для мобільних пристроїв є шкідливе ПЗ. Дослідження, проведене лабораторією G Data SecurityLabs, показує, що на початку 2018 року доля вірусів для смартфонів і планшетних комп'ютерів збільшилася на 140% у співвідношенні з загальною кількістю шкідливого ПЗ [1].

Також експерти відзначають особливу активність з боку крос-платформенних троянських програм, які на даний момент домінують на фоні інших загроз. Більшість з них були створені для розповсюдження спаму та іншої нелегальної діяльності, яку ведуть електронні шахраї. Збільшення частки подібних злочинів лише показує, що нелегальний ринок шкідливих програм знаходиться у своєму зеніті [5].

У першій половині 2018 року фахівці G Data SecurityLabs зареєстрували черговий рекорд: появу 1245403 нових сімейств шкідливих програм. Це на 15,7% більше в порівнянні з другою половиною 2017 року. Експерти прогнозують подальше продовження зростання. До кінця року G Data Software очікує появу як мінімум 3,5 мільйонів нових сімейств вірусів, і це буде становити кількість вірусів, рівне числу зареєстрованих з 2012 по 2016 рік.

Троянські програми як і раніше будуть домінувати, як окрема категорія. Зростання їх числа свідчить про те, що справи у кіберзлочинців йдуть більш ніж успішно, тому що ця група шкідливого ПЗ допомагає здійснювати більшість кримінальних послуг, серед яких атаки з перевантаження цілих систем. Також буде помітне зростання рекламного шкідливого ПЗ. Кількість атак, здійснених через незакриті уразливості і при попутному завантаженні, збільшилося лише на частки відсотків.

Існує серйозна небезпека отримання мобільного вірусу через онлайн-магазини додатків App Store: шкідливе ПЗ поширюється переважно з завантаженими додатками. Особливу небезпеку це набуває у світі того, що переважна більшість власників мобільних пристроїв сьогодні не користуються мобільним антивірусом для сканування на наявність заражених програм.

Крім того, все частіше починає зустрічатися загроза атаки через існуючі бездротові мережі: мобільні пристрої все більше сприйнятливі до таких атак, – існують мобільні додатки, використовуючи які зловмисник легко отримує доступ

до електронної пошти та соціальних мереж «жертви». Основними наслідками цієї загрози є перехоплення даних через GPRS, 3G або WI-FI мережі. На мобільний пристрій може надійти повідомлення з настройками мережі, зберігши й активувавши яке, користувач змінить точки доступу, куди і піде необхідний (через проміжний сервер) шахраям трафік.

Тепер розглянемо більш детально інші загрози для мобільних пристроїв. Поточна схема монетизації більшості мобільних троянських програм на даний час пов'язана з відправкою SMS-повідомлень на короткі номери. У результаті або з рахунку користувача списуються гроші, або власника телефону без його згоди підписують на платний сервіс. У другому випадку, більш поширеному в Азіатському регіоні, користувачеві з сервісу приходить SMS-повідомлення з інформацією про підписку. Щоб власник мобільного пристрою не запідозрив недобре, троянські програми видаляють повідомлення про платну підписку, як тільки воно приходить. Таким чином, троянські програми можуть функціонувати на одному пристрої дуже довго – і приносити своєму власнику постійний дохід.

За даними Juniper GTC, 17% всіх пристроїв були вражені SMS троянськими програмами [6].

Незважаючи на всі прийоми кіберзлочинців, як і раніше більш серйозну небезпеку становить крадіжка або втрата самих пристроїв – за статистикою, з цим зустрічається кожен 20-й абонент. В результаті виникає необхідність в командах геолокації, блокування або знищення даних, що зберігаються на таких пристроях. Крім того, близько 20% підлітків допускають відправку з мобільного пристрою конфіденційних або персональних даних.

Один з аспектів безпеки мобільних пристроїв пов'язаний з розвитком мобільних платежів. Експерти відзначають, що смартфони і комунікатори, корінним чином змінили ставлення до можливостей стільникового телефону. Тепер смартфонами користуються не тільки бізнесмени, але і звичайні користувачі, яким зручніше купувати цифровий контент або контролювати стан банківського рахунку прямо з мобільного пристрою.

Одним з найпоширеніших видів атаки став також фішинг з використанням URL-адрес, схожих на адреси веб-сайтів податкових служб, подарункових

ваучерів, преміальних програм та облікових записів в соціальних мережах. Згідно з дослідженням компанія McAfee Labs було встановлено, що серед 100 перших результатів пошуку по найпопулярніших щоденних запитам 51 відсоток посилався на шкідливі сайти, і на кожній з таких сторінок з викривленими результатами пошуку містилося в середньому понад п'ять шкідливих посилань [7-8].

У жовтні 2018 р. на замовлення компанії Juniper агентствами KRC Research і Synovate було проведено міжнародне дослідження, в ході якого було опитано 6000 власників смартфонів і планшетних комп'ютерів в 16 країнах світу. Дослідження показало, що понад 76% споживачів використовують мобільні пристрої для доступу до секретних бізнес-ресурсам або важливої персональної інформації, у тому числі: 51% вводять або змінюють паролі, 43% перевіряють банківські рахунки, 30% – комунальні платежі, 20% передають фінансову інформацію, наприклад, номери кредитних карт, 18% використовують мобільні пристрої для доступу інформації, що становить корпоративну таємницю роботодавця, 17% – до медичних даних, 16% – для передачі даних соціального страхування.

В даний час наявність систем управління ІБ є однією з ключових умов стратегічного розвитку будь-якої організації. Відповідно до стандарту ISO/IEC 27001:2005 [14] визначення вимог до розробки, впровадження, застосування, моніторингу, аналізу, підтримці та покращенню системи управління ІБ має здійснюватися в контексті менеджменту ризиків ІБ конкретної організації. Основним і найбільш складним етапом управління ризиками ІБ є аналіз ризиків.

1.3 Аналіз існуючих програмних продуктів, що реалізують функції оцінки ризиків та загроз ІБ

Для розв'язання задачі оцінки ризиків і загроз ІБ були обрані наступні програмні комплекси аналізу і контролю інформаційних ризиків: CRAMM (компанія Insight Consulting), RiskWatch (компанія RiskWatch) і ГРИФ (компанія Digital Security). Розглянемо далі дані методи та побудовані на їх базі програмні системи [17].

1.3.1 Огляд інтерфейсу та функціональності системи «ГРИФ». ГРИФ – комплексна система аналізу та управління ризиками ІС компанії. ГРИФ із складу Digital Security Office дає повну картину захищеності інформаційних ресурсів у системі і дозволяє вибрати оптимальну стратегію захисту інформації компанії [17,23]. Функціональність системи ГРИФ дозволяє: аналізувати рівень захищеності всіх цінних ресурсів компанії; оцінювати можливу шкоду, що понесе компанія в результаті реалізації загроз ІБ; ефективно управляти ризиками за допомогою вибору контрзаходів, найбільш оптимальних по співвідношенню ціна/якість. Система ГРИФ надає можливість проводити аналіз ризиків ІС за допомогою аналізу моделі інформаційних потоків, а також, аналізуючи модель загроз і вразливостей – залежно від того, якими вихідними даними своєму розпорядженні користувач, а також від того, які дані цікавлять користувача на виході. У даній роботі буде розглянута тільки модель загроз і вразливостей, так як вона є найбільш близьким аналогом програмному продукту, що розробляється. Робота з моделлю аналізу загроз і вразливостей передбачає визначення вразливостей кожного ресурсу з цінною інформацією, і підключення відповідних загроз, які можуть бути реалізовані через дані вразливості. У результаті виходить повна картина того, які слабкі місця є в ІС і той збиток, який може бути нанесений.

На першому етапі роботи з продуктом користувач вносить об'єкти своєї ІС: відділи, ресурси, загрози ІС , уразливості, через які реалізуються загрози (див. рис 1.2).

Рис 1.2. Головне вікно проекту програми ГРИФ

Система ГРИФ містить великі вбудовані каталоги загроз та вразливостей. Для досягнення максимальної повноти і універсальності даних каталогів, експертами Digital Security була розроблена спеціальна класифікація загроз, в якій реалізований багаторічний практичний досвід у галузі ІБ. Використовуючи каталоги загроз і вразливостей, користувач може вибрати загрози та вразливості, пов'язані з його ІС. Каталоги містять близько 100 загроз і 200 вразливостей (див. рис 1.3).

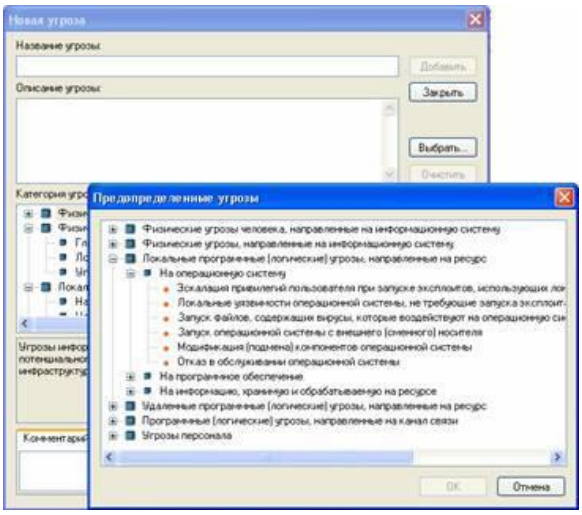


Рис 1.3. Форма для додавання нової загрози програми ГРИФ

Далі користувачеві необхідно проставити зв'язки, тобто визначити до яких відділів відносяться ресурси, які загрози діють на ресурс і через які вразливості вони реалізуються (див. рис 1.4).

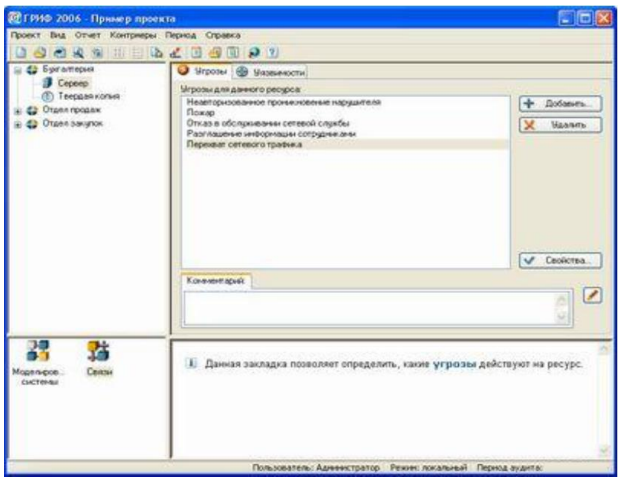
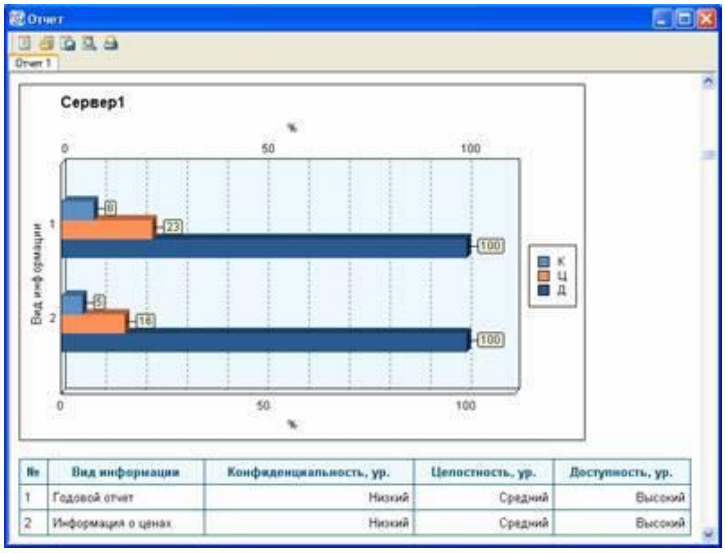


Рис 1.4. Форма для додавання зв’язків програми ГРИФ

Алгоритм системи ГРИФ аналізує побудовану модель і генерує звіт, який містить значення ризику для кожного ресурсу. Конфігурації звіту може бути практично будь-якою, таким чином це дозволяє користувачеві створювати як короткі звіти для керівництва, так і детальні звіти для подальшої роботи з результатами (рис 1.5).



№	Вид информации	Конфиденциальность, ур.	Целостность, ур.	Доступность, ур.
1	Годовой отчет	Низкий	Средний	Высокий
2	Информация о ценах	Низкий	Средний	Высокий

Рис 1.5. Звіт за значеннями ризиків для кожного ресурсу програми ГРИФ

Система ГРИФ містить модуль управління ризиками, який дозволяє проаналізувати всі причини того значення ризику, який утворюється після обробки алгоритмом занесених даних.

Таким чином, знаючи причини, користувач буде мати всі дані, необхідні для реалізації контрзаходів і, відповідно, зниження рівня ризику. Завдяки розрахунку ефективності кожного можливого контрзаходу, а також визначення значення залишкового ризику, користувач зможе вибрати найбільш оптимальні контрзаходи, які дозволять знизити ризик до необхідного рівня з найменшими витратами (див. рис 1.6).

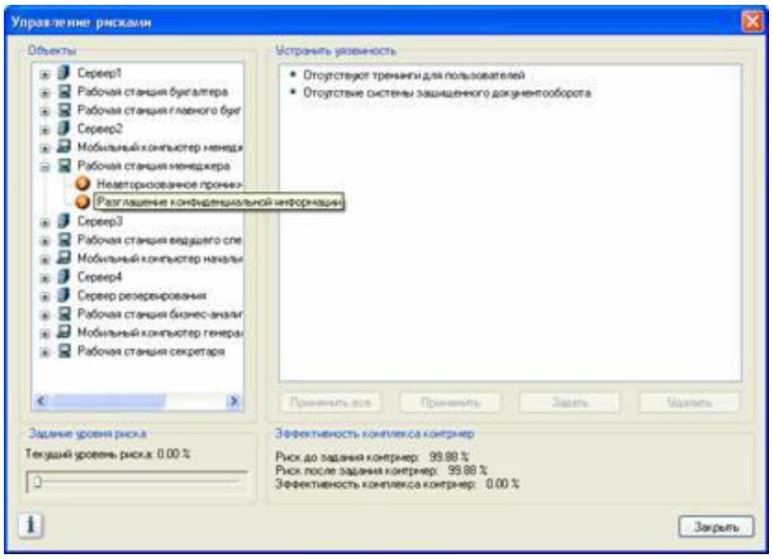


Рис 1.6. Форма для завдання контрзаходів програми ГРИФ

У результаті роботи з системою ГРИФ будується докладний звіт про рівень ризику кожного цінного ресурсу ІС компанії, всі причини ризику з докладним аналізом вразливостей і оцінкою економічної ефективності всіх можливих контрзаходів.

Недоліки системи ГРИФ:

– ГРИФ у набагато більшому ступені підходить для аудиту вже існуючих ІС, що знаходяться на стадії експлуатації, ніж чим для ІС, що знаходяться на стадії розробки;

– ГРИФ не дозволяє створювати власні шаблони звітів або модифікувати наявні;

– можливість внесення доповнень до бази знань ГРИФ не доступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретної організації.

1.3.2 Огляд інтерфейсу та функціональності системи «RiskWatch». ПЗ RiskWatch є потужним засобом аналізу та управління ризиками [18]. У методі RiskWatch в якості критеріїв для оцінки та управління ризиками використовуються прогнозування річних втрат (Annual Loss Expectancy, ALE) і оцінка повернення від інвестицій (Return on Investment, ROI) [17,22].

Сімейство програмних продуктів RiskWatch має масу переваг. RiskWatch

допомагає провести аналіз ризиків і зробити обгрунтований вибір заходів і засобів захисту. Програма RiskWatch більш орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки та витрат на створення системи захисту. Треба також зазначити, що в цьому продукті ризики у сфері інформаційної та фізичної безпеки комп'ютерної мережі підприємства розглядаються спільно.

В основі продукту RiskWatch знаходиться методика аналізу ризиків, яка складається з чотирьох етапів.

Перший етап – визначення предмета дослідження. Тут описуються такі параметри, як тип організації, склад досліджуваної системи, базові вимоги в галузі безпеки. Для полегшення роботи аналітика, в шаблонах, що відповідають типу організації ("комерційна ІС", "державна/військова ІС" і т.д.), є списки категорій захищуваних ресурсів, втрат, загроз, вразливостей і заходів захисту. З них треба вибрати ті, що реально присутні в організації (рис 1.7).

Рис 1.7. Вікно визначення категорії ресурсів, які захищаються

Другий етап – введення даних, що описують конкретні характеристики системи. Дані можуть вводитися вручну або імпортуватися із звітів, створених інструментальними засобами дослідження уразливості комп'ютерних мереж.

Функціональність цього етапу:

– докладний опис ресурсів, втрат і класів інцидентів, де класи інцидентів

виходять шляхом зіставлення категорії втрат і категорії ресурсів;

– для виявлення можливих вразливостей використовується опитувальник, база якого містить більше 600 питань. Питання пов'язані з категоріями ресурсів.

– задається частота виникнення кожної з виділених загроз, ступінь уразливості і цінність ресурсів. Все це використовується в подальшому для розрахунку ефекту від впровадження засобів захисту.

Третій етап – кількісна оцінка. На цьому етапі розраховується профіль ризиків, і вибираються заходи забезпечення безпеки. Спочатку встановлюються зв'язки між ресурсами, втратами, погрозами і вразливостями, виділеними на попередніх етапах дослідження (ризик описується сукупністю цих чотирьох параметрів).

Фактично, ризик оцінюється з допомогою математичного очікування втрат за рік. Загальновідома формула (m = p*v, де m – математичне сподівання, p – ймовірність виникнення загрози, v – вартість ресурсу) зазнала деяких змін, у зв'язку з тим, що RiskWatch використовує певні американським інститутом стандартів NIST оцінки, звані LAFE і SAFE (див. рис 1.8).

LAFE (Local Annual Frequency Estimate) – показує, скільки разів на рік у середньому ця загроза реалізується в даному місці (наприклад, в місті). SAFE (Standard Annual Frequency Estimate) – показує, скільки разів на рік у середньому ця загроза реалізується в цій "частини світу" (наприклад, в країні). Вводиться також поправочний коефіцієнт, який дозволяє врахувати, що в результаті реалізації загрози захищається ресурс може бути знищений не повністю, а тільки частково.

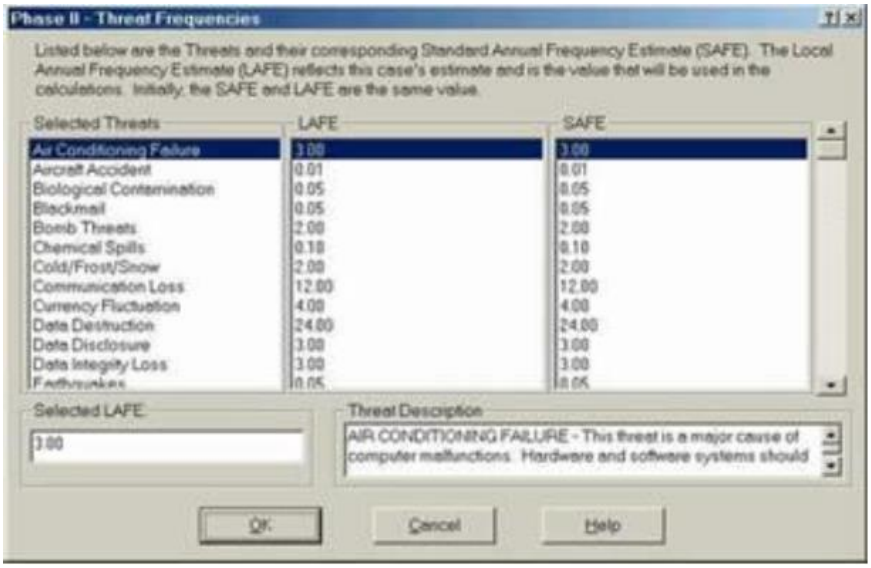


Рис 1.8. Вікно з оцінками LAFE и SAFE для однієї з загроз

Додатково розглядаються сценарії "що якщо:", які дозволяють описати аналогічні ситуації за умови впровадження засобів захисту. Порівнюючи очікувані втрати за умови впровадження захисних заходів і без них можна оцінити ефект від таких заходів.

RiskWatch включає в себе бази з оцінками LAFE і SAFE, а також з узагальненим описом різних типів засобів захисту.

Ефект від впровадження засобів захисту кількісно описується за допомогою показника ROI (Return on Investment – віддача від інвестицій), який показує віддачу від зроблених інвестицій за певний період часу (див. рис 1.9).

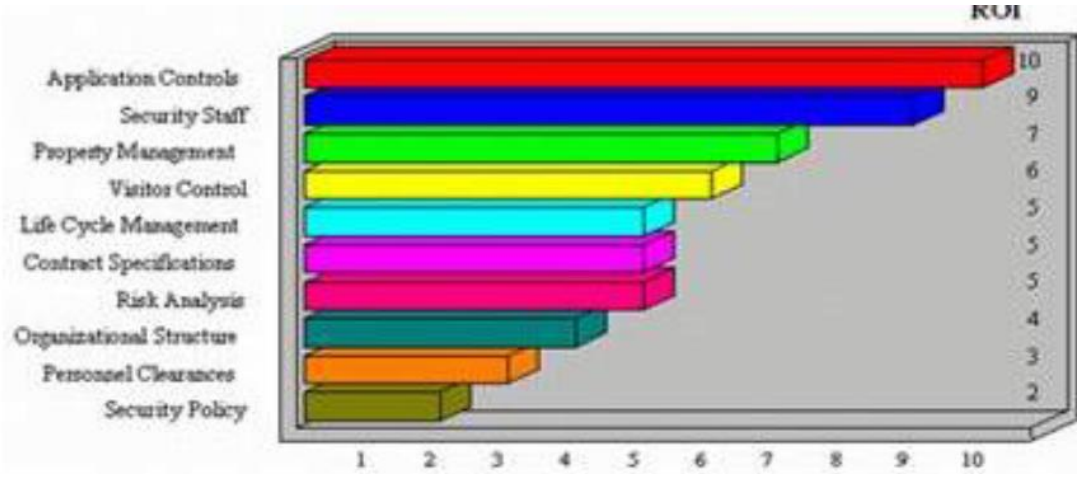


Рис 1.9. Звіт про показники ROI для різних мір захисту

Четвертий етап – генерація звітів. Типи звітів: короткі підсумки; повні і короткі звіти про елементи, описані на стадіях 1 та 2; звіт від вартості ресурсів захисту і очікуваних втрат від реалізації загроз; звіт про загрози та заходи протидії; звіт про ROI; звіт про результати аудиту безпеки.

Таким чином, розглянутий засіб дозволяє оцінити не тільки ті ризики, які зараз існують у підприємства, але й ту вигоду, яку може принести впровадження фізичних, технічних, програмних та інших засобів і механізмів захисту. Підготовлені звіти і графіки дають матеріал, достатній для прийняття рішень про зміну системи забезпечення безпеки підприємства.

Для вітчизняних користувачів проблема полягає в тому, що отримати використовувані в RiskWatch оцінки (такі як LAFE і SAFE) для наших умов досить проблематично. Хоча сама методологія може з успіхом застосовуватися.

Підводячи підсумок, можна відзначити, що конкретну методику проведення аналізу ризиків на підприємстві та інструментальні засоби, що підтримують її, потрібно вибирати, з огляду на наступні фактори:

– наявність експертів, здатних дати достовірні оцінки обсягу втрат від загроз ІБ;

– наявність на підприємстві достовірної статистки по інцидентам у сфері ІБ;

– чи потрібна точна кількісна оцінка наслідків реалізації загроз або достатньо оцінки на якісному рівні.

До недоліків RiskWatch можна віднести:

– такий метод підходить, якщо потрібно провести аналіз ризиків на програмно-технічному рівні захисту, без урахування організаційних та адміністративних чинників;

– отримані оцінки ризиків (математичне очікування втрат) далеко не вичерпує розуміння ризику з системних позицій – метод не враховує комплексний підхід до ІБ;

– ПЗ RiskWatch існує тільки англійською мовою;

– висока вартість ліцензії (від 10 000 доларів за одне робоче місце для невеликої компанії) [30].

1.3.3. Огляд інтерфейсу та функціональності системи «CRAMM». Метод CRAMM (CCTA Risk Analysis and Managment Method) був розроблений Агентством по комп'ютерам й телекомунікаціям Великобританії (Central Computer and Telecommunications Agency) за наказом Британського уряду і узятий на озброєння в якості державного стандарту. Він використовується, починаючи з 1985 р., урядовими та комерційними організаціями Великобританії. За цей час CRAMM придбав популярність у всьому світі. Фірма Insight Consulting Limited займається розробкою і супроводом однойменного програмного продукту, що реалізує метод CRAMM.

Метод CRAMM обраний нами для більш детального розгляду, і це не випадково. В даний час CRAMM – це досить потужний і універсальний інструмент, що дозволяє, крім аналізу ризиків, вирішувати також і ряд інших аудиторських завдань, включаючи [17,24]:

– проведення обстеження ІС і випуск супровідної документації на всіх етапах його проведення;

– проведення аудиту відповідно до вимог Британського уряду, а також стандарту BS 7799:1995 «Code of Practice for Information Security Management»;

– розробка політики безпеки і плану забезпечення безперервності бізнесу.

В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектора. Версії ПЗ CRAMM, орієнтовані на різні типи організацій, відрізняються одна від одної своїми базами знань (profiles). Для комерційних організацій є Комерційний профіль (Commercial Profile), для урядових організацій – Урядовий профіль (Government profile). Урядовий варіант профілю, також дозволяє проводити аудит на відповідність вимогам американського стандарту ITSEC («Помаранчева книга»).

Грамотне використання методу CRAMM дозволяє отримувати дуже хороші результати, найбільш важливим з яких, мабуть, є можливість економічного обґрунтування витрат організації на забезпечення ІБ та безперервності бізнесу. Економічно обґрунтована стратегія управління ризиками дозволяє, в кінцевому

підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

CRAMM передбачає поділ всієї процедури на три послідовних етапи. Завданням першого етапу є відповідь на питання: «Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції безпеки, або необхідно проведення більш детального аналізу?» На другому етапі проводиться ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується питання про вибір адекватних контрзаходів.

Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки і набір звітних документів.

На першій стадії дослідження проводиться ідентифікація та визначення цінності ресурсів що захищаються (див. рис 1.10).

Оцінка проводиться за десятибальною шкалою, причому критеріїв оцінки може бути кілька – фінансові втрати, втрати репутації і т.д. В описах CRAMM [50] як приклад наводиться така шкала оцінки за критерієм "Фінансові втрати, пов'язані з відновленням ресурсів": 2 бали – менше $ 1000; 6 балів – від $ 1000 до $ 10000; 8 балів – від $ 10 000 до $ 100 000; 10 балів – понад $ 100 000.

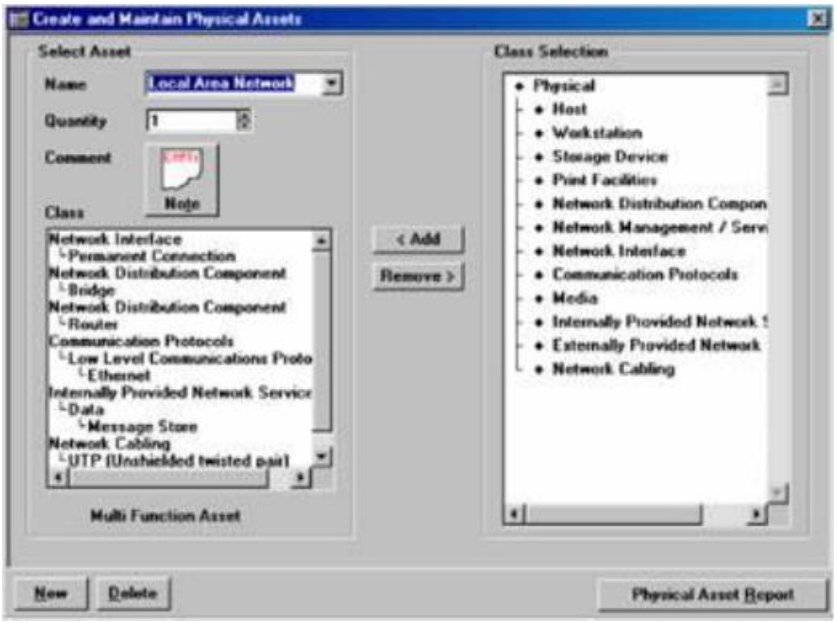


Рис 1.10. Вікно ідентифікація та визначення цінності ресурсів.

При низькій оцінці за всіма використовуваним критеріям (3 бали і нижче)

вважається, що розглянута система вимагає базового рівня захисту (для цього рівня не потрібно докладної оцінки загроз ІБ) і друга стадія дослідження пропускається.

На другій стадії ідентифікуються та оцінюються загрози в сфері ІБ, проводиться пошук та оцінка вразливостей системи що захищається. Рівень загроз оцінюється за наступною шкалою: дуже високий, високий, середній, низький, дуже низький. Рівень уразливості оцінюється як високий, середній або низький. На основі цієї інформації обчислюється оцінка рівня ризику за семибальною шкалою (див. рис 1.11).

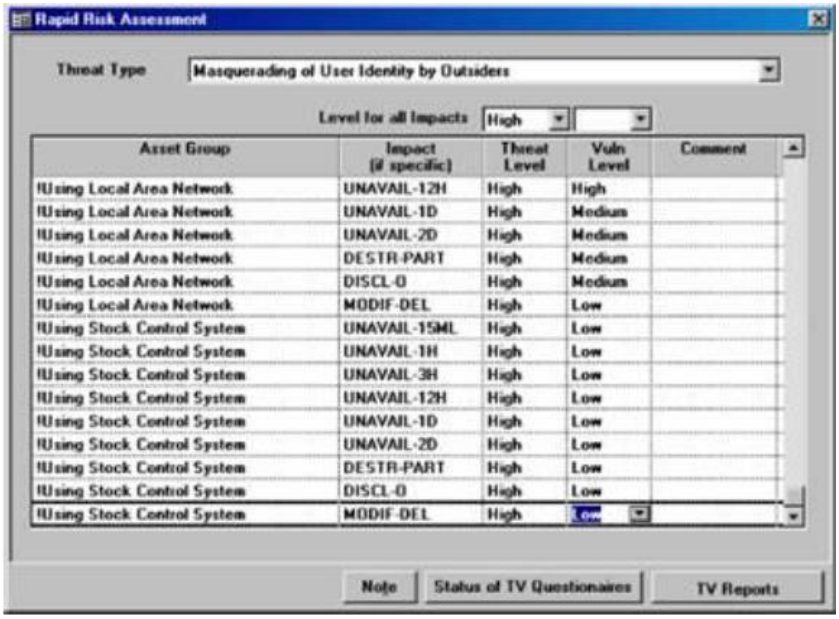


Рис 1.11. Вікно оцінки рівня ризику

На третій стадії CRAMM генерує варіанти заходів протидії виявленим ризикам. Продукт пропонує рекомендації наступних типів (див. рис 1.12): рекомендації загального характеру; конкретні рекомендації; приклади того, як можна організувати захист в даній ситуації.

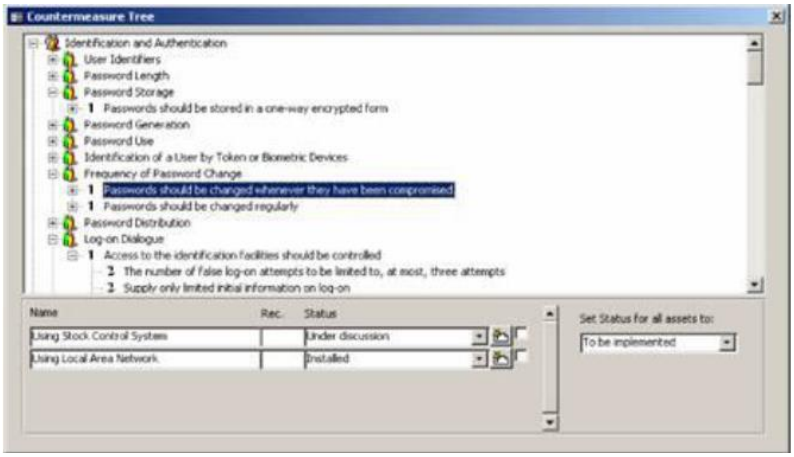


Рис 1.12. Вікно з рекомендованими контрзаходами

CRAMM має потужну базу, яка містить опис близько 1000 прикладів реалізації підсистем захисту різних комп'ютерних систем. Дані описи можна використовувати як шаблони. Рішення про впровадження в систему нових механізмів безпеки і модифікація старих приймає керівництво організації, враховуючи пов'язані з цим витрати, їх прийнятність та кінцеву вигоду для бізнесу. Завданням аудитора є обґрунтування рекомендованих контрзаходів для керівництва організації. У разі прийняття рішення про впровадження нових контрзаходів і модифікації старих, на аудитора може бути покладено завдання підготовки плану впровадження нових контрзаходів та оцінки ефективності їх використання. Вирішення цих завдань виходить за рамки методу CRAMM.

До недоліків методу CRAMM можна віднести наступне:

– використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора;

– CRAMM в значно більшою мірою підходить для аудиту вже існуючих ІС, що знаходяться на стадії експлуатації, ніж чим для ІС, що знаходяться на стадії розробки;

– аудит за методом CRAMM – процес досить трудомісткий і може вимагати місяці безперервної роботи аудитора;

– програмний інструментарій CRAMM генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці;

– CRAMM не дозволяє створювати власні шаблони звітів або модифікувати

наявні;

– можливість внесення доповнень до бази знань CRAMM не доступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретної організації;

– ПЗ CRAMM існує тільки англійською мовою;

– вартість ліцензії від 2000 до 5000 доларів.

Проведемо порівняльний аналіз розглянутих програмних продуктів системи захисту інформації для визначення їх переваг та недоліків.

Виходячи з порівняльного аналізу було визначено наступне:

– системи Гриф та CRAMM обмежена в можливості завдання власних контрзаходів, при тому, що база зумовлених слабо покриває весь спектр реальних засобів та рішень. Також Гриф не дозволяє задавати власні властивості активів;

– використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора;

– для вітчизняних користувачів проблема полягає в тому, що отримати використовувані в RiskWatch оцінки (такі як LAFE і SAFE) для наших умов досить проблематично;

– висока вартість ліцензії для RiskWatch (від 10 000 доларів за одне робоче місце для невеликої компанії) та CRAMM (від 2 000 до 5 000 доларів за одне робоче місце для невеликої компанії).

В результаті аналізу для дослідження ризиків та загроз ІБ при використанні мобільних пристроїв було обрано програмний продукт ГРИФ.

1.4. Висновки до розділу

У цьому розділі сформульовано та описано вирішувану проблему. Проаналізовано основані загрози та вразливості для мобільних пристроїв. Їх виявлення та усунення дозволить зменшити економічні втрати підприємства. Проведено докладний аналіз окремих існуючих програмних продуктів (ГРИФ, RiskWatch, CRAMM), що реалізують функції оцінки ризиків та загроз ІБ. Визначено їх переваги та недоліки.

РОЗДІЛ 2

Теоретичне дослідження

2.1. Теоретичний аналіз методів та підходів до оцінювання загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень

Задача аналізу ризиків безпеки інформації поділяється на дві стадії:

– ідентифікацію ризиків (Risk Identification);

– оцінку ризиків (Risk Estimation).

Задача оцінки ризиків передбачає:

– визначення методу оцінки ризиків, причому оцінка, в свою чергу, може бути якісною і кількісною;

– оцінку наслідків інцидентів ІБ;

– визначення характеристик ймовірності (випадковості) інцидентів ІБ;

– обчислення рівня ризику.

Необхідно визначити, які підходи до оцінки ризиків використовувати – якісні або кількісні. Враховуючи, що призначенням аналізу ризиків є обґрунтування виділення фінансових коштів на заходи з обробки ризиків, основним критерієм має бути ступінь корисності результатів для обґрунтування таких вкладень [10-13].

Таким чином, з одного боку, якісні методи прості для розуміння і використання, з іншого – якісні методи не можуть дати конкретну оцінку, наскільки вигідно застосування комплексу контрзаходів і чи вигідно взагалі. Прикладами прогрманих засобів, які використовують ці методи є OCTAVE, PRo Audit Advisor, COBRA, Proteus, FRAP, КОНДОР+, RiskAdv і їм подібні. [14]

У свою чергу, за допомогою кількісних методів можна із заданою точністю сказати про необхідні засоби та заходи захисту, а також про ступінь економії коштів при їх впровадженні. Представниками програмних засобів, які використовують кількісні методи, є RISK, OCTAVE. [14]

Досить часто для проведення оцінки використовуються програмні комплекси, в основі яких лежить змішаний підхід, зокрема CRAMM, MSAT, NIST,

ГРИФ. [14]

У той же час існуючі методи і засоби мають ряд недоліків.

Розглянемо чотири підходи до кількісної оцінки ризику [15-16]:

1. Статистичні методи – передбачається визначення ймовірності реалізації загрози для розглянутого інформаційного активу за інтервал часу на основі виконання наступних вимог:

– об'єкти, до аналізу яких передбачається використовувати статистику, і об'єкти, на яких зібрана статистика, є еквівалентними (вимога еквівалентності об'єктів);

– умови, при яких передбачається використовувати статистику, і умови її збору є еквівалентними (вимога еквівалентності умов);

– обсяги вибірок статистики є достатніми, методи обробки – коректними, а джерела відомостей – заслуговують довіри (вимога переконливості).

До недоліків цієї групи методів слід віднести критичність до вихідних даних, які, як правило, або відсутні, або їх недостатньо для побудови коректних висновків.

2. Ймовірнісно-статистичні методи використовують залучення додаткової інформації про розподіл збитків у разі реалізації загрози безпеці інформаційного активу. Передбачається, що для розглянутих умов функціонування організаційно-технічної системи підприємства відома функція розподілу збитку інцидентів ІБ. На її основі визначається частка катастрофічних подій від загального числа негативних подій.

Вважаючи цю частку постійної або прогнозуючи з тимчасового ряду її значення на заданий момент часу, можна визначити ймовірні характеристики катастрофічних подій. При цьому точність і достовірність результатів, отриманих із застосуванням ймовірнісно-статистичних методів, визначається якістю і обсягом додаткової інформації про розподіл збитків.

3. Теоретико-ймовірнісні методи використовуються для визначення частот або ймовірностей реалізації рідкісних загроз безпеці інформації зі значними наслідками, за якими статистика практично відсутня. В основі цього методу лежать закономірності переростання ініціюючих подій в надзвичайні, декомпозиція задачі,

оцінки приватних показників і визначення частоти рідкісних негативних подій з урахуванням взаємозв'язку приватних показників.

Теоретико-імовірнісний метод досить трудомісткий, має низьку точність і достовірність отримуваних в процесі дослідження результатів, але при відсутності інших оцінок його застосування виправдане.

4. Експертні методи ґрунтуються на знаннях і досвіді експертів.

Такі методи можуть бути використані, якщо немає статистичних показників. Експерт повинні дати відповідь на запропоновані запитання щодо стану чи подальшої поведінки інформаційних даних, що характеризуються параметрами, які невизначені або властивостями, які невивчені. Для інтерпретації або математичної обробки експертних даних можна використовувати математичний апарат теорії нечітких множин.

Складність проведення аналізу для ризиків ІБ шляхом застосування експертного методу зв'язана, перш за все, із невизначеністю характеристик масивів даних, на основі яких відбулося формування досвіду експерта і, як наслідок, з відсутністю чітких гарантій щодо отримання достовірних результатів.

Основними складовими частинами проведення дослідження загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень є [18-21]:

– дослідження загроз для безпеки інформації, що зберігається на мобільному пристрої (МП);

– аналіз ризиків для мобільних пристроїв;

– огляд методик та методів для аналізу ризиків і загроз для МП;

– вибір методики;

– реалізація системи підтримки прийняття рішень з оцінки ризиків і загроз в ІС підприємства з елементами мобільного зв'язку.

Для дослідження оцінювання загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень оберемо ймовірнісно-статистичні та експертні методи. Основними факторами для вибору цих методів є: відсутність або неповнота статистик по інцидентам ІБ при використанні МП на підприємстві.

Для апробації запропонованих етапів дослідження проведемо експеримент по оцінці ризиків на підставі існуючої системи захисту інформації та розробленого

програмного продукту на основі контрольного прикладу.

2.2. Теоретичні методи розв'язання завдань оцінювання загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень

В попередньому підрозділі розглянуто чотири основні методи кількісної оцінки ризиків: статистичний, ймовірнісно-статистичний, теоретико-ймовірнісний та експертний.

Для розв'язання задачі кількісної оцінки ризиків обрано два методи: ймовірнісно-статистичний та експертний [15].

2.2.1 Ймовірнісно-статистичний метод. Ймовірнісно-статистичний метод базується на використанні допоміжної інформації щодо розподілу збитків для аналізованого об'єкту від небезпеки, яка розглядається, при її реалізації.

Припустимо, розподіл $f(w)$ негативних подій по збитку відомо. Вважаючи цю частку $q = \int_{KC}^{\infty} f(w)dw$ постійною $q(t) = const$ або прогнозуючи з тимчасового ряду за допомогою деякої моделі її значення на заданий момент часу, можна побудувати методику оцінки ймовірності катастрофічної події.

Індивідуальна ймовірність негативної події $(Q_{\Sigma}(\Delta t))$ для n_{Σ} знаходять за співвідношенням:

$$Q_{\Sigma}(\Delta t) = n_{\Sigma}(\Delta t)/N, \qquad (2.1)$$

де n_{Σ} – загальне число негативних подій для об'єкта, що розглядається в оцінюваному році;

N – число подій для об'єкта, що розглядається в оцінюваному році.

Ймовірність катастрофічної події $(Q(\Delta t))$:

$$Q(\Delta t) = Q_{\Sigma}(\Delta t) q . \qquad (2.2)$$

Якщо значення q приймається відомим абсолютно точно, тоді (δ) оцінки $Q(\Delta t)$ знаходиться за формулою:

$$\delta = \frac{Z_{\gamma}}{\sqrt{\frac{Q}{q} N}} ; \qquad (2.3)$$

де (δ) - відносна статистична похибка, Z_{γ} – оцінка катастрофічних подій.

Тут потрібний обсяг спостережень для його оцінки з потрібною точністю можна буде найти при виконанні нерівності:

$$N \geq N_3 = \frac{Z_{\gamma}^2 q}{Q \delta_T^2} . \qquad (2.4)$$

За сумісного використання об’єднання даних за декілька років та допоміжної інформації про розподіл негативних подій за розміром збитку умову (2.4) можна представити так:

$$N \geq N_4 = \frac{Z_{\gamma}^2 q}{Q \delta_T^2} . \qquad (2.5)$$

В загальному статистична похибка оцінки $Q(\Delta t)$ з (2.2) визначається співвідношенням:

$$\delta_Q = \sqrt{q^2 \delta_Q^2 + Q_Q^2 \delta_q^2}\ ; \qquad (2.6)$$

де δ_q^2 – дисперсія оцінки q.

Долю q_j класу негативних подій, що розглядається можна визначити двома способами:

$$q_j = P\left(w_{qC_{j-1}}\right) < W = w_{qC_j}\ . \qquad (2.7)$$

– як долю подій (негативних) j-го класу від загального числа подій (негативних) в аналізованому році. Для зменшення статистичної похибки оцінки необхідно об'єднувати статистичні дані за інтервал спостереження;

– за відомим розподілом негативних подій по збитку. Однак частота негативних подій з важкими наслідками, що знаходяться на «хвості» розподілу негативних подій за розміром збитку мала, тобто вони є рідкісними подіями (відбуваються не щороку або для об'єкта аналізу не відбувалися до розглянутого моменту часу взагалі). Для таких подій навіть при використанні об'єднаної вибірки за інтервал спостереження характерна значна статистична невизначеність оцінок як ймовірності реалізації, так і їх частки. Тому для прогнозу частки негативних подій, що знаходяться на «хвості» розподілу (катастроф), доцільно використовувати умову (2.7) і теоретичний розподіл негативних подій по збитку, яке встановлюють за статистичними даними відомими методами перевірки згоди розрахованого розподілу з теоретичним. Можна використовувати й інші розподіли негативних подій за розміром збитку, що відносяться до класу розподілів з «важкими правими хвостами».

Об’єднання неоднорідних даних по збитку на основі моделей динаміки. Для негативних подій, які класифікуються як катастрофічні, точність оцінки q_j по (2.7) істотно залежить від точності визначення виду і параметрів форми розподілу $F(w)$. Для її підвищення також необхідно збільшити обсяг статистичних даних, що пов'язано з розширенням інтервалу спостереження. Однак з плином часу умови прояву розглянутої небезпеки змінюються і

статистичні дані вже не належать досліджуваній Генеральній сукупності; при цьому змінюється не тільки число n негативних подій, а й їх розподіл $F(w)$ по збитку. Це означає, що пряме об'єднання статистик неможливо. Для об'єднання даних по збитку від негативних подій в деякому інтервалі часу спостереження необхідно перераховувати з урахуванням тенденцій зміни їх розподілу по збитку.

Припустимо, є статистичні дані негативних подій за T років, що включають дані про збитки в n_1, n_2, ... , n_T негативних подіях. Будемо вважати умови реалізації негативних подій змінними по роках, а протягом одного року незмінними. Тоді випадкові величини W_1, ... , W_T, що характеризують наслідки негативних подій, розрізняються, тобто в загальному випадку наявні дані про негативні події належать різним генеральним сукупностям, описуються своїми функціями розподілу $F_1(w)$, ... , $F_T(w)$. При цьому параметри (в першу чергу математичні очікування $M[W]$), а можливо, і види розподілу розрізняються.

Зазначені функції розподілу відрізняються і від функції розподілу $F_T(w) = P(W_T < w)$ можливих наслідків W_T негативних подій в оцінюваній році.

Об'єднаймо відомі статистичні дані про негативні події за T років. Припустимо, що види розподілів випадкових величин W_1, ... , W_T близькі, а різняться лише масштаби розподілів, тобто математичні очікування $M[W_1]$, $M[W_2]$, ... , $M[W_T]$. Наведемо відомі статистичні дані про наслідки негативних подій за вказані роки до оцінюваної генеральної сукупності негативних подій, що описується функцією розподілу $F_T(w) = P(W_T < w)$. Для цього скористаємося теорією стохастичної подоби. Інваріантом подібності різних вибірок при однакових законах розподілу є рівність математичних сподівань:

$$M[W_i] = idem \forall t = 1,...,T . \qquad (2.8)$$

Звідси витікає співвідношення для коефіцієнта перерахунку даних про негативні події, отриманих в 1-му році, на рік що оцінюється:

$$k_{idem\forall t} = \frac{M[W_T]}{M[W_t]} \forall t = 1,...,T . \quad (2.9)$$

Дані по збитку в k-й негативний події перераховуються за формулою:

$$W_{kT} = k_{idem\forall t} w_{kt} . \quad (2.10)$$

де $k = 1,...,n$.

Обсяг об'єднаної вибірки зростає приблизно в T раз. Враховуючи істотне збільшення обсягу статистичних даних в об'єднаній вибірці, більш точно можна оцінити параметри розподілу $F_T(w)$ на рік, що оцінюється, а після класифікації даних про збитки – долі qj негативних подій різних класів.

2.2.2 Експертний метод. Цей метод базується на застосування досвіду та знань висококваліфікованих фахівців в досліджуваній предметній області – експертів. Він є доцільним, якщо відсутні окрім статистики по об'єкту (рідкісними є негативні події), ще й математичні моделі (наявна складно формалізована задача).

Основна ідея методу – експертам пропонується дати відповіді на запитання щодо стану або поведінки вподальшому об'єктів з параметрами, які невизначені, або властивостями, які невивчені. Оцінки експертів оформляють, в тому числі, у вигляді якісних атрибутів або кількісних характеристик ймовірностей розглянутих подій на певному часовому проміжку. Головним моментом тут є формування шкали оцінки, яку використовують експерти. Така оптимальна шкала повинна мати відносно невелике число градацій (від 3 до 10), де для кожної градації є певний інтервал ймовірностей. Також кожна градація повинна містити коротку текстову якісну характеристику.

Для представлення та подальшого математичного опрацювання отриманих від експертів даних потрібно використовувати моделі, які базуються на нечітких множинах або методах математичної статистики.

Обробка результатів опитування експертів. На базі оцінок експертів виходить узагальнена інформація про досліджуваний об'єкт (явище) і формується рішення, що задається метою експертизи. Залежно від цілей експертизи при обробці оцінок можуть вирішуватися такі проблеми:

– формування узагальненої оцінки;

– визначення відносних ваг об'єктів;

– встановлення ступеня узгодженості думок експертів і інші.

Розглянемо деякі методи вирішення кожного з перерахованих завдань.

Формування узагальненої оцінки. Отже, нехай група експертів оцінила який-небудь об'єкт, тоді x_j – оцінка j-го експерта, $j=\overline{1,m}$, де m – число експертів. Для формування узагальненої оцінки групи експертів найчастіше використовуються середні величини. Наприклад, медіана (ME), за яку береться така оцінка, по відношенню до якої число більших оцінок дорівнює числу менших. Може використовуватися також точкова оцінка для групи експертів, яка обчислюється як середнє арифметичне $(\overline{x_y})$:

$$\overline{x_y}=\frac{\sum_{j=1}^{m}x_j}{m}. \qquad (2.11)$$

Визначення відносних ваг об’єктів – це визначення, наскільки той чи інший фактор (об'єкт) важливий (істотний) з точки зору будь-якого критерію.

В цьому випадку говорять, що потрібно визначити вагу кожного фактора.

Один з методів визначення ваг полягає в наступному. Нехай x_{ij} – оцінка фактора i, дана j-им експертом, $i=\overline{1,n}$, $j=\overline{1,m}$, n – число порівнюваних об'єктів, m – число експертів. Тоді вага i-го об'єкта, підрахована за оцінками всіх експертів (wi), дорівнює:

$$w_i=\frac{\sum_{j=1}^{m}w_i}{m}; \qquad (2.12)$$

де w_{ij} – вага і-го об'єкта, підрахована за оцінками j-го експерта, дорівнює:

$$w_{ij} = \frac{x_{ij}}{\sum_{i=1}^{n} x_{ij}}. \quad (2.13)$$

Встановлення ступеня узгодженості думок експертів. У разі участі в опитуванні декількох експертів розбіжності в їх оцінках неминучі, проте величина цієї розбіжності має важливе значення. Групова оцінка може вважатися достатньо надійною тільки за умови гарної узгодженості відповідей окремих фахівців. Для аналізу розкиду та узгодженості оцінок застосовуються статистичні характеристики – міри розкиду.

Варіаційний розмах (R):

$$R = x_{\max} - x_{\min}; \quad (2.14)$$

де $x_{\max}$ – максимальна оцінка об'єкту; $x_{\min}$ – мінімальна оцінка об'єкту.

Середнє квадратичне відхилення (2.5), що обчислюється за формулою:

$$\delta = \sqrt{\frac{\sum_{j=1}^{m} \left(x_j - \overline{x_y}\right)^2}{m-1}}; \quad (2.15)$$

де x_j – оцінка, дана *j*-им експертом; *m* – кількість експертів.

Коефіцієнт варіації (V), який виражається у відсотках:

$$V = \frac{\delta}{\overline{x_y}} * 100\%. \quad (2.16)$$

Недоліки методу:

– неможливість гарантій достовірності отриманих оцінок;

– труднощі щодо проведення опитування експертів і обробці даних, які отримані при дослідженні.

Важливо відмітити, що другий недолік цілком може бути подоланий, а от перший – має принципове значення. Підвищення точності експертних оцінок є можливим через запрошення експертів з вищою кваліфікацією та за рахунок збільшення числа таких незалежних експертів.

2.3. Підхід до оцінки загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень

При проведенні якісної оцінки ризиків ІС організації захищеність кожного цінного ресурсу розраховується при допомозі аналізу загроз конкретного ресурсу, і вразливостей, через які ці загрози могли бути реалізованими. Здійснюючи оцінку імовірності реалізації актуальних для цінного ресурсу загроз і ступеня впливу реалізації загрози на ресурси, необхідно проводити аналіз інформаційних ризиків ресурсів організації [25, 26].

В результаті роботи програма представляє наступні дані:

– інвентаризацію ресурсів;

– значення ризику для кожного цінного ресурсу організації;

– значення ризику для ресурсів після завдання контрзаходів (залишковий ризик);

– ефективність контрзаходів.

Базуючись на введених власником ІС даних, потрібно виконати побудову моделі ризиків та загроз, які є актуальними для ІС компанії (див. рис 2.1). На основі побудованої моделі потрібно проаналізувати ймовірності реалізації загроз ІБ на кожен ресурс та, відповідно, розраховані ризики.

Основний зміст підходу до оцінки загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень підприємства описано в [25-30].

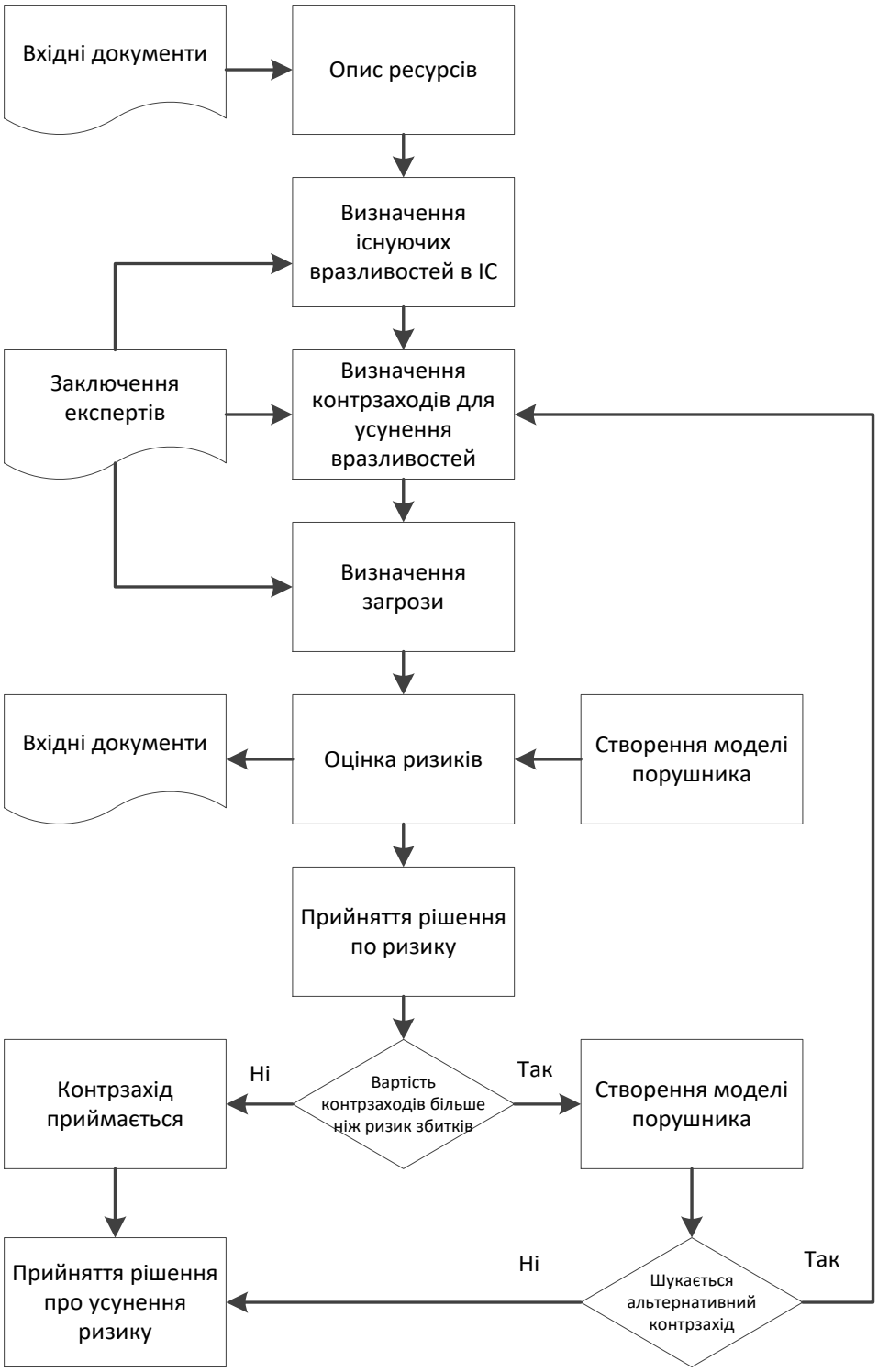


Рис 2.1. Модель оцінки загроз та ризиків

Таким чином, підхід до оцінки ризиків загроз та ризиків для організації ІБ потребує такі вхідні дані:

– ресурси;

– критичність ресурсу;

– відділи, до яких відносяться ресурси;

– загрози, що діють на ресурси;

– уразливості, через які реалізуються загрози;

– ймовірність реалізації загрози через дану вразливість;

– критичність реалізації загрози через дану вразливість.

2.4. Математична постановка дослідження оцінювання загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень

Розрахунок ризиків загрозі для ІБ підприємства:

– спершу необхідно провести розрахунок рівня загрози за вразливостями на основі критичності та ймовірності реалізації загрози через дану уразливість. Рівень загрози свідчить про те, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її впровадження.

$$У_{\text{у}} = \frac{КР_{\text{у}}}{100} * \frac{В_{у}}{100}; \quad (2.17)$$

де $У_{\text{у}}$ – рівень загрози по вразливості; $КР_{\text{у}}$ – критичність загрози; $В_{\text{у}}$ – ймовірність реалізації загрози.

Отримуємо значення рівня загрози по уразливості в інтервалі від 0 до 1.

– на другому етапі потрібно виконати розрахунок рівня загрози за уразливістю з урахуванням контрзаходів на основі критичності та ймовірності реалізації загрози через дану уразливість. Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її впровадження після прийняття контрзаходів

Для розрахунку рівня загрози по вразливості з урахування контрзаходів використовують формулу:

$$У_{\text{у\_к\_кон}} = \frac{КР_{\text{у}}}{100} * \frac{В_{\text{у\_к\_кон}}}{100}; \quad (2.18)$$

де $B_{\text{у\_к\_кон}}$ – рівень загрози по вразливості з урахуванням контрзаходів; $Y_{\text{у\_контр}}$ – ймовірність реалізації загрози з урахуванням контрзаходів.

Отримуємо значення рівня загрози по уразливості в інтервалі від 0 до 1.

– на третьому етапі розраховується ризик по кожному ресурсу в процентній та грошовій формах за наступними формулами:

$$P = KP_p * \frac{KP_y}{100} * \frac{B_y}{100}; \tag{2.19}$$

$$P_{грн} = C_p * \frac{KP_y}{100} * \frac{B_y}{100}; \tag{2.20}$$

де P – ризик по ресурсу в %; KP_p – критичність ресурсу; $P_{грн}$ – ризик по ресурсу в грн.; $C_{\text{р}}$ – вартість ресурсу;

– на четвертому етапі розраховується ризик по кожному ресурсу з урахуванням контрзаходів в процентній та грошовій формах за наступними формулами:

$$P_{\_контр} = KP_{\text{р}} * \frac{KP_y}{100} * \frac{B_{y\_контр}}{100}; \tag{2.21}$$

$$P_{грн\_контр} = C_{\text{р}} * \frac{KP_y}{100} * \frac{B_{y\_контр}}{100}; \tag{2.22}$$

де $P_{\_контр}$– ризик по ресурсу в %; $P_{грн\_контр}$ – ризик по ресурсу в грн.

– на п’ятому етапі розраховується загальний ризик по кожному ресурсу та загальний ризик по кожному ресурсу з урахуванням контрзаходів за формулами:

$$P_{\_общ} = 1 - \prod_{i=1}^{n} (1\text{-}P); \tag{2.23}$$

$$P_{\_контр\_общ} = 1 - \prod_{i=1}^{n} (1 - P_{\_кконт}); \quad (2.24)$$

де $P_{\_общ}$ – розраховується загальний ризик по кожному ресурсу; $P_{\_контр\_общ}$ – загальний ризик по кожному ресурсу з урахуванням контрзаходів.

– на шостому етапі розраховується ризик по ІС (P_{ic}) та ризик по ІС з урахуванням контрзаходів ($P_{ic\_контр}$) розраховується за наступними формулами:

$$P_{ic} = \sum_{i=1}^{n} P; \quad (2.25)$$

$$P_{ic\_контр} = \sum_{i=1}^{n} P_{\_кконт}. \quad (2.26)$$

В результаті проведення розрахунків згідно з методикою оцінки ризиків та загроз ІБ отримують такі дані:

– ризик реалізації по одній загрозі для ресурсу;

– ризик реалізації по одній загрозі для ресурсу з урахуванням контрзаходів;

– ризик реалізації сумарно по всіх загрозам для ресурсу;

– ризик реалізації сумарно по всіх загрозам для ресурсу з урахуванням контрзаходів;

– ризик в цілому для ІС;

– ризик в цілому для ІС з урахуванням контрзаходів;

– ефективність контрзаходів.

2.5. Висновки до другого розділу

В цьому розділі проведено теоретичний аналіз методів та підходів до оцінювання загроз та ризиків для організації ІБ підприємства. Описано чотири види методів для кількісної оцінки ризику (статистичні, ймовірнісно-статистичні,

теоретико-ймовірнісні, експертні). Для розв’язання задачі кількісної оцінки ризиків основна увага приділена ймовірнісно-статистичним та експертним методам. Запропоновано підхід до оцінки загроз та ризиків та сформульована математична модель задачі для оцінки загроз та ризиків для організації ІБ при використанні мобільних бізнес-рішень.

РОЗДІЛ 3
ПРАКТИЧНЕ ДОСЛІДЖЕННЯ ОЦІНЮВАННЯ ЗАГРОЗ ТА РИЗИКІВ ДЛЯ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Програмна реалізація підходу до оцінювання загроз та ризиків ІБ

Умови проведення експериментального дослідження оцінювання загроз та ризиків ІБ:

– для проведення експериментального дослідження використовується спроектований та розроблений автором роботи програмний засіб та комплекс «Гриф»; [20]

– вхідні дані для розрахунку ризику однакові.

Мета проведення експериментального дослідження – порівняти можливості по оцінці ризиків та загроз ІБ при використанні мобільних пристроїв в роботі підприємства.

3.1.1. Розробка алгоритму для оцінювання загроз та ризиків ІБ. В роботі пропонується алгоритм для оцінювання загроз та ризиків ІБ системи захисту інформації підприємства (див. рис 3.1.)

На першому етапі виконання алгоритму відбувається отримання ресурсів для оцінювання. Наступним етапом відбувається внесення даних про ресурси, загрози, вразливості та контрзаходи до БД. Дані вносяться з відомостей про ресурси та заключень експертів.

Потім відбувається розрахунок показників ризику для ресурсу.

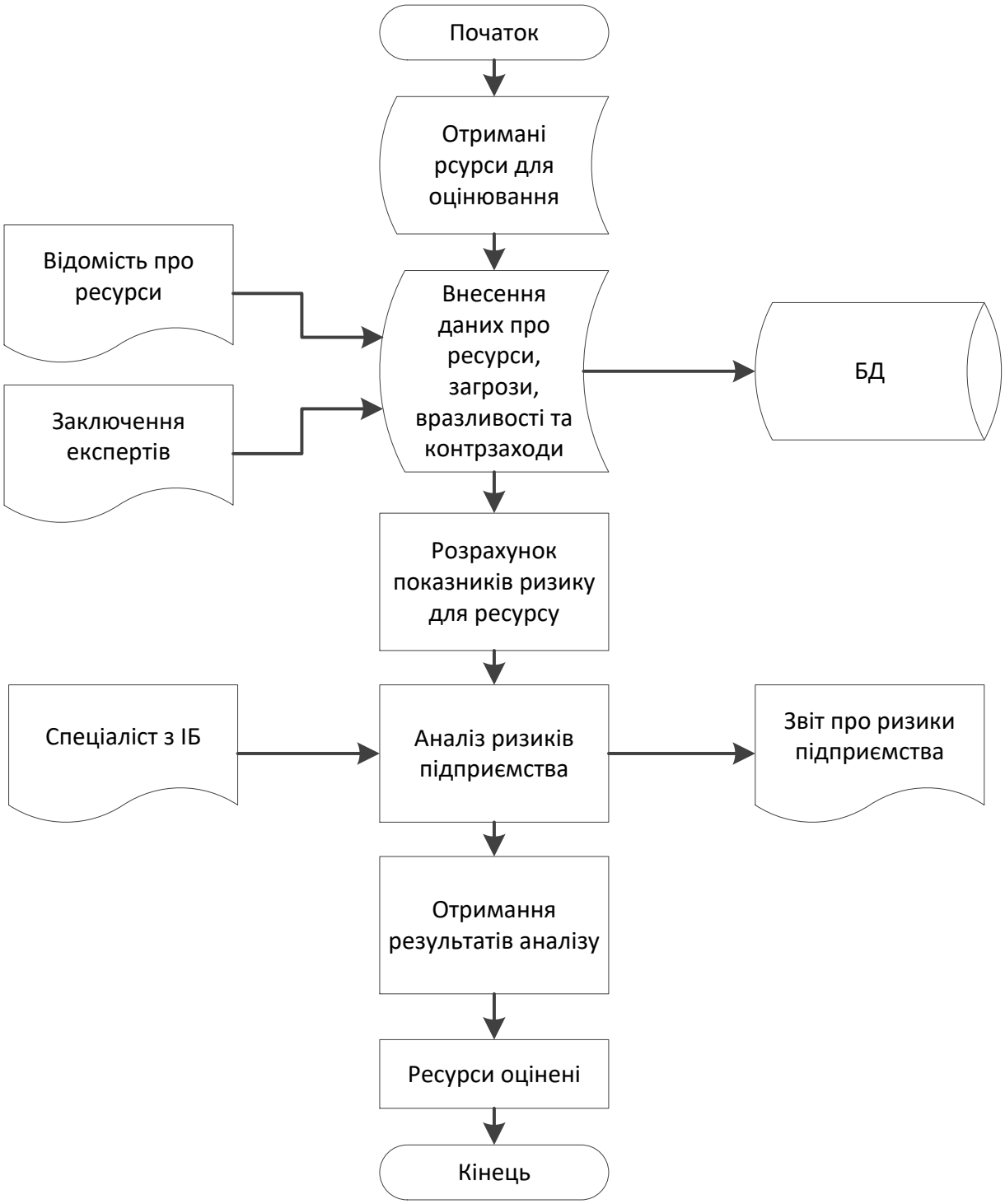


Рис 3.1. Блок-схема алгоритму для оцінювання загроз та ризиків ІБ

Спеціаліст по ІБ виконує аналіз ризиків підприємства, на основі чого генерується звіт про ризики підприємства.

Потім відбувається отримання результатів аналізу та висновок, що результати оцінені.

3.1.2. Опис архітектури програмного продукту. В результаті процесу розробки програмного продукту для оцінювання загроз та ризиків ІБ системи захисту інформації підприємства були розроблені з використанням [31] класи, які реалізують основну бізнес-логіку програмного продукту (див. рис 3.2).

Рис 3.2. Діаграма класів програмного засобу

Опис класів, які реалізують основну бізнес-логіку програмного продукту наведено в таблиці 3.1.

Таблиця 3.1

Опис класів, які реалізують основну бізнес-логіку програмного продукту

Класи	Призначення
Auth	Авторизація користувача в системі
Usersc	Додавання, редагування даних користувача
Addresurs, Resyrcu, Updresurs	Додавання, редагування та видалення записів про ресурси
Adduyaazvim, Upduyazvim, Uyazvimost	Додавання, редагування та видалення записів про вразливості
AddUgrozu, Ugrozu, UpdUgrozu	Додавання, редагування та видалення записів про загрози
AddRisk, Risk, UpdRisk	Додавання, редагування та видалення записів про ризики
AddConter, Contrmeru, Updcontr	Додавання, редагування та видалення записів про контрзаходи
RepResurs, ReportRisk, RepUgrozu, RepStIC	Створення звітів

3.2. Структура БД програмного продукту

3.2.1. Інформаційний список документів. Вхідні та вихідні документи, які використовуються для оцінювання загроз та ризиків ІБ, наведені в таблиці 3.2.

Таблиця 3.2

Інформаційний список документів

Код документу	Назва	Вхідний/вихідний
БС-01	Відомість про ресурси	вхідний
БС-02	Заключення експертів	вхідний
БС-03	Звіт по ресурсам	вихідний
БС-04	Звіт по загрозам	вихідний
БС-05	Відомість аналізу вартості ІС	вихідний
БС-06	Звіт по ризикам	вихідний

В якості джерел довідкової інформації використовуються таблиці ресурсів, загроз, вразливостей, контрзаходів, ризиків ти витрати на ІС. Форми вихідних документів наведені в додатку. [29]

3.2.2. Модель даних. Глобальна інфологічна модель даних включає: [29, 30]

– оцінювання ризиків;

– додавання, редагування, видалення користувачів;

– додавання, редагування, видалення витрат на ІС.

В БД є наступні сутності: Ugrozu, Risks, Resurcu, Users, Zatratu, Schala_gradacuu, Kontrmeru, Uyazvimostu. Вони необхідні для найбільш зручної роботи з програмним продуктом, який цілком відповідає предметній області. Фізична модель даних наведена на рис 3.3.

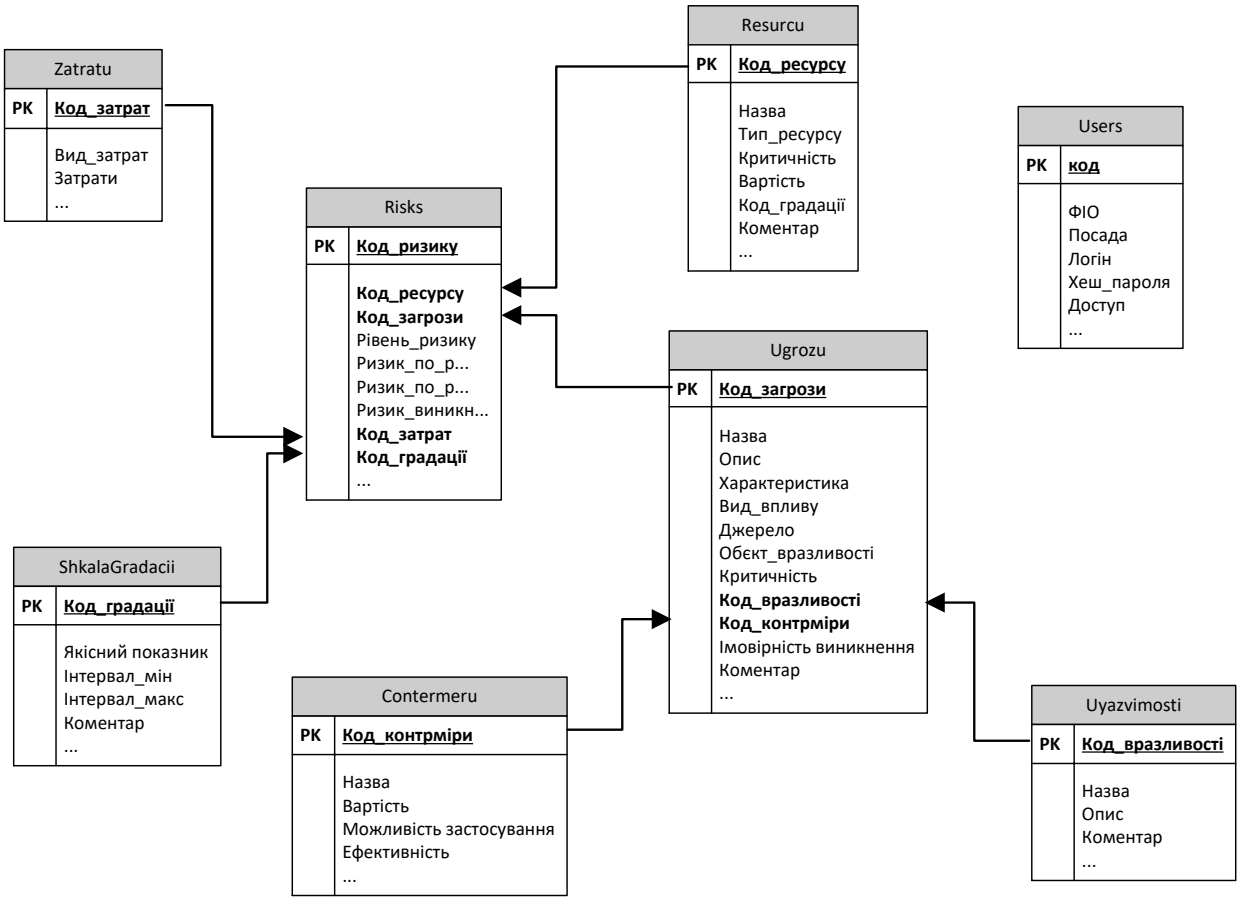


Рис 3.3. Фізична модель даних

Сутність Ugrozu містить інформацію про загрози. Сутність Risks містить перелік та характеристики ризиків. Сутність Resurcu – містить перелік та опис ресурсів ІС. Users – список користувачів. Zatratu – перелік та призначення затрат. Особливо слід відмітити сутність Schala_gradacuu – котра містить шкалу градації загроз. Сутності Kontrmeru та Uyazvimostu містять переліки контрмір та вразливостей, відповідно. Між сутностями встановлено зв’язки «один до багатьох»

по ключових полях.

В якості джерела початкових даних для контрольного прикладу розглянемо абстрактне IT підприємство. Початкові дані формують експерти виходячи з власного досвіду або статистичних даних.

3.3. Порівняльне тестування програмних продуктів

3.3.1. Опис роботи з розробленим програмним продуктом. Після запуску програмного продукту, користувач побачить вікно для авторизації. Після вводу правильного логіну та паролю буде відкрито головне вікно програми.

Для того, щоб можна було почати оцінювати ризики ІБ , треба заповнити наступні довідники:

– довідник ресурсів;

– довідник вразливостей;

–довідник контрзаходів;

– довідник загроз.

Вікно для роботи з списком ресурсів наведене на рис 3.4.

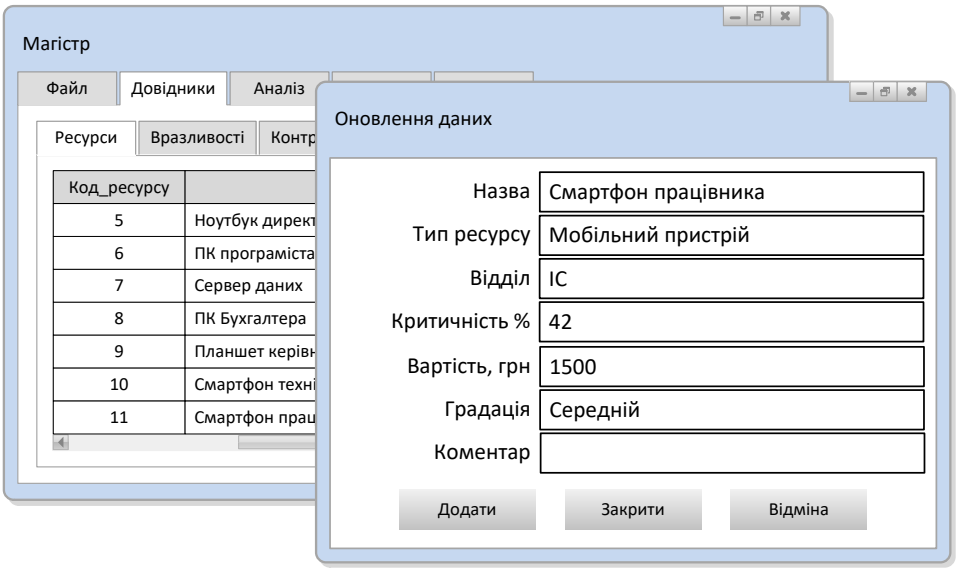


Рис 3.4. Вікно введення інформації про ресурси

Вікно для роботи з списком вразливостей наведене на рис 3.5.

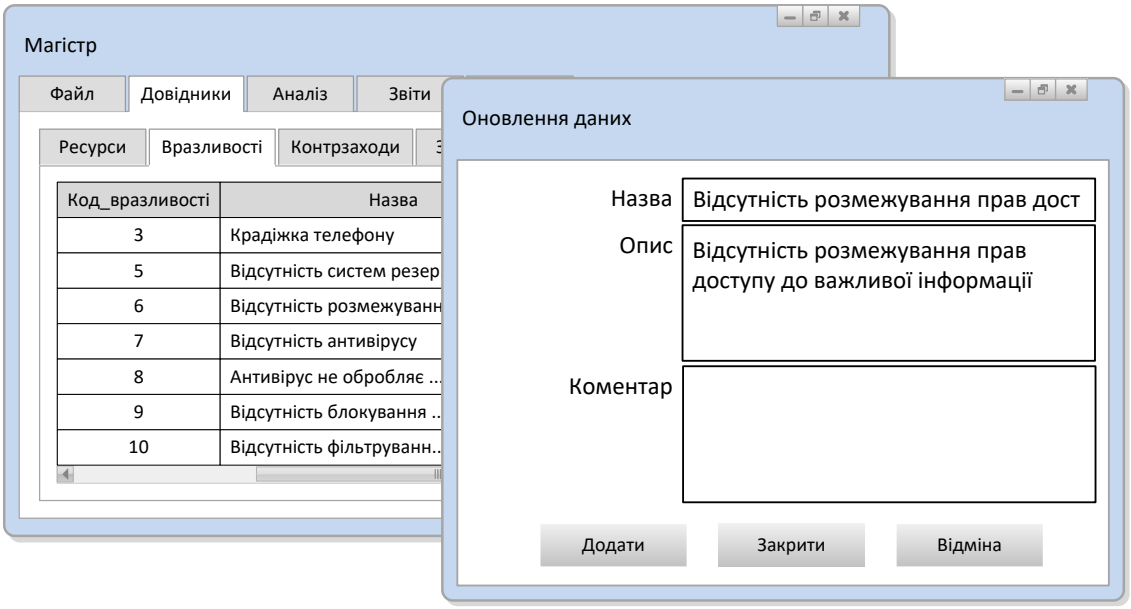


Рис 3.5. Вікно введення інформації про вразливості

Вікно для роботи з довідником контрзаходів наведене на рис 3.6.

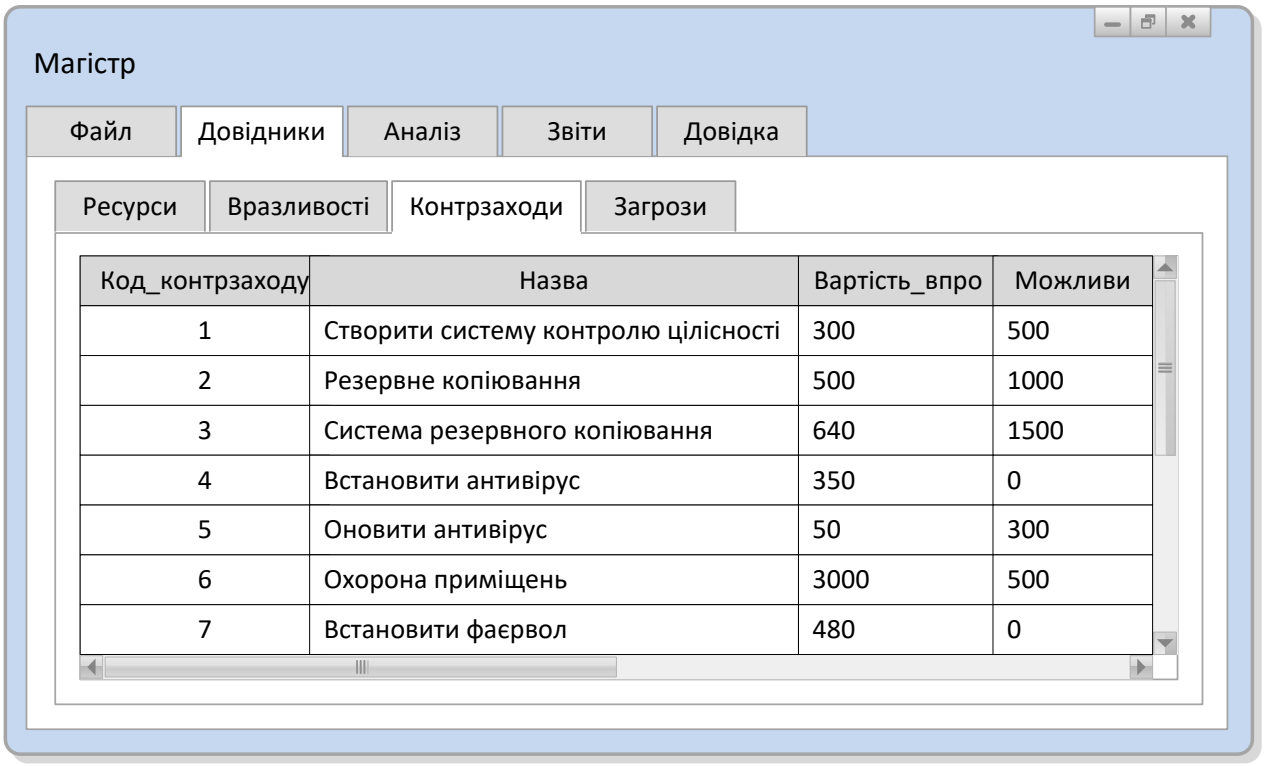


Рис 3.6. Вікно введення інформації про контрзаходи

Вікно для роботи з довідником загроз наведене на рис 3.7.

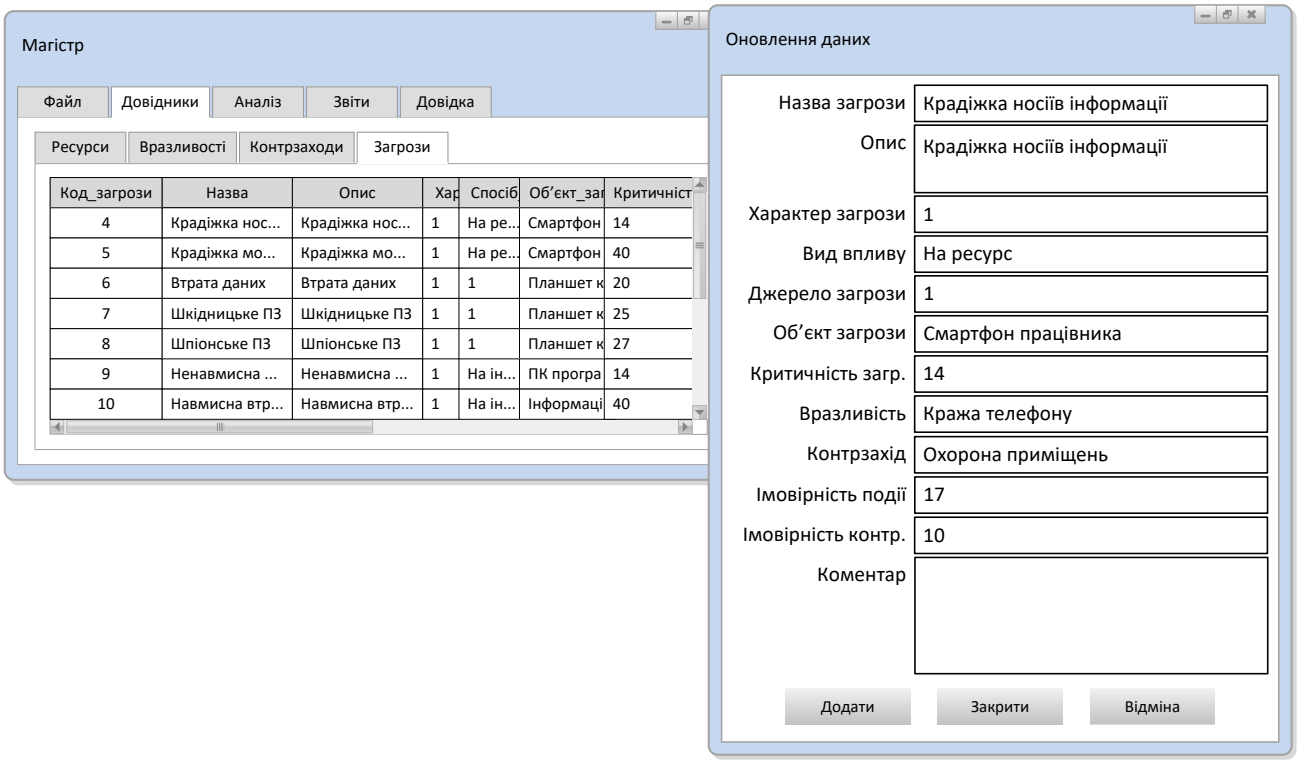


Рис 3.7. Вікно введення інформації про загрози

Після заповнення довідників можливо приступити до оцінки ризиків. Для цього необхідно заповнити аналіз ризиків (див. рис 3.8).

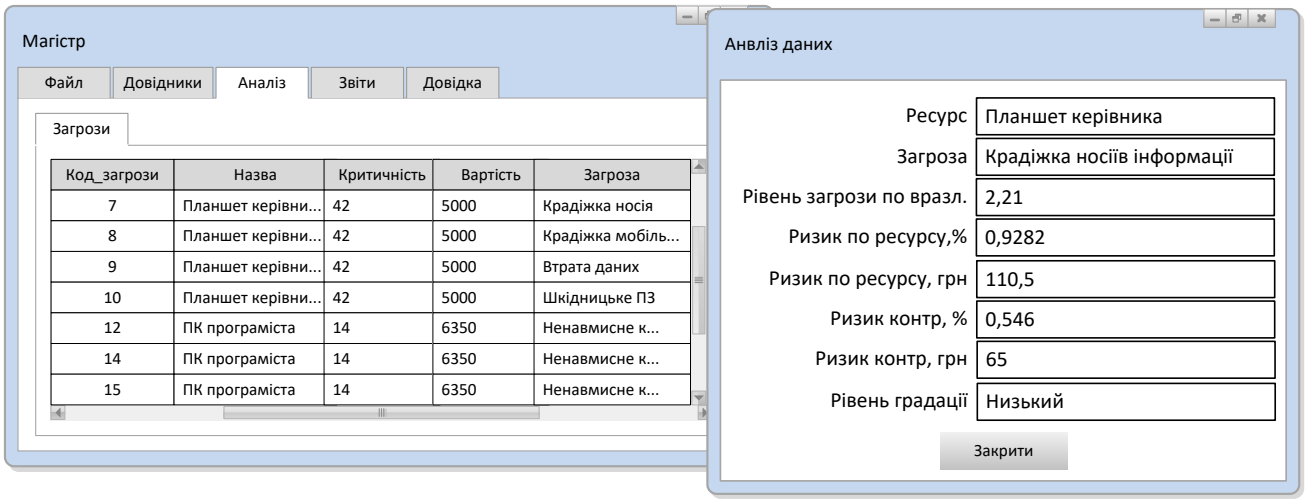


Рис 3.8. Вікно перегляду інформації про ризики

Програмний продукт дозволяє провести комплексну оцінку ризиків згідно попередньо введених наборів даних.

3.3.2. Опис роботи з програмним продуктом «Гриф». Після запуску програмного продукту, користувач побачить вікно для авторизації. Після вводу правильного логіну та паролю буде відкрито головне вікно програми. Для початку роботи потрібно створити новий проект, або завантажити вже існуючий. Для того, щоб можна було почати оцінювати ризики інформаційнії безпеці, треба заповнити наступні довідники:

– довідник відділів (рис 3.10);

– довідник ресурсів (рис 3.11-3.12);

– довідник загроз (рис 3.13-3.14).

– довідник вразливостей (рис 3.15-3.16);

На початковому етапі слід ввести перелік відділів підприємства (див. рис 3.9).

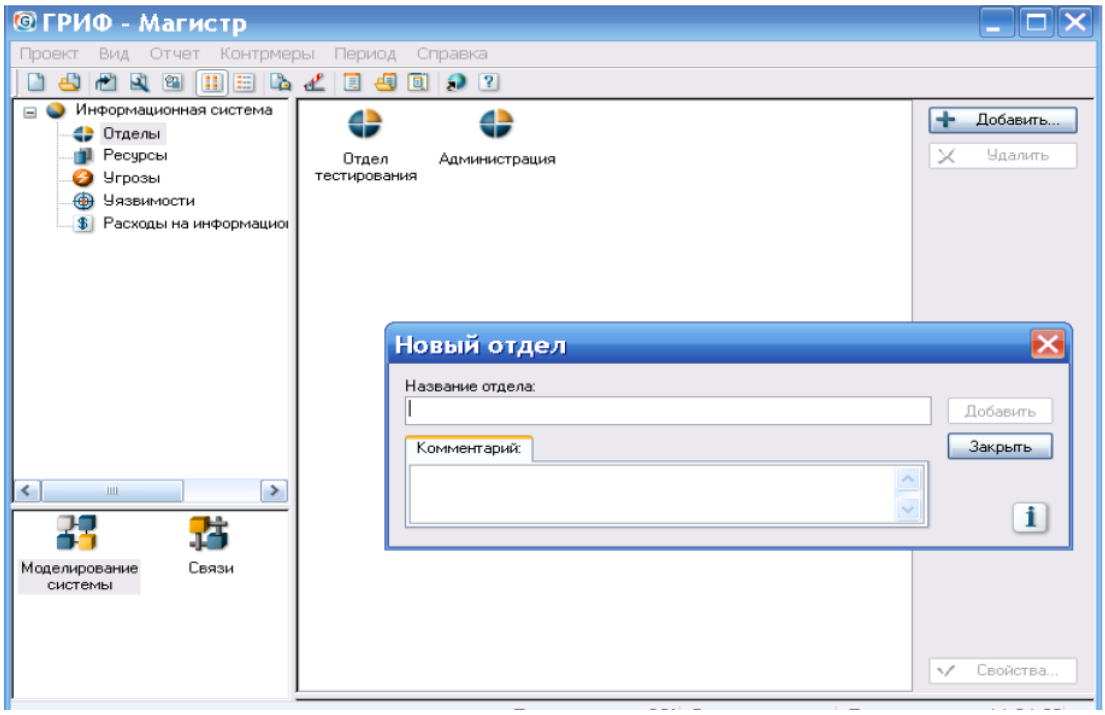


Рис 3.9. Вікно введення інформації про відділи підприємства

На наступному етапі потрібно ввести перелік пристроїв (див. рис 3.10).

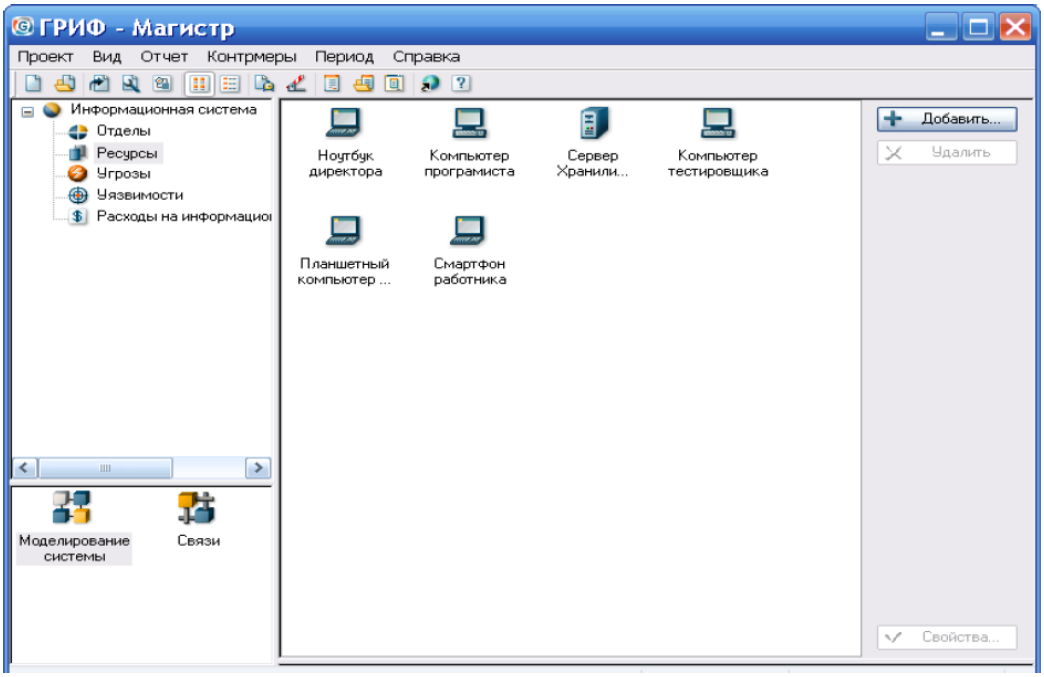


Рис 3.10. Перелік пристроїв

Вікно редагування властивостей пристрою неведено на рис 3.11.

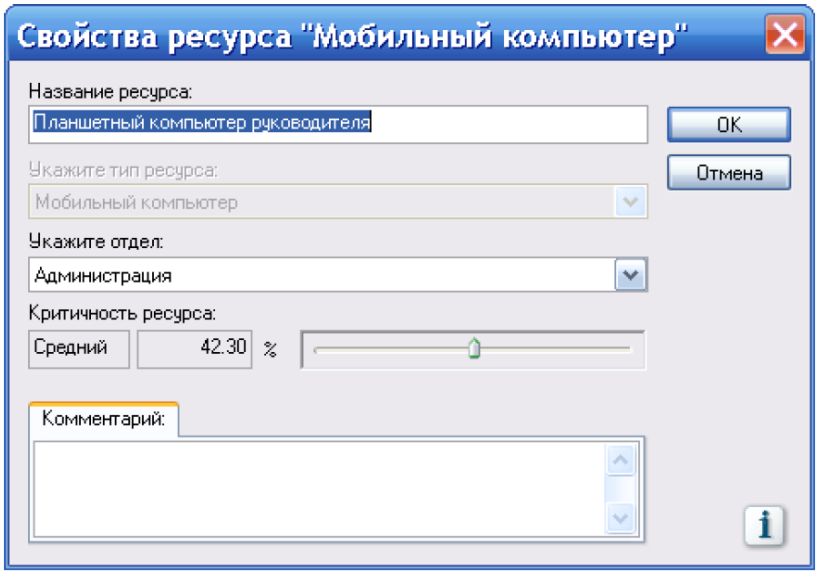


Рис 3.11. Вікно введення інформації про ресурси

Вводимо інформацію про загрози та вразливості на основі початкових даних (див.рис 3.12).

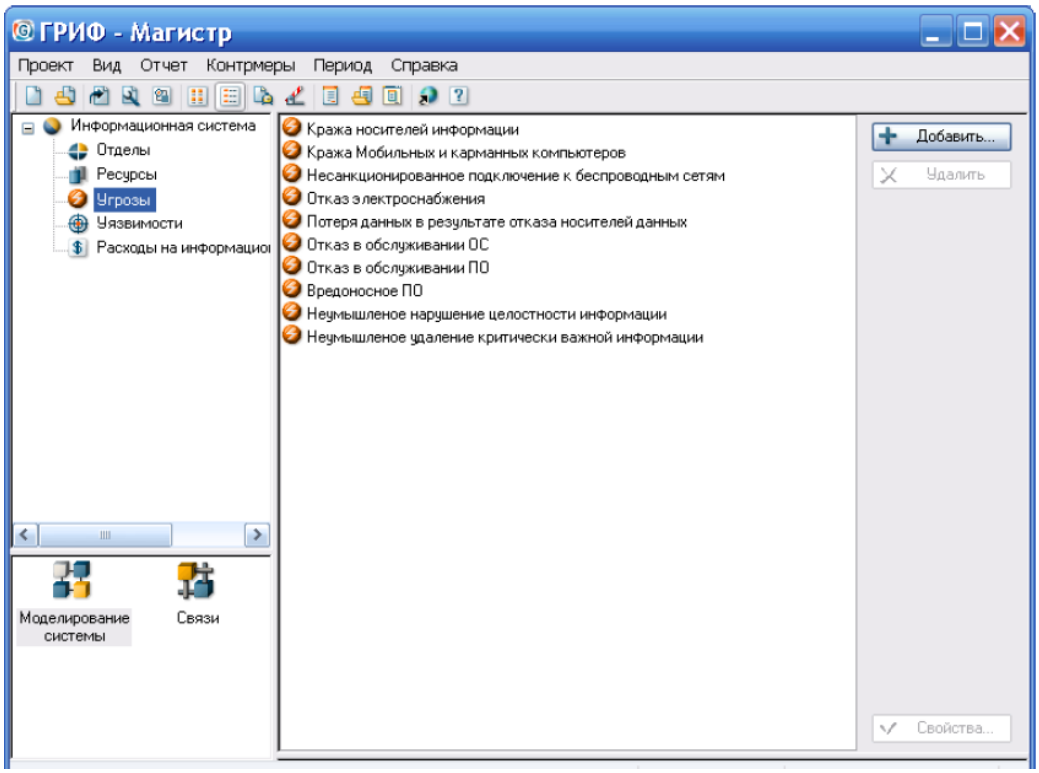


Рис 3.12. Вікно довідника, загроз

На рис 3.13 наведено вікно введення інформації про загрози.

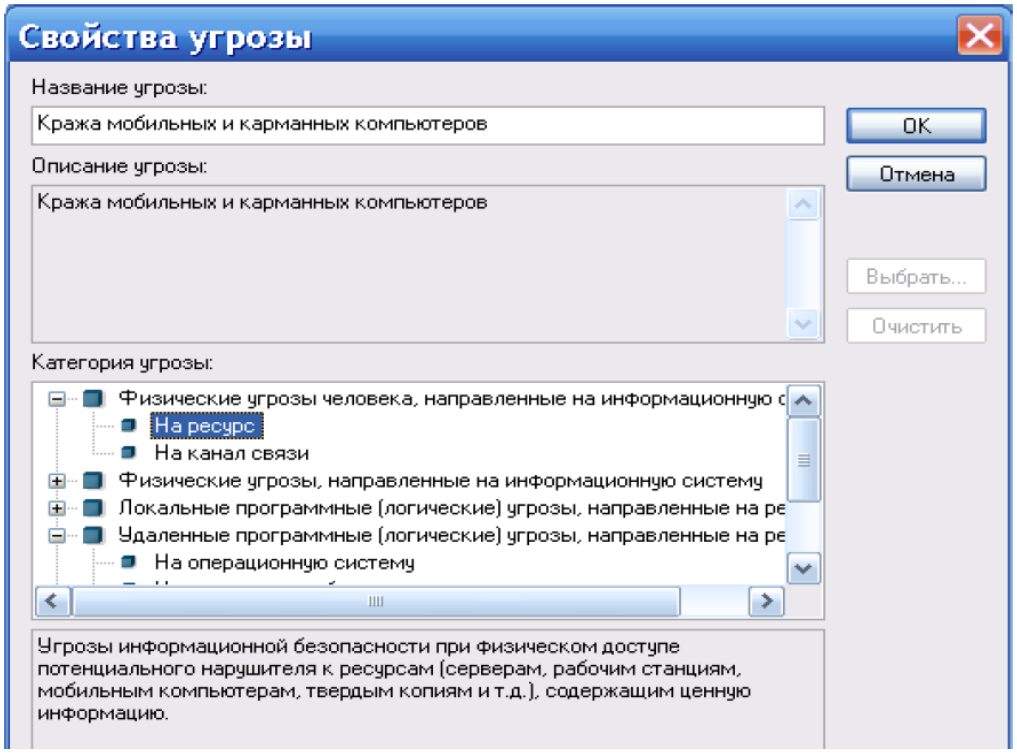


Рис 3.13. Вікно введення інформації про загрози

На рис 3.14 представлено вікно довідника вразливостей.

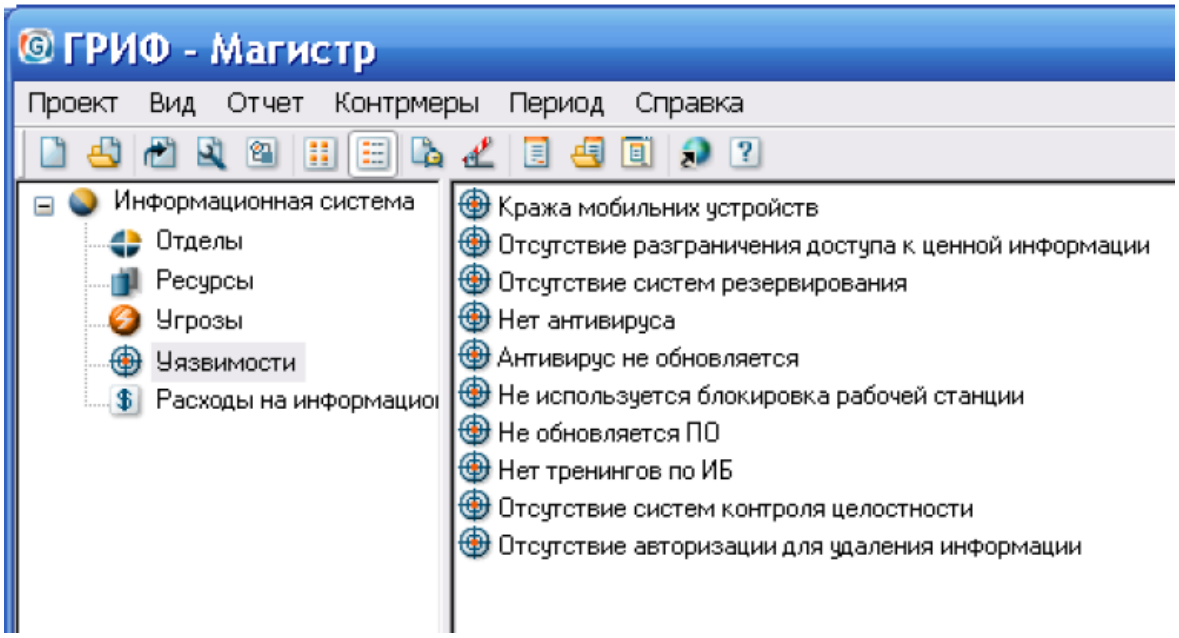


Рис 3.14. Вікно довідника вразливостей

Введення даних про ту чи іншу вразливість представлене на рис 3.15.

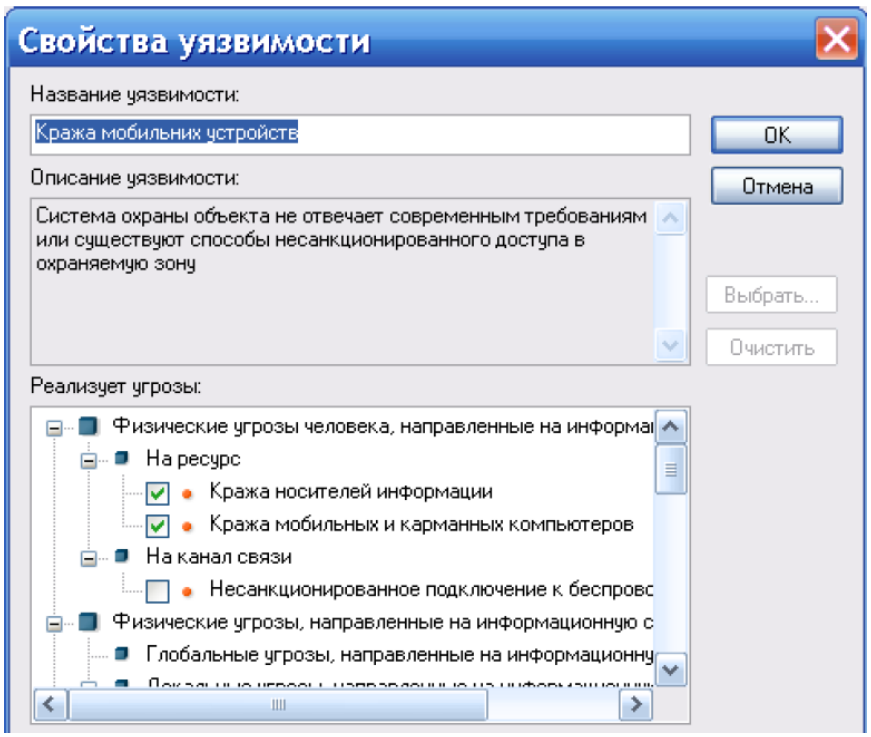


Рис 3.15.Вікно введення інформації про вразливості

Введення інформації про контрзаходи показане на рис 3.16.

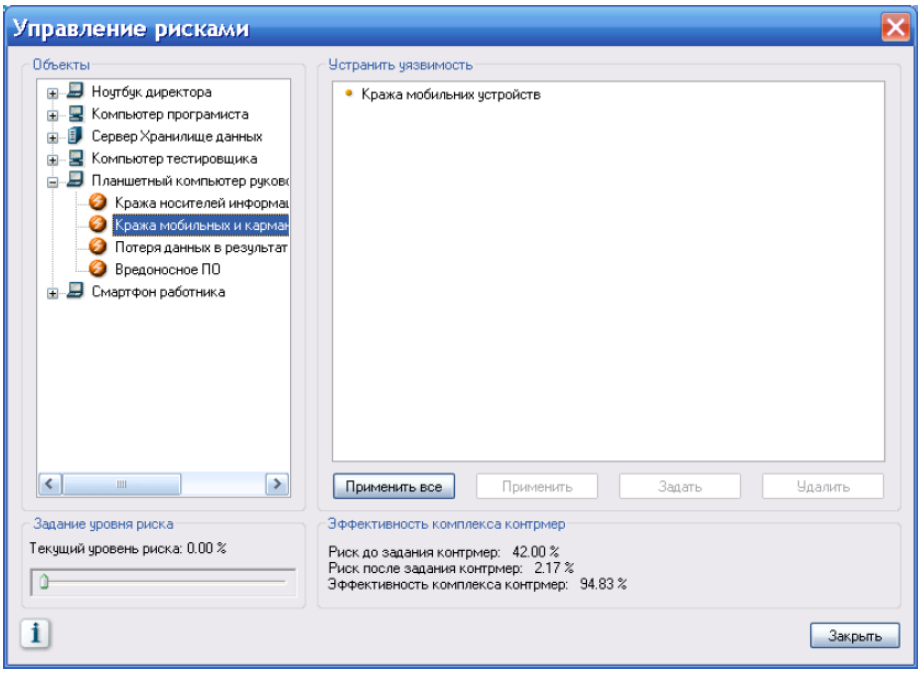


Рис 3.16. Вікно введення інформації про контрзаходи

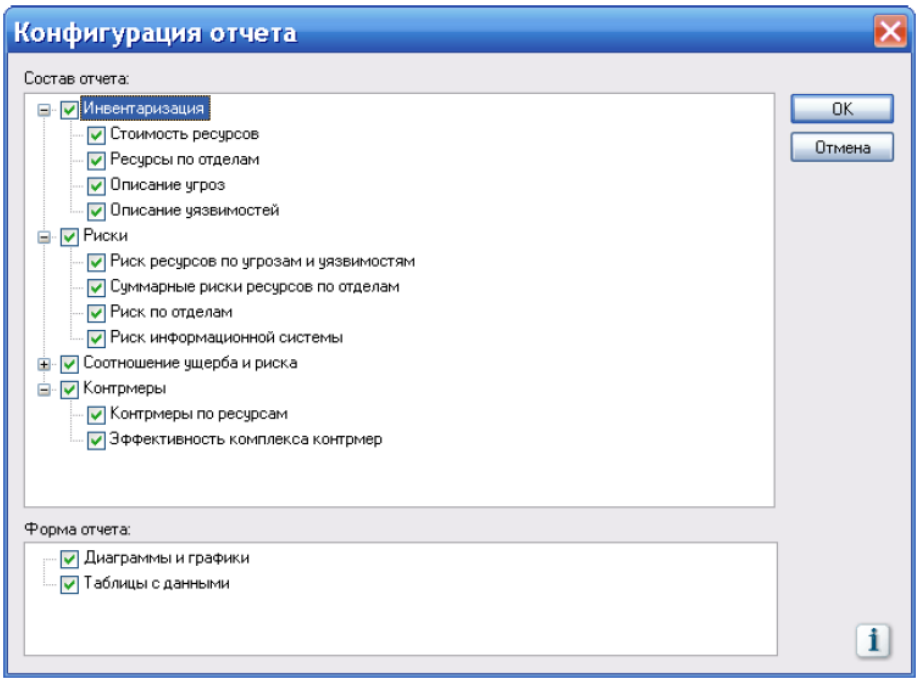


Рис 3.17. Вікно конфігурування звіту

Для відображення результатів розрахунків створюємо звіт з потрібною нам конфігурацією відображення інформації (див. рис 3.17).

3.3.3. Результати оцінки ризиків на основі контрольного прикладу. Результати оцінки ризиків по ІБ наведено у звіті, наведеному в додатку. Звіт для порівняльної оцінки в системі «Гриф» наведено в додатку.

Результати оцінювання загроз та ризиків ІБ якогось тестового ІТ-підприємства:

– отримані результати показують, що найбільшому ризику підлягають мобільні пристрої. На даний час мобільні пристрої мають низький рівень захисту інформації. Найбільш поширеними загрозами для них є: зараження шкідливим ПЗ та крадіжка пристроїв з ціною інформацією.

Більшість загроз для мобільних пристроїв можна усунути за допомогою встановлення спеціального ПЗ для захисту інформації, вчасного оновлення існуючого ПЗ та ОС, дотримання правил користування мобільними пристроями. Найменшому ризику з розглянутих ресурсів підлягають персональні комп'ютери (ПК).

Для ПК розроблено різноманітні засоби для захисту та збереження інформації.

– отримані результати показують достатньо адекватні та достовірні оцінки ризиків ІБ, які отримані при використанні розробленого програмного засобу та комплексу «Гриф».

Переваги розробленого програмного засобу над комплексом «Гриф»:

– можливість вільно встановлювати значення критичності ресурсу;

– можливість завдавати власні типи ресурсів;

– можливість додавати більш ніж один контрзахід, щоб зменшити ймовірність виникнення загрози;

– можливість встановити ПП на ОС Windows 7.

Недоліком пропонованого програмного засобу є те, що він може оцінювати ризики тільки для тих ресурсів, для яких можна визначити точну їх вартість.

3.4. Висновки до третього розділу

В цьому розділі запропоновано програмну реалізацію підходу до оцінки ризиків та загроз ІБ. Розроблено і описано алгоритм для проведення поетапної оцінки загроз та ризиків ІБ. Описано архітектуру програмного продукту, представлено діаграму класів розробленого продукту. Докладно описано основні сутності БД. Результати проведеного порівняльного тестування розробки та програмного комплексу ГРИФ дозволяють стверджувати про можливість використання розробленого продукту для проведення практичного дослідження.

РОЗДІЛ 4
ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою цього розділу дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності від дослідження і використання методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень, а також прийняття рішення щодо подальшого розвитку і впровадження або ж недоцільність впровадження відповідної розробки.

Для здійснення оцінки потрібно зробити розрахунки трудомісткості кожної операції, що мала місце при проведенні наукових досліджень.

4.1. Розрахунок норм часу на виконання науково-дослідної роботи

Реалізація проекту дослідження і використання методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень складається з низки послідовних та взаємопов’язаних етапів. Кожен із етапів реалізації проекту характеризується метою та змістом, оцінкою часу виконання, кількістю та спеціалізацією виконавців, а також приблизною оцінкою вартості.

Реалізація проекту складається із підготовчого етапу, етапу технічної пропозиції, створення технічного завдання, проектування системи, практичної реалізації, тестування, верифікації та заключного етапу.

Норми часу на виконання науково-дослідницької роботи розраховуватимуться на основі середнього часу виконання стадії в годинах, що наведені в таблиці 4.1 разом із інформацією про виконавців і сумарною кількості затраченого часу.

Таблиця 4.1

Операції технологічного процесу та їх час виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	Підготовча стадія	Проектний менеджер Інженер-програміст	10
2	Технічна пропозиція	Проектний менеджер Інженер-програміст	10
3	Створення технічного завдання	Проектний менеджер Інженер-програміст	20
4	Проектування системи	Інженер-програміст	20
5	Практична реалізація	Інженер-програміст	135
6	Тестування системи	Тестувальник	20
7	Верифікація системи	Тестувальник Інженер-програміст Проектний менеджер	20
8	Створення документації	Інженер-програміст	20
9	Заключна стадія	Проектний менеджер	10
Разом			265

В підсумку на реалізацію проекту дослідження і використання методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень необхідно 265 людино-годин, залучення трьох спеціалістів та виконання дев’яти різноманітних стадій реалізації проекту.

4.2. Визначення витрат на оплату праці та відрахувань на соціальні заходи

Визначення витрат на оплату праці та відрахувань на соціальні заходи прямо залежить від кількості витраченого працівниками часу на роботу, ставки в годину

чи місяць, кількість відрахувань на соціальні заходи встановлених в законному порядку на час розрахунку.

В результаті розрахунку потрібно визначити основну та додаткову заробітну плату, витрати на соціальні заходи та на основі цих даних визначити сумарні витрати на оплату праці. Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами. Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Наймані працівники для дослідження і використання методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень працюють згідно контракту, який в якому вказано їхню погодинну ставку. Тобто розрахунок заробітної плати працівників відбуватиметься на базі тарифної ставки та кількості відпрацьованих годин.

У штаті найманих працівників для дослідження і використання методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень залучено проектного менеджера, інженера-програміста і тестувальника.

Тарифні ставки учасників процесу дослідження і використання методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень:

- Проектний менеджер – 150 грн./год.
- Інженер-програміст – 130 грн./год.
- Тестувальник – 100 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \, , \qquad (4.1)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в виконує три спеціаліста, то основна заробітна плата буде розраховуватись за даною формулою 4.1;

$$З_{осн.} = 150 \cdot 35 + 130 \cdot 200 + 100 \cdot 30 = 34250 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати й визначається за формулою (4.2).

Коефіцієнт додаткових виплат працівникам становить 0,1.

$$Здод. = Зосн. \cdot Кдопл., \quad (4.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам

$$З_{дод} = 34250 \cdot 0,1 = 3425 \text{ грн.}$$

Звідси загальні витрати на оплату праці (фонд заробітної плати) визначаються за формулою (4.3):

$$Во.п. = Зосн. + Здод. \quad (4.3)$$

$$В_{о.п.} = 34250 + 3425 = 37675 \text{ грн.}$$

З цієї суми утримуються обов’язкові відрахування на соціальні заходи:

– Єдиний соціальний внесок, що становить 22%;
– Військовий збір, що становить 1,5%;
– податок на доходи фізичних осіб: 18%;

Сума відрахувань становить 41,5% від фонду оплати праці та визначається за формулою:

$$В_{с.з.} = Ф_{оп} \cdot 0,415 \quad (4.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$B_{с.з.} = 37675 \cdot 0{,}415 = 15635{,}125$$

Усі витрати обчислюються детально наведені в таблиці 4.2 та обчислюються за формулою:

$$Взп = ФЗП + ФОП \quad (4.5)$$

$$В_{зп} = 34250 + 15635{,}125 = 49885{,}125 \text{ грн.}$$

Таблиця 4.2

Розрахунки витрат на оплату праці

з/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на плату праці, грн. (6=3+4+5)
		Тарифна ставка,	Кількість відпрацьо	Фактично нарах.			
1.	Проектний менеджер	150	35	5250	525	-	-
2.	Інженер-програміст	130	200	26000	2600	-	-
3.	Тестувальник	100	30	3000	300	-	-
Разом		380	265	34250	3425	15635,125	49885,125

Опираючись на розрахунки витрат на оплату та таблицю результатів 4.2 видно, що всього витрати на плату праці становлять 49885,125 грн.

4.3. Розрахунок матеріальних витрат

Матеріальні витрати є невід’ємною частиною розробки та визначаються як добуток кількості витрачених матеріалів та їх ціни за формулою:

$$M_{ві} = q_i \cdot p_i \,, \tag{4.6}$$

де: q_i – кількість витраченого матеріалу і–го виду; p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою:

$$З_{м.в.} = \sum M_{ві} \,. \tag{4.7}$$

Результати проведених розрахунків наведено у таблиці 4.3.

Таблиця 4.3

Результати розрахунків матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Фактично витрачено матеріалів	Ціна одиниці, грн.	Загальна сума витрат, грн.
1	CD диски	шт.	2	7,45	14,90
2	Папір для друку	листів	500	0,15	75,00
3	Чорнила для принтера	шт.	1	80,00	80,00
Всього					169,90

Згідно проведених розрахунків, матеріальні витрати становлять 169,90 грн.

4.4. Розрахунок витрат на електроенергію

Однією із статей витрат є витрати на електроенергію під час проходження усіх етапів реалізації кінцевого продукту.

Затрати на електроенергію одиниці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S, \quad (4.8)$$

де W – необхідна потужність, кВт; T – кількість годин на реалізацію розробки; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютерів для реалізації кінцевого продукту – 400 Вт, кількість годин роботи обладнання згідно таблиці 4.1 – 265 годин.

Визначимо витрати на електроенергію згідно формули :

$$З_в = 0{,}4 \cdot 265 \cdot 2{,}42 = 256{,}52 \text{ грн.}$$

Згідно формули затрати на електроенергію становлять 256,52 грн.

4.5. Розрахунок суми амортизаційних відрахувань

Для будь якої діяльності характерною є властивість зношування на зниження якості властивостей інструментарію та фондів за допомогою яких ведеться діяльність. Для вирішення проблеми із відновленням даних фондів використовується амортизація, що являє собою процес трансформації вартості основних фондів на вартість продукції, яка щойно була створена, задля повного відновлення основних фондів.

Для визначення амортизаційних відрахувань використовується формула:

$$A = \frac{Б_В \cdot Н_А}{100\%} \quad (4.9)$$

де A – амортизаційні відрахування за звітний період, грн.; $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; $Н_А$ – норма амортизації.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Річний робочий фонд становитиме 2352 годин, так як робочий день становить 8 годин, а кількість робочих днів в місяці становить 24,5 годин.

Для даної розробки засобом розробки є комп'ютер. Його сума становить 18500 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 18500 \cdot 5\% / 100\% = 925 \text{ грн.}$$

Згідно проведених обчислень амортизаційні відрахування становлять 925 грн.

4.6. Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2 \ldots 0{,}6 \,, \qquad (4.10)$$

де $H_в$ – накладні витрати.

Отже, накладні витрати становлять згідно формули (4.10):

$$H_в = 37675 \cdot 0{,}2 = 7535 \text{ грн.}$$

Накладні витрати згідно розрахунку формули, становить 7535 грн.

4.7. Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків наведено у таблиці 4.4.

Таблиця 4.4

Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	43103,6	63,74
Відрахування на соціальні заходи	15635,125	23,12
Матеріальні витрати	169,9	0,25
Витрати на електроенергію	256,52	0,38
Амортизаційні відрахування	925	1,37
Накладні витрати	7535	11,14
Собівартість	67625,145	100,00

Собівартість ($С_в$) програмного продукту розрахуємо за формулою:

$$С_в = В_{з.п.} + В_{с.з.} + З_{м.в.} + З_в + А + Н_в \text{ .} \quad (4.11)$$

Отже, собівартість програмного продукту дорівнює:

Св = 49885,125+ 15635,125+ 169,90 + 256,52+ 925+ 7535= 74406,67 грн.

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 74406,67 грн.

4.8. Розрахунок ціни програмного продукту

Ціну науково-дослідної роботи можна визначити можна визначити за формулою:

$$Ц = \frac{С_В \cdot (1 + Р_{рен}) + К \cdot В_{н.і.}}{К} \cdot (1 + ПДВ), \quad (4.12)$$

де $Р_{рен.}$ – рівень рентабельності (30 %); $К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем); $В_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту); *ПДВ* – ставка податку на додану вартість (20%).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та $В_{н.і.}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + Р_{рен}) \cdot (1 + ПДВ) \qquad (4.13)$$

Звідси ціна на роботу складе:

$$Ц = 74406{,}67 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 116074{,}4 \text{ грн.}$$

Загальний розрахунок ціни програмного продукту становить 116074,4 грн.

4.9. Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$Е_р = \frac{П}{C_B}, \qquad (4.14)$$

де $П$ – прибуток; C_B – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - С_в \ . \qquad (4.15)$$

Розраховуємо плановий прибуток:

$$П_{пл} = 116074{,}4 - 74406{,}67 = 41667{,}73 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{С_В} . \qquad (4.16)$$

Тоді,

$$E_р = 41667{,}73 / 74406{,}67 = 0{,}56.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$T_р = \frac{1}{E_р} \ , \qquad (4.17)$$

Термін окупності дорівнює:

$$T_р = 1 / 0{,}5 = 1{,}78 \text{ р.}$$

Згідно формул плановий прибуток від розробки становить 41667,73 грн., економічна ефективність дорівнює 0,56, а термін окупності становить 1,78 роки що вважається доцільним та економічно вигідним.

4.10. Висновки до розділу

В організаційно-економічній частині дипломної роботи освітнього рівня «магістр» було розраховано основні техніко-економічні показники дослідження і використання методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень (див. таблиця 4.5).

Орієнтоване значення економічної ефективності становить 0,56, що є достатньо високим значенням.

Період окупності повинен варіюватися від 1 до 3 років, тоді розвиток вважається доцільним та економічно вигідним. Термін окупності даної роботи становить 1,78 років.

Таблиця 4.5

Техніко-економічні показники науково-дослідної роботи

№ п/п	Показник	Значення
1	Собівартість, грн.	74406,67
2	Плановий прибуток, грн.	41667,73
3	Ціна, грн.	116074,4
4	Економічна ефективність	0,56
5	Термін окупності, рік	1,78

На основі проведених обрахунків можна зробити висновок, що дослідження і використання методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень є доцільним у зв’язку з невеликим терміном окупності та великим обсягом планового прибутку.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1. Охорона праці

Метою дипломної роботи магістра є дослідження методів та засобів оцінювання загроз та ризиків для організації інформаційної безпеки при використанні мобільних бізнес-рішень. Оскільки, проведення робіт з розробки та використання системи передбачає використання комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки виконавцем дипломної роботи.

Для ефективної і безпечної роботи колективу працівників з розробки програмного забезпечення комп'ютерних систем, в тому числі і фахівців з оцінювання зрілості вимог, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [34].

Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин». Згідно Правил приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог:

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України

від 28.10.98 N 247 (далі - ДБН В.2.5-13- 98), з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами Типових норм належності вогнегасників, затверджених наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 02.04.2004 № 151 зареєстрованих у Міністерстві юстиції України 29.04.2004 за № 554/9153 (НАПБ Б.03.001-2004), і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2004.

Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог НАПБ Б.06.004-2005, ДБН В.2.5-13-98, НАПБ А.01.001-2004 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників,

температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним.

Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв.

Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі.

Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При експлуатації програмної системи підтримки процесу розробки вимог, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-1.28-10.

Організація робочого місця фахівця із запровадження або оцінювання рівня зрілості вимог програмного забезпечення повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ГОСТ

12.2.032-78 "ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования".

Відстань від екрана до ока фахівців, які працюють за комп'ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп'ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп'ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з побудови та оцінювання моделей і рівнів зрілості вимог програмного забезпечення при проектуванні комп'ютерних систем.

5.2. Вплив радіації на працездатність населення

Вплив радіації на організм людини називають опроміненням. Під час цього процесу енергія радіації передається клітинам, руйнуючи їх. Опромінення може викликати всілякі захворювання: інфекційні ускладнення, порушення обміну речовин, злоякісні пухлини і лейко, безпліддя і багато іншого. Коли радіоактивне випромінювання проходить через тіло людини або ж коли в організм потрапляють заражені речовини, то енергія хвиль і частинок передається нашим тканинам, а від них клітинам. Радіонукліди накопичуються в організмі поступово [34].

Як відомо, вплив радіації на організм людини або тварини може бути двох видів: зсередини або зовні. Здоров'я не додає ні один з них. Крім того, науці відомо, що внутрішній вплив радіаційних речовин небезпечніше зовнішнього. Найчастіше радіаційні речовини потрапляють в наш організм разом із зараженою водою і їжею. Вплив радіації на організм майже завжди негативний. Хоча доведено, що ультрафіолетова радіація підвищує працездатність організму, оскільки такі промені не тільки мають терапевтичне значення, але при відсутності природного сонця, особливо восени та взимку, є незамінним профілактичним засобом відносно

різних інфекцій. Багато районів з підвищеним радіаційним фоном є визнаними курортами (наприклад, Кавказькі Мінеральні Води, Карлові Вари і т.п.) В Україні в лікувальних закладах достатньо широко використовується корисне опромінення альфа-частинками в радонових ваннах як лікування.

Проте, в основному, радіація за своєю природою шкідлива для життя людини. Спочатку людина втрачає фізичну працездатність, а потім – розумову. Малі дози опромінення можуть призвести до тимчасової втрати працездатності, середні та великі – до онкологічних захворювань і, як наслідок, смерті. Науковий комітет по дії атомної радіації при ООН спробував висловити генетичні наслідки опромінення через такі параметри, як скорочення тривалості життя і періоду працездатності. Ці параметри, звичайно, не можуть дати адекватного уявлення про страждання жертв спадкових недуг або таких речах, як відчай батьків хворої дитини, але до них і неможливо підходити з кількісними мірками. Цілком віддаючи собі звіт в тому, що ці оцінки не більш ніж перша груба прикидка, ООН приводить в своїй доповіді наступні цифри: хронічне опромінення населення з потужністю дози 1 Гр на покоління скорочує період працездатності на 50 000 років, а тривалість життя – також на 50 000 років на кожен мільйон живих немовлят серед дітей першого опроміненого покоління; ті ж параметри при постійному опроміненні багатьох поколінь виходять на стаціонарний рівень: скорочення періоду працездатності складе 340 000 років, а скорочення тривалості життя – 286 000 років на кожен мільйон живих немовлят.

Проникаюча радіація, поширюючись у середовищі, іонізує його, а при проходженні через живу тканину іонізує атоми і молекули, що входять до складу клітин. Це призводить до порушення нормального обміну речовин, зміни характеру життєдіяльності клітин, окремих органів і систем організму, як наслідок - виникає променева хвороба. Аналіз і узагальнення основних результатів наукових досліджень показали, що медичні наслідки Чорнобильської аварії суттєво відрізнялися від прогнозованих ефектів, зокрема значно знижувалася працездатність населення аж до отримання інвалідності та настання смертельних випадків. Всі особи, що зазнали загального хронічного опромінювання в діапазоні потужності поглинених доз 10-4 — 5 * 10-4 Гр/добу (0,01—0,05 рад/добу) чи

еквівалентних доз 0,05 — 0,15 Зв/рік (5 — 15 бер/рік), залишаються здоровими і працездатними.

Відомо, що ступінь променевих (радіаційних) уражень залежить від отриманої дози випромінювання та часу, впродовж якого людина підпадає під його дію. Якщо доза не перевищує 50Р, то виключена навіть втрата працездатності, не кажучи вже про променеву хворобу. Доза в 200-300Р, отримана за короткий час, може викликати тяжкі радіаційні ураження. Здоровий організм людини здатний за цей час виробляти нові клітин на заміну загиблих. Навіть найменші дози викликають необоротні генетичні зміни, які передаються з покоління в покоління, призводять до розвитку синдрому Дауна, епілепсії, появі інших дефектів розумового і фізичного розвитку. Особливо страшно те, що радіаційному зараженню піддаються і продукти харчування, і предмети побуту. Останнім часом почастішали випадки вилучення контрафактної та низькоякісної продукції, що є потужним джерелом іонізуючого випромінювання.

Найпростіший і ефективний спосіб захистити себе від негативного впливу смертоносних променів - триматися подалі від їхнього джерела. Якщо знати все про радіацію і вміти правильно користуватися приладами для її вимірювання, то можна практично повністю уникнути її негативного впливу. Незважаючи на високу небезпеку, яку несе в собі практично будь-яке джерело радіації, методи захисту від опромінення все ж існують.

Всі способи захисту від радіаційного впливу можна розділити на три види: час, відстань і спеціальні екрани. Хоча необхідно знати, що на сьогодні ідеального засобу захисту від радіації не існує. Найкращий спосіб захисту від радіації - взагалі не мати контакту з зараженими предметами і не перебувати в місцях з підвищеним радіаційним фоном.

5.3. Планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації

Найбільш повне та організоване виконання заходів цивільного захисту (ЦЗ) на об’єкті досягається завчасною розробкою плану заходів, які необхідно проводити при загрозі або виникненні надзвичайної ситуації (НС).

План дій органів управління і сил ЦЗ (міністерств, відомств, областей, районів, міст, підприємств, установ і організацій) із запобігання і ліквідації НС розробляється на підставі законодавчих, директивних і нормативних документів і призначений для координації і діяльності центральних і місцевих органів виконавчої влади, керівництва, а також оперативності їх реагування на загрозу і виникнення НС, відвернення або зниження можливої загибелі людей, мінімізація матеріальних збитків і втрат та організацію задоволення першочергових потреб населення, яке постраждало [34]. План визначає порядок дій і відповідальність керівництва відповідних органів управління підприємств, установ і організацій, а також основні заходи щодо організації і проведення робіт із запобігання і ліквідації НС техногенного і природного характеру, узгодження термінів їх виконання, фінансові, матеріальні та інші ресурси, які необхідні для цих заходів і робіт. У план дій включаються заходи щодо захисту робітників і службовців, підтримування виробничої діяльності та інші з урахуванням обстановки після виникнення НС, передбачаються необхідна кількість сил і засобів для ліквідації наслідків НС. Основними вихідними даними при розробці плану дій на об’єкті є рішення та вказівки вищого штабу ЦЗ, розпоряджень начальника ЦЗ об’єкта, документів, що характеризують об’єкт (комунально-енергетичні мережі, стан будівель і споруд, вододжерела та ін.). План дій розробляється на підставі наказу начальника ЦЗ об’єкта. До розробки документів плану залучається керівний склад і спеціалісти об’єкта. Начальник штабу ЦЗ складає графік розробки окремих документів (розділів) і контролює його виконання.

План дій розробляється у двох (при необхідності і більше) примірниках. Підписується план дій начальником штабу ЦЗ об’єкта, погоджується з територіальними управліннями (відділами) з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи і затверджується начальником ЦЗ об’єкта. Після затвердження зміст плану дій доводиться до виконавців. План дій органів управління і сил ЦЗ із запобігання та

ліквідації НС – це програма здійснення запобіжних та захисних заходів. Він дозволяє цілеспрямовано та організовано вирішувати завдання ЦЗ в умовах НС мирного та воєнного часу. При визначенні цих заходів враховується важливість та особливості виробничої діяльності об’єкта, основні завдання органів управління та сил ЦЗ щодо запобігання і ліквідації НС.

План дій органів управління та сил ЦЗ на мирний час складається із п’яти розділів текстової частини і додатків до них. Текстова частина плану включає такі розділи: 1. Висновки із оцінки обстановки на території об’єкта. 2. Приведення в готовність та організація роботи органів управління в НС. 3. Сили ЦО об’єкта, що залучаються до виконання аварійно-рятувальних, пошукових та відновлювальних робіт. 4. Організація забезпечення заходів та дій ЦЗ. 5. Організація управління, оповіщення і зв’язку. Окремо розробляється “План дій органів управління та сил ЦЗ об’єкта при переведенні з мирного на воєнний стан” за ступенями готовності воєнного часу та раптовому нападі супротивника. Крім цього, на об’єкті господарської діяльності розробляються плани служб ЦЗ, щодо забезпечення заходів і дій органів управління і сил ЦЗ при загрозі і виникненні НС та при переведенні органів управління і сил з мирного на воєнний стан.

5. 4. Висновки до розділу

В цьому розділі описані важливі питання охорони праці, вплив радіації на працездатність населення та планування заходів цивільного захисту на об’єкті у випадку надзвичайної ситуації.

РОЗДІЛ 6
ЕКОЛОГІЯ

6.1. Статистика екології об’єктів природного середовища

Складається з статистики екології атмосфери, статистики екології водних ресурсів та статистики екології земельних ресурсів [35]. Розглянемо кожну з цих частин окремо.

Статистика екології атмосфери. Під забрудненням атмосферного повітря розуміють збільшення концентрації фізичних, хімічних та біологічних компонентів понад рівень, що виводить природні системи зі стану рівноваги. Найбільші забруднення атмосфері спричиняють три різновиди людської діяльності: механічна обробка як земної поверхні (сільгоспроботи, утворення кар'єрів тощо) так і різних матеріалів (пиляння, свердлування, розмелювання), що спричинює забруднення атмосфери аерозолями, дрібними частками речовин; виготовлення й робота з леткими речовинами (пальне, розчинники, гази тощо) - спричинює забруднення газами й парами; продукти згоряння (в топках електростанцій, моторах двигунів тощо) - спричиняють всі види забруднень. Система показників викидів шкідливих речовин в атмосферне повітря:

- показники обсягів та щільності викидів;
- показники викидів в атмосферу шкідливих речовин (ШР);
- показники охорони атмосферного повітря;
- показники складу викидів в атмосферу ШР стаціонарними джерелами;
- показники щільності викидів шкідливих речовин;
- показники навантаження забруднювальних речовин на природу.

Сучасний стан забруднення атмосфери – це комплексна характеристика, яка містить такі складові: середньодобові концентрації пилу; середньодобові концентрації діоксиду азоту (NO_x); середньодобові концентрації діоксиду сірки SO_2); середньодобові концентрації оксиду вуглецю; вміст основних забруднюючих речовин в атмосферному повітрі за даними спостережень Держкомгідромету; перелік речовин, вміст яких в атмосферному повітрі міст зумовив найбільше

забруднення за середньорічними і максимальними концентраціями (в кратності ГДК); середній вміст бенз(а)пирену в атмосферному повітрі міста в кратності ГДК; середньозважений вміст окремих іонів (%) в загальній мінералізації атмосферних опадів; санітарно-хімічні показники – досліджено проб всього; кількість проб, що не відповідають нормативам; їх відсоток до досліджених.

Статистика екології водних ресурсів. Гідросфера - це водна сфера нашої планети, сукупність океанів, морів, вод континентів, льодовикових покровів. Запаси води на Землі величезні - 1,46-109 м3 (0,025% її маси). Але це, переважно, гірко- солона морська вода, непридатна для пиття й технологічного використання. Прісна вода, яку використовує людство для своїх потреб, становить лише 1% її загальної кількості на планеті, причому її містять річки, озера й підземні води. Річковий стік України становить у середньому 83,5 млрд. $м^3$, а в посушливі роки зменшується до 48,8 млрд. $м^3$. Підземні води України мають не менше значення для забезпечення водою населення: близько 70% населення сіл і селищ міського типу задовольняють свої потреби в питній воді за рахунок ґрунтових вод (колодязі) чи глибших водоносних горизонтів (свердловин). Стан підземних вод України в цілому кращий, ніж поверхневого стоку, хоча місцями вони забруднюються стоками промислових підприємств, тваринницьких комплексів. Система показники використання та забруднення водних об'єктів складається з таких группоказників: забору та використання води; використання свіжої води; використання прісної води; використання та відведення свіжої води підприємствами галузей економіки; якості води; екологічної безпеки водних об'єктів; скидання забруднювальних речовин у водні об’єкти; очищення зворотних вод на очисних спорудах.

Статистики екології земельних ресурсів. Земельні ресурси - одні з найбільш універсальних природних ресурсів, які необхідні для всіх галузей господарства. Найціннішою частиною земельних ресурсів є сільськогосподарські землі оскільки вони забезпечують людство продуктами харчування. Через діяльність людини, структура земної поверхні постійно змінюється: зменшуються площі сільськогосподарських угідь і лісів, структура грунтів деградує, вони перенасичені шкідливими хімічними сполуками, мають дефіцит вологи або перезволоженість, надлишок води в грунтах та їхню засоленість. Повсюдно родючість грунтів

катастрофічно зменшується. Великих збитків сільському господарству завдає ерозія грунтів. Одне з найбільших лих після ерозії грунтів - їх засолення, основна причина якого полягає в неправильному зрошенні. Тому користуватися грунтом, землею слід розумно й бережно. Потрібні термінові заходи для відтворення структури й родючості грунтів - їх нейтралізація, розсолення, збагачення гумусом тощо.

При статистичному аналізі екології земельних ресурсів використовується система показників екологічного стану земель, до складу якої входять такі групи показників: показники порушення і рекультивації земель; показників стану та забруднення грунтів; показники санітарно-хімічного і мікробіологічного стану грунтів; показники забруднення грунтів cs-137; показники і напрямки природоохоронних витрат. Основні показники ступеня забрудненості ґрунтів - коефіцієнт концентрації забруднення ґрунту; інтегральний показник поелементного забруднення ґрунту; коефіцієнт зворотної реакції ґрунтів на динаміку забруднення.

6.2. Методологічні основи обробки екологічної інформації на базі комп’ютерних технологій

Це комплексне питання, яке містить такі складові [35]:

– зведення і первинне оброблення статистичних даних;

– статистична оцінка екологічного стану НПС і закономірностей його розподілу;

– статистичне групування в екології;

– дисперсійний аналіз в екології;

– кореляційний аналіз зв’язків в екології;

– статистичний аналіз тенденцій і закономірностей динаміки в екології;

– індексний метод в екології.

Зведення і первинне оброблення статистичних даних. Статистичне зведення — це первинне наукове оброблення даних спостереження для характеристики суцільного явища узагальнюючими показниками. Етапи: статистичне групування;

підсумовування даних; табличне і графічне оформлення одержаних даних. За допомогою статистичного зведення розв'язують такі завдання: групування даних, розроблення системи показників для характеристики груп і всієї статистичної сукупності, обчислення групових і загальних показників, зведення результатів обчислення у статистичних таблицях. У результаті обробки та систематизації статистичних матеріалів отримуємо ряди цифрових показників, які характеризують окремі сторони явищ, що вивчаються, в просторі або зміну цих явищ у часі. Тому побудова статистичних рядів є основою будь-якого первинного оброблення статистичної інформації.

Статистична оцінка екологічного стану НПС і закономірностей його розподілу. Властивістю статистичної сукупності є коливання, мінливість значень будь-якої ознаки, тобто варіація. Вона зумовлена дією безлічі взаємопов’язаних причин, серед яких є основні і другорядні. Основні причини формують центр розподілу, другорядні - варіацію ознак, сукупна їх дія - форму розподілу. Аналіз варіаційного ряду розподілу полягає у виявленні закономірностей зміни частот залежно від зміни кількісної ознаки, яка покладена в основу групування. При аналізі варіаційних рядів найуживанішими є такі групи показників: центра розподілу, розміру варіації, форми розподілу.

Статистичне групування в екології. Метою статистичного групування є поділ сукупностей на однорідні типові групи за існуючими для них кількісними ознаками з метою всебічної характеристики їхнього стану, розвитку і взаємодії. Метод статистичних групувань робить статистику одним з наймогутніших знарядь соціального пізнання і використовується для вирішення трьох взаємопов'язаних завдань: виділення різних соціально-економічних типів явищ (процесів) та всебічна їх характеристика; дослідження структури масової сукупності; вивчення взаємодії між окремими ознаками сукупності. Суть методу статистичних групувань полягає у тому, що складне масове явище розглядається не як єдине нероздільне ціле, а в ньому виділяються окремі групи одиниць із статистичними показниками, які дають кількісну характеристику якісно своєрідній частині одиниць усієї сукупності. Тобто кожна з одержаних груп об'єднує однорідні одиниці сукупності.

Дисперсійний аналіз в екології. Для кількісної оцінки взаємозв'язків і їхньої

суттєвості при незначній кількості спостережень застосовується дисперсійний аналіз. Головне призначення дисперсійного аналізу — статистично виявити вплив різних факторів на мінливість ознаки, що вивчається. В результаті дисперсійного аналізу одержуються дані, що характеризують загальне розсіювання, або дисперсію ознаки, обумовлену дією всіх факторів; часткову або факторну дисперсію, викликану впливом організованих і врахованих дослідником факторів; та залишкову дисперсію, пов’язану з невідомими експериментатору, випадковими, неорганізованими факторами. за його допомогою розв'язуються такі завдання: кількісне вимірювання сили впливу факторних ознак та їх сполучень на результативну; визначення вірогідності впливу та його довірчих меж; аналіз окремих середніх та статистична оцінка їх різниці.

Кореляційний аналіз зв’язків в екології. Goглибленням дослідження й кількісною оцінкою характеру та механізму взаємодії факторних і результативних ознак є метод аналізу регресії та кореляції, тобто кореляційний аналіз. При кореляційній залежності будь-якому значенню однієї змінної величини може відповідати декілька чи навіть безліч різноманітних, тобто варіюючих значень іншої змінної величини. Розрахунки на основі кореляційних моделей підвищують ступінь точності аналізу, часто виявляють недоліки попереднього аналізу. Перевага цього методу полягає також і в тому, що він дає можливість розв'язувати задачі, які не можна вирішити за допомогою інших методів економічного аналізу. У дослідженнях важливо вивчати не стільки міру кореляції, скільки форму її й характер зміни однієї ознаки залежно від зміни іншої. Ці задачі розв'язуються методами регресійного аналізу. Використання методу кореляції і регресії дозволяє вирішити такі основні завдання: встановити характер і тісноту зв'язку між досліджуваними явищами; визначити і кількісно виміряти ступінь впливу окремих факторів і їх комплексу на рівень досліджуваного явища; на підставі фактичних даних моделі залежності екологічних показників від різних факторів розраховувати кількісні зміни аналізованого явища при прогнозуванні показників і давати об'єктивну оцінку діяльності підприємств. Використання прикладних програм - це єдиний практичний інструмент розв'язування задач багато- факторного кореляційно-регресійного та аналізу в багатовимірному просторі.

Статистичний аналіз тенденцій і закономірностей динаміки в екології. Екологічні процеси - явище не статичне, а динамічне. Тобто протягом певного часу - місяць за місяцем, рік за роком змінюється стан забруднень природних сфер, рівень викидів забруднюючих речовин в навколишнє середовище, об'єм промислових і побутових відходів на звалищах тощо. Дослідження процесів зміни і розвитку явищ у часі відбувається на основі побудови і аналізу рядів динаміки. Для будь-якого динамічного ряду характерні перелік хронологічних дат (моментів) або інтервалів часу і конкретні значення відповідних статистичних показників, які називають рівнями ряду. Тому кожен ряд динаміки має елементи двох типів - рівні і періоди: рівні - цифри, з яких складається ряд; періоди - дати, якім відповідають рівні ряду.

Індексний метод в екології. Статистична практика при вивченні екологічних явищ широко використовує індекси. Знання методології побудови індексів значно розширює аналітичні можливості дослідника, збагачує результативну інформацію досліджень. За допомогою індексів можна характеризувати зміну в часі і просторі найрізноманітніших показників: обсяги викидів в атмосферу, скидів шкідливих речовин у водне середовище, інтенсивність забруднень і т. д. За допомогою індексного методу вирішуються такі завдання: характеризують загальну зміну складного економічного явища чи окремих його елементів (складових); виділяють вплив одного з факторів через елімінування впливу інших; відокремлюють впливу зміни структури явища на зміну індексованої величини.

6.3. Висновки до розділу

В цьому розділі розглянуті питання статистики екології об'єктів природного середовища та методологічні основи обробки екологічної інформації на базі комп'ютерних технологій.

Висновки

Основними результатами дипломної роботи є:

– проведено аналіз різних методів для оцінювання ризиків ІБ;

– виконано побудову моделі оцінювання загроз та ризиків ІБ при реалізації мобільних бізнес-рішень;

– розроблений програмний засіб здатний вести список ресурсів, загроз, вразливостей, контрзаходів, користувачів системи та проводити оцінку ризиків для кожного ресурсу підприємства;

– досліджено ризики та загрози ІБ при реалізації та використанні мобільних пристроїв. Для дослідження обрано кількісні методи оцінки ризиків;

– запропоновано підхід до оцінювання ризиків ІБ при реалізації та використанні бізнес-рішень. Визначено основні поняття підходу;

– спроектовано БД для оцінювання загроз та ризиків ІБ підприємства, побудовано логічну та фізичну моделі ІБ, створено програмну реалізація БД.

Вхідними даними є ймовірності реалізації загроз і вразливостей для кожного ресурсу, вартість ресурсів, що захищаються (оцінка втрат у разі виходу з ладу інформаційного ресурсу). Вихідними даними є кількісна та якісна оцінка для кожного ризику підприємства.

Для дослідженні використовувалися розроблений програмний продукт та вже існуючий програмний продукт «Гриф». В результаті проведеного дослідження можна зробити висновок про можливість використання даного програмного продукту для оцінки ризиків та загроз інформаційній безпеці на підприємстві.

Інформаційна система створена на платформі .NET у програмному продукті Microsoft Visual Studio 2010. Програмний продукт реалізував всі необхідні функції. Написано на мові програмування C#.

Розроблений програмний продукт може застосовуватися для оцінки ризиків ІБ організацій усіх сфер діяльності, так як він характеризує ІС з боку ризиків і відповідно може бути конкретизована під конкретну організацію. З іншого боку, враховуючи дуже динамічний розвиток автоматизації процесів розробки ПЗ, даний програмний продукт дозволяє адміністраторам ІБ, на відміну від розглянутих

прототипів, вносити доповнення до БД загроз та вразливостей, що дозволить оцінити ризики для мобільних пристроїв. Ступінь конкретизації залежить від рівня зрілості організації, специфіки її діяльності, необхідного рівня захищеності, моделі зловмисника та інших чинників. Тобто в кожному конкретному випадку програмний продукт може бути адаптовано під конкретні потреби підприємства з урахуванням специфіки його функціонування та ведення бізнесу.

Рівень точності одержуваної на виході оцінки залежить в першу чергу від повноти списку загроз і вразливостей, як основних складових ризику, точності оцінки інформаційних ресурсів, а також точності оцінки ймовірнісних характеристик реалізації загроз. Для оцінки цих характеристик може знадобитися залучення, як технічних фахівців, так і представників управління самої компанії, що дозволить надалі результативніше фінансувати і контролювати процес впровадження системи захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дослідження компанії IDC. URL: http://www.idc.com/ (дата звернення: 10.11.2019).
2. Дослідження компанії Gartner. URL: www.gartner.com/ (дата звернення: 11.11.2019)
3. Дослідження компанії Research & Branding Group. URL: http://www.rb.com.ua/ukr/ (дата звернення: 10.11.2019).
4. Гензерский И. В. Анализ угроз для мобильных устройств и способов их защиты / И. В. Гензерский, В. Н. Федорченко // Системи обробки інформації. - 2011. - № 7. - С. 68-71.
5. Астрахов А.М. Искусство управления информационными рисками. М:ДМК Пресс, 2010. 312 с.
6. Дослідження компанії G Data SecurityLabs. URL: http://ru.gdatasoftware.com/security-labs (дата звернення: 10.11.2019)
7. Доклад «Мобильные угрозы 2017/2019». URL: http://www.juniper.net/ru/ru/dm/interop/go/.(дата звернення: 10.11.2019).
8. McAfee Threats Report: First Quarter 2015. URL: http://www.mcafee.com /us/resources/reports/rp-quarterly-threat-q1-2015.pdf (дата звернення: 10.11.2019).
9. Сайт SecureList. URL: http://www.securelist.com/ru/analysis (дата звернення: 10.11.2019).
10. Дослідження компанії KRC Research. URL: http://www.krcresearch.com/selectReports.html (дата звернення: 10.11.2019).
11. ISO/IEC 27001:2005 “Information technology - Security techniques - Information security management systems - Requirements”.
12. Вишняков Я.Д. Общая теория рисков: учебное пособие для студентов ВУЗов. / Я.Д. Вишняков, Н.Н. Радаев. с 2-е изд., испр. М.: Издательский центр «Академия», 2008. 368 с.
13. Мохор В.В. Количественная оценка рисков безопасности информации на основе пробит-анализа. // “Реєстрація, зберігання і обробка даних”, Том 12, № 3, 2010. - С. 85-92.

14. Оксенюк В.Ю. Використання програмних засобів для оцінки та управління ризиками інформаційної безпеки. *Інформаційні моделі, системи та технології*: Праці VII наук.-техн. конф. (Тернопіль, 11-12 грудня 2019 р.) Тернопіль, 2019. С. 75.

15. Долмарев В. В. Энциклопедия безопасности информационных технологий, Методология создания систем защиты информации / В. В. Долмарев. - К.: ООО «ДС», 2001. - 688 с.

16. Галицкий А. Защита информации в сети - анализ технологий и синтез решений. - ДМКПресс, 2004. - 615 с.

17. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. / С. А. Петренко, С. В. Симонов - М.: Компания Айти; ДМКПресс, 2004. - 653 с.

18. Конеев И.Р. Информационная безопасность. / И.Р. Конеев, А.В. Беляев. - СПб.: БХВ-Петербург, 2003. - 752 с.

19. RiskWatch Обзор продукта. URL: http://www.riskwatch.com (дата звернення: 10.11.2019).

20. ГРИФ Обзор продукта/ URL: http:// www.dsec.ru/soft (дата звернення: 10.11.2019).

21. CRAMM Обзор продукта. URL: http://www.cramm.com (дата звернення: 10.11.2019).

22. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=40384&cat_id=38824 (дата звернення: 10.11.2019)

23. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?artid=40396&catid=38835. (дата звернення: 10.11.2019).

24. Практичні правила управління інформаційною безпекою. URL: http://www.npo- echelon.ru/common_files/gost/GOST-17799-2005.pdf. (дата звернення: 12.10.2019)

25. Управління інформаційною безпекою. Міжнародний стандарт. URL: http://www.securitycn.net/img/uploadimg/20070924/ 183844756.pdf. (дата звернення: 13.10.2019)

26. Предотвращение и мониторинг инцидентов связанных с вредоносным ПО. NIST 800-30 (стандарт США) URL: csrc.nist.gov/publications /nistpubs/800-30/sp800-30.pdf. (дата звернення: 11.10.2019)

27. Рубен А. Эффективная робота с СУБД. СПб.: Питер, 2009. 822 с.

28. Семенов И. SQL стандарт в СУБД MS SQL SERVER, ORACLE, VFP и ACCESS: манипулирование данными. М.: СДИ. 2006. 462 с.

29. Швецов В., Бази данных. М.:Apress 2008. 337 с.

30. Михеев Р. MS SQL Server 2005 для администраторов. СПб: БХВ-Петербург, 2007. 544 с.

31. Нейгел К. C# 2005 и платформа .NET 3.0 для профессионалов. М.: Диалектика, 2007. 426 с.

32. Закон України «Про охорону праці» від 14.10.1992 № 2695-12 // Відомості Верховної Ради України. 1992. - №49. - Ст. 669.

33. Закон України «Про охорону праці» від 02.06.2011 № 3458-17 (зі змінами) // Відомості Верховної Ради України. 2011. - №50. - Ст. 551.

34. Зеркалов Д.В. Безпека життєдіяльності та основи охорони праці. Навчальний посібник. К.: «Основа». 2016. 267 с.

35. Тарасова В.В. Екологічна статистика. Київ: Центр учбової літератури, 2008. 392 с.

Додаток А
Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »

11–12 грудня 2019 року

ТЕРНОПІЛЬ
2019