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 кібербезпеки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітній рівень)

на тему: *«Метод мінімізації ризиків інформаційної безпеки при побудові системи захисту інформації»*

Виконав: студент *VI* курсу, групи *СБм-61*

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Омелянюк Д.С.
підпис (прізвище та ініціали)

Керівник *Загородна Н.В.*
підпис (прізвище та ініціали)

Нормоконтроль *Кареліна О.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Метод мінімізації ризиків інформаційної безпеки при побудові системи захисту інформації // Дипломна робота ОР «Магістр» // Омелянюк Дмитро Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2019 // С. 108 , рис. – 21 , табл. – 20 , слайдів – 10 , додат. – .

Ключові слова: ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА ЗАХИСТУ, РИЗИК, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ, ТЕОРІЯ ІГОР, ДЕТЕРМІНОВАНА ГРА.

В роботі проведено огляд літературних джерел в області дослідження. Проведено порівняльний аналіз методів оцінки ризиків та класифікаційних моделей загроз та порушника. Визначено, що одним із основних етапів розробки політики безпеки на підприємстві є управління ризиками, що включає в себе методи їх оцінки та мінімізації. Запропоновано метод мінімізації ризиків інформаційної системи, що дозволяє формувати структуру системи захисту інформації з мінімальними значення ризику інформаційної безпеки. Використання математичного апарату теорії ігор, у тому числі максимінної стратегії, забезпечує отримання мінімального гарантованого значення ризику інформації, що відрізняє розроблений підхід від методів експертної оцінки. Розроблений підхід є гнучким, що дозволяє змоделювати поведінку порушників різного типу.

ANNOTATION

Method of information safety risk minimization at information protection system development // Thesis of the Master degree // Omelianiuk Dmytro// Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2019 // P.108 , Tables – , Fig. – , Diagrams – , Annexes. – , References – .

Keywords: INFORMATION SECURITY POLICY, PROTECTION SYSTEM, RISK, INFORMATION AND COMMUNICATION SYSTEM, OFFENDER MODEL, THREAT MODEL, GAME THEORY, DETERMINISTIC GAME.

The paper reviews literature sources in the field of research. A comparative analysis of risk assessment methods and classification models of threats and offenders is conducted. It has been determined that one of the main stages of enterprise security policy development is risk management, which includes methods of their assessment and minimization. The method of minimizing the risks of the information system is proposed, which allows to form the structure of the information security system with minimal values of the risk of the information security. The use of mathematical core of game theory, including the maximum strategy, ensures the minimum guaranteed value of information risk, which distinguishes the developed approach from the methods of expert evaluation. The developed approach is flexible, allowing to model the behavior of offenders of different types.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПІБ – політика інформаційної безпеки

АС – автоматизована система

ІКС – інформаційно комунікаційна система

КС – комп’ютерна система

НСД – несанкціонований доступ

ТЗІ – технічний захист інформації

ІТС – інформаційно телекомунікаційна система

КВІ – канали витоку інформації

ОС – операційна система

ПЗ – програмне забезпечення

СЗІ – система захисту інформації

ІБ – інформаційна безпека

ЗОТ - засоби обчислювальної техніки

СУІБ – система управління інформаційною безпекою.

ВСТУП

Примітна особливість нинішнього періоду – перехід від індустріального суспільства до інформаційного, в якому інформація стає більш важливим ресурсом, ніж матеріальні ресурси.

Інформація, що знаходиться на електронних носіях грає все більшу роль в житті сучасного суспільства. Уразливість такої інформації обумовлена цілою низкою чинників: величезні обсяги і можлива анонімність доступу, можливість "інформаційних диверсій". Все це робить завдання забезпечення захищеності інформації, розміщеної у комп'ютерному середовищі, набагато складнішою проблемою, ніж, скажімо, збереження таємниці традиційного поштового листування.

Проблема забезпечення захисту інформації є однією з найважливіших при побудові надійної інформаційної структури установи на базі автоматизованих систем.

Тому одним із основних етапів забезпечення інформаційної безпеки є розробка політики безпеки інформації. Головною метою політики безпеки інформації є забезпечення інформаційної безпеки, котра циркулює в рамках виробничої діяльності всіх підрозділів підприємства і збереження головних якостей інформації таких, як цілісність, конфіденційність та доступність. Управління ризиками є одним з важливих етапів розробки власної політики безпеки. Суть заходів управління ризиками полягає в тому, щоб оцінити їх розмір, виробити ефективні і економічні заходи зниження ризиків. Методи оцінки ризиків є доволі стандартизованими і описаними і міжнародних стандартах, а суть управління ризиками зводиться до того, що переконатися, що ризики знаходяться в прийнятних межах і залишаються такими. Тому актуальною задачею є дослідження методів мінімізації ризиків на основі побудованих експертних оцінок.

Таким чином, мета роботи – розробка методу мінімізації ризиків інформаційної безпеки при побудові системи захисту інформації для

забезпечення необхідного рівня захищеності з врахуванням обмежених витрат на систему захисту інформації.

З поставленої мети випливають такі задачі дослідження:

- зробити аналіз літературних джерел в області досліджень;
- дослідити математичні підходи для формування політики безпеки;
- побудувати модель загроз та порушника;
- розробити математичну модель у формі гри конфліктуючих сторін – захисника та зловмисника;
- побудувати методу мінімізації ризиків в залежності від виділених ресурсів.

Об'єкт дослідження – процес побудови системи безпеки підприємства

Предмет дослідження – моделі політики безпеки та методи оцінки і мінімізації ризиків на підприємстві

Методами дослідження є як загальнонаукові методи пізнання: порівняння, системний аналіз, так і спеціальні: методи математичного програмування, методи теорії ігор, методи оцінки ризиків, методи математичної статистики.

Наукова новизна: запропонована в роботі комплексна математична модель системи безпеки враховує не лише ймовірності настання загроз, а й ймовірності спрацювання тих чи інших засобів захисту при різних видах загроз.

Практичне значення роботи полягає в тому, що запропонований метод мінімізації ризиків є досить універсальним і може бути використаним для широкого кола організацій.

Апробація результатів роботи. Окремі результати роботи доповідались на VII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

1 ТЕОРЕТИЧНА ЧАСТИНА

1.1 Аналітичний огляд політики безпеки інформації

На даний момент, розвиток інформації у світі зростає із фундаментальною швидкістю, тому інформація завжди потребує захисту, від зловмисників котрі бажають змінити або знищити інформацію. Для забезпечення властивостей та зниженню ризиків інформації котра циркулює в АС використовують політику інформаційної безпеки.

Політика інформаційної безпеки – це набір вимог, правил обмежень рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора — організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

Крім того, певні вимоги (рекомендації) пред'являють галузеві або загальні, місцеві чи міжнародні стандарти. Зазвичай це виражається у вигляді зауважень зовнішніх аудиторів, які проводять перевірки діяльності підприємства. Відсутність політики викликає негативну оцінку, яка в свою чергу впливає на публічні показники підприємства — позиції в рейтингу, рівень надійності.

Метою політики безпеки інформації є впровадження та ефективне управління системою забезпечення інформаційною безпеки, спрямованою на:

- захист інформаційних активів;
- забезпечення стабільної діяльності організації;
- мінімізації ризиків інформаційної безпеки;

- створення позитивних для організації відносин з партнерами.

Щоб політика інформаційної безпеки доступно пояснювала свої цілі усім користувачам АС вона повинна бути документом першого рівня, її повинні розширювати і доповнювати інші документи (положення та інструкції), які вже будуть описувати щось конкретне, і це наглядно зображено на рисунку 1.1.

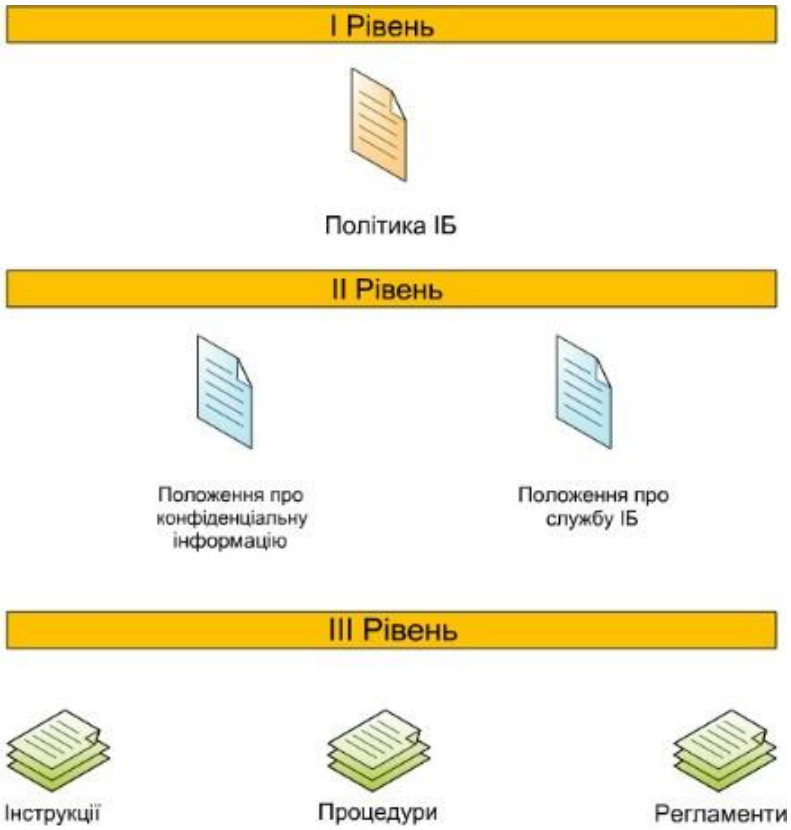

Рисунок 1.1 – Рівні документації

Політика безпеки інформації включає в себе:

- аналіз структури підприємства;
- модель загроз інформації, котра циркулює в АС;
- модель порушника інформації, котра циркулює в АС;
- нормативно-правове забезпечення.

Як правило, визначення політики безпеки зводиться до наступних практичних кроків:

1. Вибір національних і міжнародних керівних документів і стандартів в області ІБ, і визначення на їх основі основних вимог і положень політики ІБ компанії, включаючи:

- управління доступом до засобів обчислювальної техніки (ЗОТ), програмам і даним;
- антивірусний захист;
- питання резервного копіювання;
- проведення ремонтних і відновлювальних робіт;
- інформування про інциденти в області ІБ та ін.

2. Визначення підходів до управління інформаційними ризиками та прийняття рішення про вибір рівня захищеності ІС. Рівень захищеності відповідно до зарубіжними стандартами може бути мінімальним (базовим) або підвищеним. Цим рівням захищеності відповідають мінімальний (базовий) або повний варіант аналізу інформаційних ризиків.

3. Структуризація контрзаходів щодо захисту інформації за такими основними рівнями: нормативно-правовий, організаційно-управлінський, технологічний і апаратно-програмний.

4. Визначення порядку сертифікації та акредитації ІС на відповідність стандартам в області ІБ. Визначення періодичності проведення нарад за тематикою ІБ на рівні керівництва, включаючи періодичний перегляд положень політики ІБ, а також порядок навчання всіх категорій користувачів інформаційної системи з питань ІБ.

5. Визначення меж системи управління інформаційною безпекою і конкретизація цілей її створення. На цьому етапі визначаються межі системи, для якої повинен бути забезпечений режим ІБ. Відповідно, система управління ІБ будуватися саме в цих межах.

6. Постановка завдання оцінки ризиків обґрунтовуються вимогами до методики оцінки інформаційних ризиків компанії. Вибір підходу залежить від рівня вимог, що пред'являються в організації до режиму інформаційної безпеки, характеру взятих до уваги загроз (спектра дії загроз) і ефективності потенційних

контрзаходів щодо захисту інформації. Розрізняють мінімальні або базові, а також підвищені або повні вимоги до режиму ІБ. Мінімальним вимогам до режиму ІБ відповідає базовий рівень ІБ. Такі вимоги застосовуються, як правило, до типових проектних рішень. Існує ряд стандартів і специфікацій, в яких розглядається мінімальний (типовий) набір найбільш ймовірних загроз, таких як: віруси, збої устаткування, несанкціонований доступ тощо. Для нейтралізації цих загроз обов'язково повинні бути прийняті контрзаходи незалежно від ймовірності їх здійснення і уразливості ресурсів.

7. Управління ризиками. Розробляється деяка стратегія управління ризиками. Можливі такі підходи до управління інформаційними ризиками компанії:

-Зменшення ризиків. Більшість ризиків можуть бути істотно зменшені шляхом використання досить простих і дешевих контрзаходів.

- Ухилення від ризику. Від деяких класів ризиків можна ухилитися.

- Зміна характеру ризику. Якщо не вдається ухилитися від ризику або ефективно його зменшити, можна прийняти деякі заходи страховки.

- Прийняття ризику. Більшість ризиків не можуть бути зменшені до незначної величини. На практиці, після прийняття стандартного набору контрзаходів, ряд ризиків зменшується, але залишається все ще значним. Необхідно знати залишкову величину ризику. В результаті виконання етапу для інформаційних ризиків компанії, що беруться до уваги, повинна бути запропонована стратегія управління ризиками.

8. Вибір контрзаходів, що забезпечують режим ІБ. На цьому етапі обґрунтовано вибирається комплекс різних контрзаходів щодо захисту інформації, структурованих по нормативно-правовому, організаційно управлінському, технологічному і апаратно-програмному рівнях забезпечення інформаційної безпеки. Надалі пропонований комплекс контрзаходів реалізується відповідно до обраної стратегії управління інформаційними ризиками. Якщо проводиться повний варіант аналізу ризиків, для кожного

ризику додатково оцінюється ефективність комплексу контрзаходів щодо захисту інформації.

9. Аудит системи управління ІБ. Перевіряється відповідність обраних контрзаходів щодо захисту інформації цілям і задачам бізнесу, декларованим в політиці безпеки компанії, проводиться оцінка залишкових ризиків і, в разі необхідності, оптимізація ризиків.

1.2 Світові стандарти із захисту даних в АС

Критерії безпеки комп'ютерних систем Міністерства оборони США, що отримали назву «Оранжева книга» (за кольором обкладинки), були розроблені Міністерством оборони США в 1983 році (перша версія) з метою визначення вимог безпеки, які висуваються до апаратного, програмного і спеціального забезпечення комп'ютерних систем і розробки відповідної методології аналізу політики безпеки, що реалізується в КС військового призначення.

У цьому документі були вперше нормативно визначене таке поняття, як «політика безпеки». Відповідно до «Оранжевої книги» безпечна КС – це система, яка підтримує керування доступом до оброблюваної в ній інформації таким чином, що відповідно авторизовані користувачі або процеси, що діють від їх імені, отримують можливість читати, писати, створювати і видаляти інформацію. Запропоновані в цьому документі концепції захисту і набір функціональних вимог послужили основою для формування інших стандартів безпеки інформації.

В «Оранжевій книзі» запропоновано три категорії вимог щодо безпеки: політика безпеки, аудит та коректність, у рамках яких сформульовано шість базових вимог безпеки. Перші чотири вимоги спрямовані безпосередньо на забезпечення безпеки інформації, дві інші – на якість самих засобів захисту:

- Вимога 1 (політика безпеки) – система має підтримувати точно визначену політику безпеки, можливість доступу до об'єктів повинна визначатися на основі їх ідентифікації і набору правил керування доступом;

- Вимога 2 (мітки) – кожен об’єкт повинен мати мітку, що використовується як атрибут контролю доступу;

- Вимога 3 (ідентифікація та аутентифікація) – всі суб’єкти повинні мати унікальні ідентифікатори; контроль доступу здійснюється на основі ідентифікації та аутентифікації суб’єкта та об’єкта доступу;

- Вимога 4 (реєстрація й облік) – всі події, що мають відношення до безпеки, мають відстежуватися і реєструватися в захищеному протоколі;

- Вимога 5 (контроль коректності функціонування засобів захисту) – засоби захисту перебувають під контролем засобів перевірки коректності, засоби захисту незалежні від засобів контролю коректності;

- Вимога 6 (безперервність захисту) – захист має бути постійним і безперервним у будь-якому режимі функціонування системи захисту і всієї системи в цілому. Наступними після «Оранжевої книги» були розроблені «Критерії безпеки інформаційних технологій» (далі «Європейські критерії»). Вони були вперше опубліковані в 1991 році, а розроблені чотирма європейськими країнами: Францією, Німеччиною, Нідерландами та Великобританією.

«Європейські критерії» розглядають такі основні завдання інформаційної безпеки:

- захист інформації від НСД з метою забезпечення конфіденційності;

- забезпечення цілісності інформації шляхом захисту її від несанкціонованої модифікації або знищення;

- забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту і рівня адекватності їх реалізації.

1.3 Головні принципи та етапи захисту від загроз в АС

Загальний аналіз проблем організовування захисту від будь-яких загроз дає можливість визначити 4 головні принципи та етапи заходів:

- організація зовнішніх рубіжів безпеки з метою своєчасного виявлення загроз;
- організація протидії загрозам та їх блокування, тобто зупинення та локалізації загроз під час їх реалізації;
- забезпечення нейтралізації та ліквідації загроз, а також подолання наслідків загроз, які не вдалося блокувати;
- попередження загроз, тобто аналіз відомих загроз та впровадження відповідних запобіжних заходів.

Стосовно автоматизованих (комп'ютерних) систем (АС) ці принципи та етапи дають можливість також визначити 4 етапи та види захисту від загроз для електронних інформаційних ресурсів АС, які циклічно повторюються з метою постійного оновлення та підвищення ефективності заходів і засобів захисту.

Етап виявлення. На організаційному рівні – це використання заходів розвідки та дезінформації. На інженерно-технічному рівні – це впровадження засобів ТЗІ, які поділяються на:

- активні засоби захисту: охоронна сигналізація та відеоспостереження;
- пасивні засоби захисту: закриття вікон та встановлення на них грат, закриття та опечатування дверей, системних блоків, роз'ємів технічних засобів АС тощо;
- комплексні засоби захисту (органічне поєднання всіх груп).

Етап зупинення. Ці заходи забезпечують апаратно-програмне блокування спроб несанкціонованого доступу (НСД) порушника (хакера) до інформації в АС або ураження системи вірусами за допомогою спеціальних апаратних комплексів та програмних засобів захисту інформації. Для цього в АС встановлюються міжмережові екрани, файерволи (брандмауери), антивірусні програмні засоби та спеціальні комплекси засобів захисту інформації від НСД.

Зазначимо, що ці заходи можуть бути спрямовані на документування методів НСД до АС для наступного дослідження їх; збереження слідів правопорушення; взаємодію (у разі необхідності) з державними правоохоронними органами щодо виявлення та розкриття правопорушення (в тому числі за готування до злочину і за замах на злочин); сприяння притягненню винних до відповідної відповідальності (кримінальної, адміністративної, цивільно-правової, дисциплінарної).

Етап нейтралізації. На організаційно-правовому рівні – це дисциплінарне або адміністративне (кримінальне) розслідування правопорушення (злочину) та притягнення винних до відповідальності. На апаратно-програмному рівні – це подолання наслідків реалізації загроз у разі порушень:

- технологічих процесів – їх відновлення за допомогою плану аварійного відновлення та проведення ремонтних заходів;
- операційної системи та програмних засобів – їх відновлення за допомогою інсталяційних файлів (дисків);
- інформаійних ресурсів – їх відновлення за допомогою резервних і архівних копій, які зберігаються на зовнішніх носіях.

Етап попередження. На організаційному рівні – це проведення аналізу відомих загроз, пошук нових запобіжних заходів, оновлення політики безпеки, навчання та тренування персоналу. На технічному рівні – це застосування пасивних засобів захисту: штор на вікнах, систем екранування, заземлення та зашумлення, а також оновлення та впровадження нових систем і засобів ТЗІ.

1.4 Ризики та методи їх оцінки

Порушення основних властивостей інформації може стати серйозною загрозою для організацій в даний час. Інформацію важче контролювати і вона піддається зростаючому числу загроз і вразливостей, в тому числі комп'ютерного шахрайства, шпигунству, саботажу, вандалізму, пожежі або повені. Інформаційні ресурси, як і матеріальні, володіють якістю та кількістю,

мають собівартість і ціну. Оцінка ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Її використовують для визначення масштабу загроз безпеці інформації та ймовірності реалізації загрози.

У роботі визначимо ризик порушення ІБ як потенційну можливість використання вразливостей активів загрозами ІБ для заподіяння шкоди, яка вимірюється з урахуванням ймовірності реалізації загроз ІБ і величини збитку від реалізації загроз ІБ. Таким чином, в представленому визначенні ризик ІБ є функція як мінімум двох змінних: величини потенційного (негативного) впливу–шкоди для організації і ймовірності реалізації загрози ІБ. Найчастіше функцію рахують як добуток втрат від порушення конфіденційності, цілісності, автентичності або доступності інформаційних ресурсів на імовірність такого порушення. Друга величина є комплексним показником. Аналіз ризиків–це процедури виявлення факторів ризиків ІБ і оцінки їх вагомості. Аналіз ризиків ІБ включає оцінку ризиків і методи зниження ризиків або зменшення пов'язаних з ними несприятливих наслідків. При аналізі спочатку проводиться виявлення відповідних факторів і оцінка їх вагомості, повнота виявлених чинників збільшує якість і точність прогнозованих ризиків. До таких факторів належать безліч активів, вразливостей і загроз. Основна мета створення класифікації загроз ІБ–повна, детальна класифікація, що описує всі існуючі загрози ІБ і яка найбільш застосовна для аналізу ризиків реальних інформаційних систем.

Ризики інформаційної безпеки розглядають як частину бізнес-ризиків та обробляють схожим чином.

Оцінка ризику полягає у визначенні його рівня (якісної або кількісної величини) і порівнянні цього рівня з максимально допустимим (прийнятним) рівнем, а також з рівнем інших ризиків. Рівень ризику визначається шляхом комбінування двох величин: ймовірності події та розмірів його наслідків. Подія полягає в реалізації загрози, що використовує уразливість активу для впливу на цей актив і порушення його безпеки. Всі відомі методики оцінки ризиків можна розділити на:

- методики, що використовують оцінку ризику на якісному рівні (наприклад, за шкалою «високий», «середній», «низький»), до таких методик, зокрема, відноситься FRAP;

- кількісні методики (ризик оцінюється через числове значення, наприклад, розмір очікуваних річних втрат)

Проаналізуємо три найвідоміші світові методики управління ризиками ІБ, які можна застосувати для аналізу ризиків ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ, визначимо переваги та недоліки кожної з них. Аналізу підлягають: методика оцінки NIST800-30 [4], методика CRAMM [5] та методика OCTAVE [6]. Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози [7] .Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій. Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях 800-30, охоплює широке коло завдань, що пов’язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий “жорсткий” механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність. Алгоритм цієї методики зображено на рис. 1.2

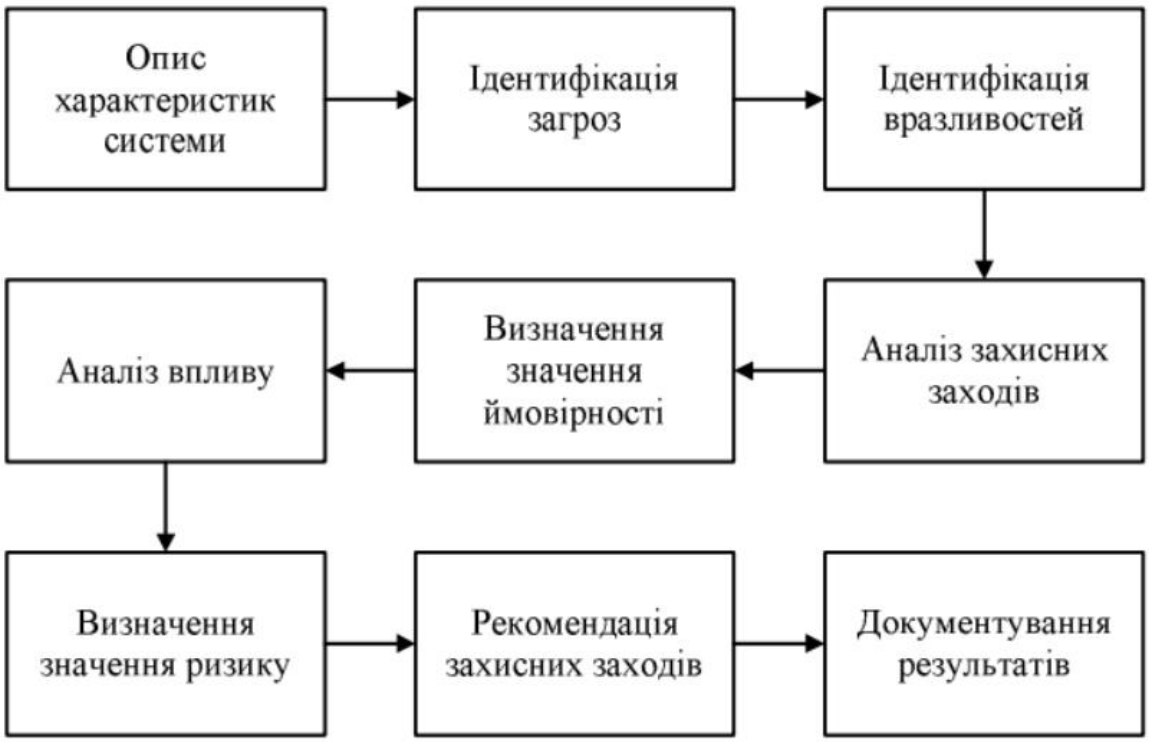

Рисунок 1.2 – Алгоритм методики управління ризиками

Використання такої методики передбачає такі етапи:

- опис характеристик системи;
- ідентифікація загроз;
- ідентифікація вразливостей;
- аналіз наявних засобів/заходів захисту;
- визначення значення ймовірності;
- аналіз впливу.
- визначення значення ризику;
-вибір засобів /заходів захисту;
-документування отриманих результатів.

Наступною методикою є методика CRAMM (CCTA Risk Analysi sand Managment Method), яку розробило Агентство з комп’ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) заподанням Британського уряду і яка прийнята за державний стандарт. Цю методику використовують, починаючи з 1985 року, державні та комерційні організації

Великобританії. За цей час CRAMM набула популярності у всьому світі. Фірма Insight Consulting Limited займається розробленням і супроводом однойменного програмного продукту, що реалізує метод CRAMM [8]. В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (CommercialProfile), для державних організацій –державний профіль (Governmentprofile). Державний варіант профілю також дає змогу проводити аудит нав ідповідність вимогам американського стандарту ITSEC.

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: “Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?” На другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання 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 [8]. Алгоритм методики CRAMM подано на рис. 1.3

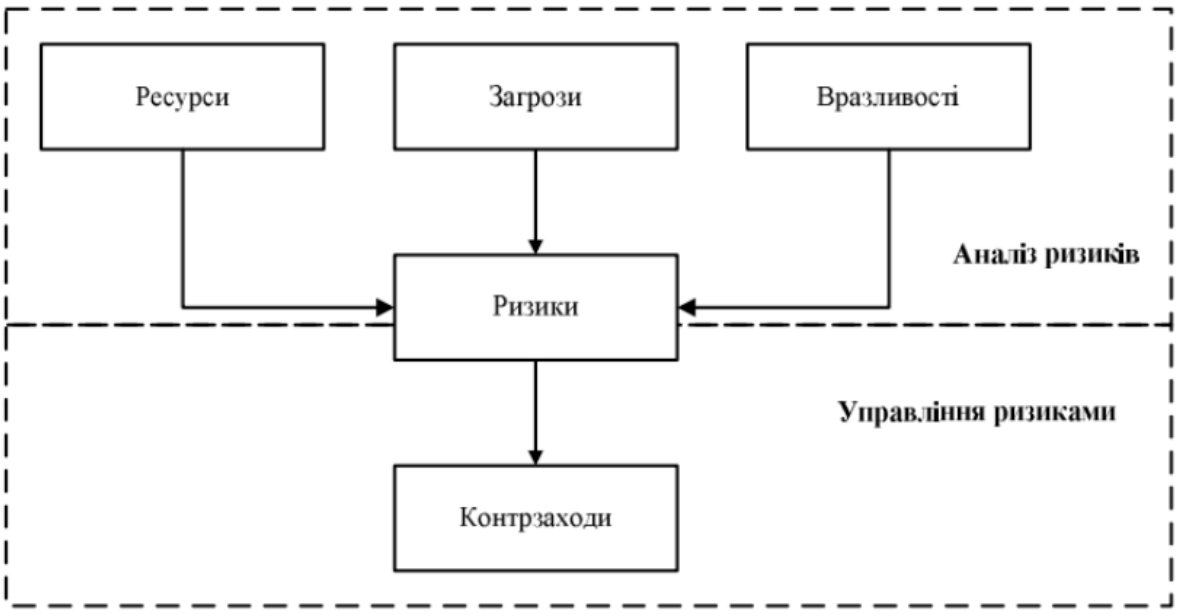

Рисунок 1.3 – Алгоритм методики управління ризиками CRAMM

Методика OCTAVE (Operationally Critical Threat, Assetand Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей. Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності[9]. Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів(workshops).Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи [9]. На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки. На другому етапі проводиться технічний аналіз вразливостей систем організації щодо загроз, чиї профілі

розроблено на попередньому етапі, який містить ідентифікацію наявних вразливостей компанії та оцінювання їх величини. На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням вразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків.

Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ. Алгоритм цієї методики зображено на рис.1.4.

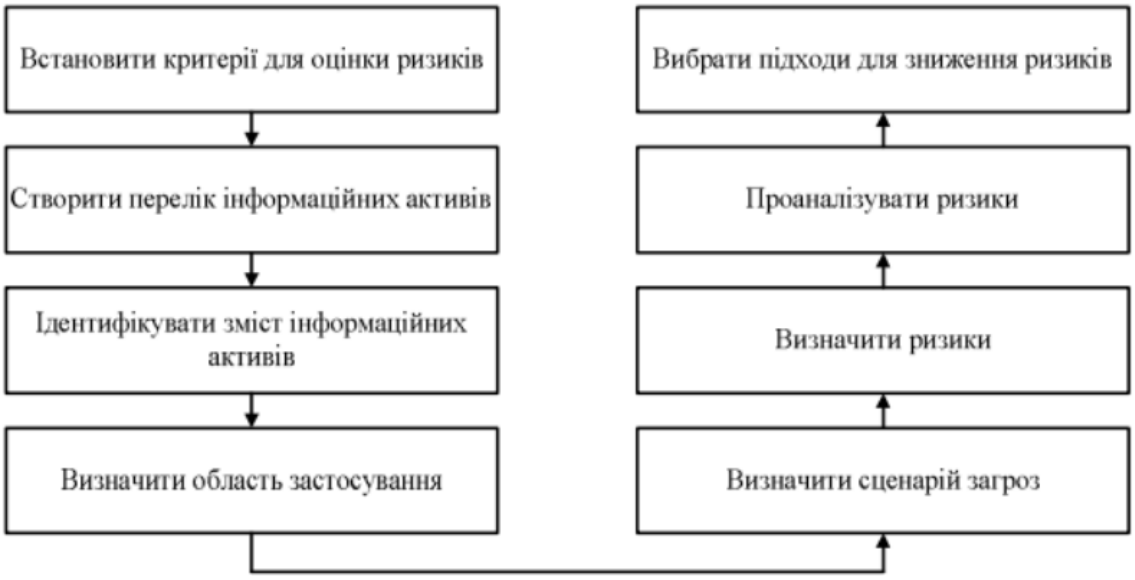

Рисунок 1.4 – Алгоритм методики управління ризиками OCTAVE

Очевидно, що кожна методика має свої переваги і недоліки. Тому важливо комбінувати існуючі та створювати нові методики з метою мінімізації ризиків.

2 МОДЕЛІ ЗАГРОЗ ТА ПОРУШНИКА

2.1 Модель загроз інформації, котра циркулює в АС

Після проведення обстеження середовищ АС необхідно визначити всі можливі потенційні загрози для АС.

Походження загроз може бути випадковим і навмисним. Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в АС в процесі її функціонування. Найбільш відомими подіями цього плану є відмови, збої, помилки, стихійні лиха та сторонній вплив. Зміст перерахованих подій (за виключенням стихійних лих, зміст яких незрозумілий) може визначатись в рамках наступних термінів:

- відмова – порушення працездатності якого-небудь елемента системи, що призводить до неможливості виконання нею основних своїх функцій;
- збій – тимчасове порушення працездатності якого-небудь елемента системи, наслідком чого може бути неправильне виконання ним у цей момент своєї функції;
- помилка – неправильне (разове або систематичне) виконання елементом однієї або декількох функцій, що відбувається внаслідок специфічного (постійного або тимчасового) його стану;
- сторонній вплив – негативний вплив на систему в цілому або окремі її компоненти, що є наслідком деяких явищ, які мають місце в середині або ззовні системи.

Навмисне походження загроз зумовлене зумисним втручанням зловмисника. Вразливості, що передують появі загрози можуть бути об'єктивними (погана якість чи недостатність елементів системи) і суб'єктивними. До останніх відносяться діяльність розвідувальних органів іноземних держав, промислове шпигунство, діяльність кримінальних елементів, дії недобросовісного персоналу АС.

Перераховані різновиди передумов інтерпретуються таким чином:

- кількісна недостатність – фізична нестача одного або декількох елементів системи, що викликає порушення технологічного процесу обробки даних і / або перевантаження наявних елементів;

- якісна недостатність – недосконаліть конструкції (організації) елементів системи, в силу цього можуть з'являтися можливості випадкового або навмисного негативного впливу на оброблювану або збережену інформацію.

Джерело загрози – це безпосередній їх генератор або носій. Таким джерелом можуть бути люди, технічні засоби, моделі (алгоритми), а також – програми, технологічні схеми обробки, зовнішнє середовище.

Спробуємо тепер, спираючись на наведену системну класифікацію загроз безпеки інформації, визначити повне безліч погроз, потенційно можливих у сучасних автоматизованих системах. При цьому ми повинні врахувати не лише всі відомі (раніше проявлялися) загрози, але й такі загрози, які раніше не виявлялися, але потенційно можуть виникнути при застосуванні нових концепцій архітектурного побудови АС і технологічних схем обробки інформації.

Всі можливі канали витоку інформації (КВІ) можна класифікувати за двома критеріями: необхідністю доступу до елементів ІТС для реалізації того чи іншого КВІ і залежністю появи КВІ від стану ІТС.

Згідно з першим критерієм КВІ можуть бути класифіковані на такі, що:

- не потребують присутності(доступу). Це означає, що секретною інформацією можна заволодіти віддалено (для прикладу, шляхом візуального спостереження через вікна приміщень ІТС чи віддаленого стеження);

- потребують присутності в приміщенні ІТС. Тут теж можливих два випадки, такі канали можуть бути непомітними і не вимагати певних дій (наприклад, візуальний перегляд зображень на екранах моніторів або документів на паперових носіях), а які можуть накласти відбиток та залишитись помітними в ІТС (наприклад, викрадення документів або машинних носіїв з цінною інфорацією).

За другим критерієм КВІ поділяються на:

- ті, які існують незалежно від того, в якому стані перебуває ІТС (наприклад, викрадати носії інформації можна незалежно від того, в робочому стані знаходяться АС чи ні);

- існуючі тільки в робочому стані ІТС (наприклад, сторонні електромагнітні випромінювання та наведення).

Наведено орієнтовну характеристику каналів несанкціонованого отримання інформації виділених нами класів:

1-го класу – канали, які проявляються безвідносно до обробки інформації і без доступу зловмисника до елементів системи. Сюди може бути віднесено підслуховування розмов, а також провокування на розмови осіб, що мають відношення до ІТС, і використання зловмисником візуальних, оптичних та акустичних засобів.

2-го класу – канали, які у процесі обробки інформації без доступу зловмисника до елементів ІТС. Сюди можуть бути віднесені електромагнітні випромінювання різних пристроїв ІТС, апаратури та ліній зв'язку, паразитні наведення в ланцюгах харчування, телефонних мережах, системах теплопостачання, вентиляції тощо.

3-го класу – канали, які проявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІТС, але без зміни останніх. До них відносяться всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів.

4-го класу – канали, які у процесі обробки інформації з доступом зловмисника до елементів ІТС, але без зміни останніх. Сюди може бути віднесено запам'ятовування і копіювання інформації в процесі обробки, використання програмних пасток тощо.

5-го класу – канали, які проявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІТС і зі зміною програмних або апаратних засобів. Серед цих каналів: підміна і розкрадання носіїв інформації й апаратури,

включення до програм блоків типу троянський кінь, комп'ютерний черв'як тощо.

6-го класу – канали, з доступом зловмисника до елементів ІТС і зі зміною останніх. Сюди може бути віднесено незаконне підключення до апаратури та ліній зв'язку).

На підставі Акту обстеження та Моделі порушника політики безпеки в СЗІ розробляється «Модель загроз для інформаційних ресурсів в ІТС», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ. Модель загроз має містити абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз для інформації, яка потребує захисту.

Модель загроз повинна визначити:

- перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

- перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу.

Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
- збої та відмови у роботі технічних або програмних засобів (ПЗ) ІТС;
- наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);
- помилки персоналу (користувачів) ІТС під час експлуатації;
- навмисні дії (спроби) потенційних порушників.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, котрі стають відмов окремих компонентів чи ІТС в цілому, руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);
- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціалізація виробничих чи технологічних процесів, які можуть зумовити незворотні зміни та втрату інформації (наприклад, форматування носіїв інформації); – неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв тощо;
- будь-які дії, що можуть стати причиною втрати конфіденційності, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);
- наслідки некомпетентного застосування засобів захисту тощо.

Навмисними загрозами суб’єктивної природи, спрямованими на дезорганізацію роботи ІТС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

- порушення цілісності фізичного середовища ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);

- порушення режимів функціонування ІТС (обладнання і ПЗ);

- впровадження та використання комп’ютерних вірусів, закладних (апаратних і програмних) пристроїв, інших засобів розвідки;

- використання (шантаж, підкуп тощо) персоналу ІТС з метою отримання винагород;

- крадіжки носіїв інформації;

- несанкціоноване копіювання носіїв інформації;

- читання залишкової інформації з оперативної пам’яті ЕОТ, зовнішніх накопичувачів;

- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;

- неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, аналіз трафіку тощо;

- впровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити, на порушення яких властивостей інформації або ІТС вона спрямована:

- загрози конфіденційності – несанкціоноване ознайомлення з інформацією;

- загрози цілісності – несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;

- загрози доступності – порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача);

- загрози спостережності та керованості ІТС – відмова в ідентифікації, автентифікації та реєстрації небезпечних дій;

Джерела виникнення (які внутрішні або зовнішні суб’єкти ІТС можуть нести загрозу):

- персонал ІТС;
- технічні засоби ІТС;
- моделі, алгоритми, програми ІТС;
- технологія функціонування ІТС;
- зовнішнє середовище;

Можливі способи здійснення (механізм реалізації) загроз:

- шляхом підключення до апаратури та ліній зв’язку;
- маскування під зареєстрованого користувача;
- подолання заходів захисту з метою використання інформації або нав’язування хибної інформації;
- застосування закладних пристроїв чи програм, вкорінення комп’ютерних вірусів.

Опис моделі загроз (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації), має бути викладений настільки детально, щоб дозволяти (на етапі аналізу ризиків, пов’язаних з реалізацією загроз для інформації в ІТС) однозначне визначення як збитків, що завдаються у випадку успішної реалізації загрози, так і ймовірності реалізації загрози (здійснення атаки) в певний спосіб. Модель загроз можна відобразити у вигляді таблиці 2.1:

Таблиця 2.1 – Модель загроз

№	Потенційні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
	1. Загрози об’єктивної природи				
1.1.	Стихійні явища (пожежа, аварії)				
1.2.	Збої та відмови системи електроживлення				
1.3.	Збої та відмови обчислювальної техніки				
1.4.	Збої, відмови та пошкодження носіїв інформації				
1.5.	Збої та відмови програмного забезпечення				
	2. Загрози суб’єктивної природи				
2.1	Зовнішні загрози				
2.1.1	Несанкціоноване підключення до технічних засобів				
2.1.2	Несанкціоноване підключення до каналів звязку				
2.1.3	Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду документів				
2.1.4	Несанкціоноване перехоплення інформації за рахунок витоку інформації за рахунок ПЕМВН				
2.1.5	Несанкціонований перегляд інформації за рахунок візуально- оптичного каналу				
2.2	Порушення нормальних режимів роботи				
2.2.1	Зараження системи комп’ютерними вірусами				
2.2.2	Втрата (розголошення) засобів розмежування доступу (паролів), магнітних носіїв інформації та резервних копій				
2.2.3	Несанкціоноване внесення змін у технічні засоби, програмне забезпечення, компоненти інформаційного забезпечення тощо				
2.2.4	Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення				

Продовження таблиці 2.1

2.2.5	Пошкодження носіїв інформації				
2.2.6	Вхід у систему недопущених осіб (подолання систем захисту)				
2.3	Помилки персоналу				
2.3.1	Помилки користувачів (впровадження і використання програм, що не є необхідними для виконання службових обов’язків; запуск програм, здатних викликати критичні зміни в системі)				
2.3.2	Помилки адміністраторів (неправильне конфігурування та адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту).				

Розрахунок загроз з урахуванням 3-х рівнів ризиків і збитків:

- високий – якщо реалізація загрози надає великих збитків (3 бали);
- середній – якщо реалізація загрози надає помірних збитків (2 бали);
- низький – якщо реалізація загрози надає незначних збитків (1 бал).

2.2 Модель порушника

На підставі Акту обстеження та визначення загроз для ІТС СЗІ розробляє «Модель порушника безпеки інформації в ІТС», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту. Модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо. Як порушник розглядається особа, яка може одержати несанкціонований доступ (НСД) до роботи з включеними до складу ІТС засобами.

Модель порушника повинна визначати:

- можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;
- категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник;
- припущення про кваліфікацію порушника; – припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Порушники спочатку поділяються на дві основні групи: зовнішні та внутрішні.

Зовнішніх порушників можна розділити на:

- добре озброєну та технічно оснащену групу, що діє зовні швидко і напролом;
- поодиноких порушників, що не мають допуску на об'єкт і намагаються діяти потайки й обережно, так як вони усвідомлюють, що сили реагування мають перед ним переваги.

Сторонні особи, що можуть бути порушниками:

- клієнти (представники організацій, громадяни); – відвідувачі (запрошені з якого-небудь приводу);
- представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо);
- представники конкуруючих організацій (іноземних служб) або особи, що діють за їх завданням;
- особи, які випадково або навмисно порушили пропускний режим (без мети порушити безпеку);
- будь-які особи за межами контрольованої зони.

Потенціальних внутрішніх порушників можна розділити на:

- допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєво важливого центру ІТС;
- основний персонал, що допущений до життєво-важливого центру (найбільш небезпечний тип порушників);
- співробітників служби безпеки, які часто формально не допущені до життєво важливого центру ІТС, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

Серед внутрішніх порушників можна виділити такі категорії персоналу:

- користувачі (оператори) системи;
- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки та супроводження програмного забезпечення (прикладні та системні програмісти);
- технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти ІТС);
- співробітники служби безпеки;
- керівники різних рівнів та посадової ієрархії.

Можна виділити також 3 основних мотиви порушень: безвідповідальність, самоствердження та з корисною метою.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості. Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки ІТС може бути викликано корисливим інтересом користувача ІТС. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для несанкціонованого доступу до інформації в ІТС.

Усіх порушників можна класифікувати за рівнем знань про ІТС:

- знає функціональні особливості ІТС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

- має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням;

- знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (методам та засобам, що використовуються):

- застосовує чисто агентурні методи отримання відомостей;

- застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути тайком пронесені крізь пости охорони;

- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

За часом дії:

- у процесі функціонування (під час роботи компонентів системи);

- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів);

- як у процесі функціонування, так і в період неактивності системи.

За місцем дії:

- без доступу на контрольовану територію організації;

- з контрольованої території без доступу до приміщень та споруджень; – усередині приміщень, але без доступу до технічних засобів;

- з робочих місць кінцевих користувачів (операторів);

- з доступом у зону даних (баз даних, архівів тощо);

- з доступом у зону управління засобами забезпечення безпеки.

Враховуються також такі обмеження та припущення про характер дій можливих порушників:

- робота з підбору кадрів і спеціальні заходи утруднюють можливість створення коаліцій порушників, тобто злочинного угрупування (змови) і цілеспрямованих дій по подоланню системи захисту двох і більше порушників;
- порушник, плануючи спробу НСД, приховує свої несанкціоновані дії від інших співробітників;
- НСД може бути наслідком помилок користувачів, адміністраторів, а також хиб прийнятої технології обробки інформації тощо.

Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про ІТС і засоби захисту. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

За результатами формування моделі порушника обов'язково повинні бути визначені: імовірність реалізації загрози, своєчасність виявлення та відомості про порушення.

Слід зауважити, що всі злочини, зокрема і комп’ютерні, здійснюються людиною. Користувачі ІТС, з одного боку, є її складовою частиною, а з іншого – основною причиною і рухаючою силою порушень і злочинів. Отже, питання безпеки захищених ІТС фактично є питанням людських відносин та людської поведінки.

Модель порушників можна відобразити у вигляді таблиці, наприклад таблиці 2.2.

Для побудови моделі використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них вказується в дужках і оцінюється за чотирьох бальною шкалою.

Таблиця 2.2 – Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загрози
	Внутрішні по відношенню до ІТС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІТС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб “під прикриттям”	4

Існують різноманітні класифікації порушника за мотивами здійснення порушень (табл. 2.3), за рівнем кваліфікації та обізнаності щодо ІТС (табл.2.4), за показником можливостей використання засобів та методів подолання системи захисту (табл. 2.5), за часом дії (табл.2.6) та за за місцем дії (табл. 2.7). Для кожного класифікаційного рівня визначено відповідний рівень ризику.

Таблиця 2.3 – Моделі порушника за мотивами здійснення порушень

Позна-чення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок (ПЗ4)	4

Як показую дослідження, левова частка порушень безпеки відбувається саме з корисливого інтересу.

Таблиця 2.4 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позна-чення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.5 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 2.6. – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 2.7 – Специфікація моделі порушника за місцем дії

Позна-чення	Характеристика місця дії порушника	Рівень загрози
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Виведемо два варіанти сумарного рівня загроз для окремих категорій можливих порушників:

- внутрішній порушник «ПВ» – варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов’язків;
- зовнішній порушник «ПЗ4»– варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій метою модифікації або викрадення інформації.

Таблиця 2.8 – Модель зовнішнього порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
прибиральник	ПВ1	М1	К1	З1	Ч4	Д1	9
	1	1	1	1	4	1	
	ПЗ4	М4	К4	З4	Ч4	Д1	21
	4	4	4	4	4	1	

Продовження таблиці 2.8

електрик	ПВ1	М1	К1	З1	Ч1	Д1	8
	1	1	1	1	3	1	
	ПЗ4	М4	К4	З4	Ч1	Д1	20
	4	4	4	4	3	1	
технік	ПВ2	М1	К2	З1	Ч4	Д3	12
	2	1	2	1	4	2	
	ПЗ4	М4	К4	З4	Ч4	Д3	22
	4	4	4	4	4	2	
користувач	ПВ3	М1	К2	З1	Ч3	Д2	11
	2	1	2	1	3	2	
	ПЗ4	М4	К4	З4	Ч3	Д2	21
	4	4	4	4	3	2	
адміністратор	ПВ4	М1	К4	З1	Ч4	Д4	17
	3	1	4	1	4	4	
	ПЗ4	М4	К4	З4	Ч4	Д4	24
	4	4	4	4	4	4	
безпека	ПВ5	М1	К1	З1	Ч4	Д3	14
	4	1	1	1	4	3	
	ПЗ4	М4	К4	З4	Ч4	Д3	23
	4	4	4	4	4	3	

Таблиця 1.9 – Модель внутрішнього порушника

Категорія порушника «ПВ»	Мотив пору-шення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можли-вості за часом дії	Можли-вості за місцем дії	Сума загроз
Служба безпеки	М1	К1	З1	Ч4	Д3	14
Адміністратор ІТС	М1	К4	З1	Ч4	Д4	17
Користувач	М1	К2	З1	Ч3	Д2	11
Технік ІТС	М1	К2	З1	Ч4	Д3	12
Електрик	М1	К1	З1	Ч1	Д1	8
Прибиральник	М1	К1	З1	Ч4	Д1	9

З таблиці 1.9 видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації становить адміністратор ІКС. Тому організація роботи цієї особи повинна бути найбільш контрольованою.

Те, що основною загрозою є персонал ІКС, підтверджують і дані, опубліковані у 2010 році американським інститутом комп′ютерної безпеки (Сан-Франциско, штат Каліфорнія), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- несанкціонований доступ – 2 %
- ураження вірусами – 3 %;
- технічні відмови апаратури мережі – 20 %;
- цілеспрямовані дії персоналу – 20 %;
- помилки персоналу (недостатній рівень кваліфікації) – 55%.

Таким чином, основною потенційною загрозою для інформації в ІТС слід вважати цілеспрямовані або випадкові деструктивні дії персоналу, оскільки вони становлять 75 % усіх випадків.

2.3 Причини порушення інформаційної безпеки

Сформована практика дослідження випадків порушення безпеки, що приділяє основну увагу методам і засобам подолання захисту, має істотний недолік – відштовхуючись від дій зловмисника, вона фактично являє собою лише аналіз технології подолання засобів захисту і не дозволяє виявити недоліки засобів забезпечення безпеки.

Крім того, подібний підхід відразу розділяє усі випадки порушення безпеки на навмисні, що класифікуються за способами подолання захисту, і ненавмисні, зумовлені помилками, закладеними б самій АС при її розробці та експлуатації. Однак, здається цілком прийнятною і дуже прагматична точка зору – важливі сам факт порушення безпеки і ті заходи, яких необхідно вживати для запобігання таким порушенням, а їхня навмисність не має значення. З цього погляду можливість успішних дій зловмисника, як і передумови випадкових порушень, визначена властивостями самої АС – її архітектурою, реалізацією та адмініструванням.

Це означає, що в основі кожного факту порушення безпеки АС лежить відповідна вада засобів захисту, то зумовлює успішне здійснення атаки. Аналіз випадків порушення безпеки повинен ґрунтуватися не стільки на дослідженні методів, використовуваних порушником, скільки на виявленні властивостей АС, що дають змогу йому здійснити свої дії. Інакше кажучи, що стало

причиною успішного здійснення порушення безпеки в тому чи іншому випадку?

Аналіз і статистика показують, що всі випадки порушення безпеки АС відбуваються з однієї або кількох наступних причин. Наведені причини порушення безпеки зручно подати у вигляді схеми Рисунок. 2.1.

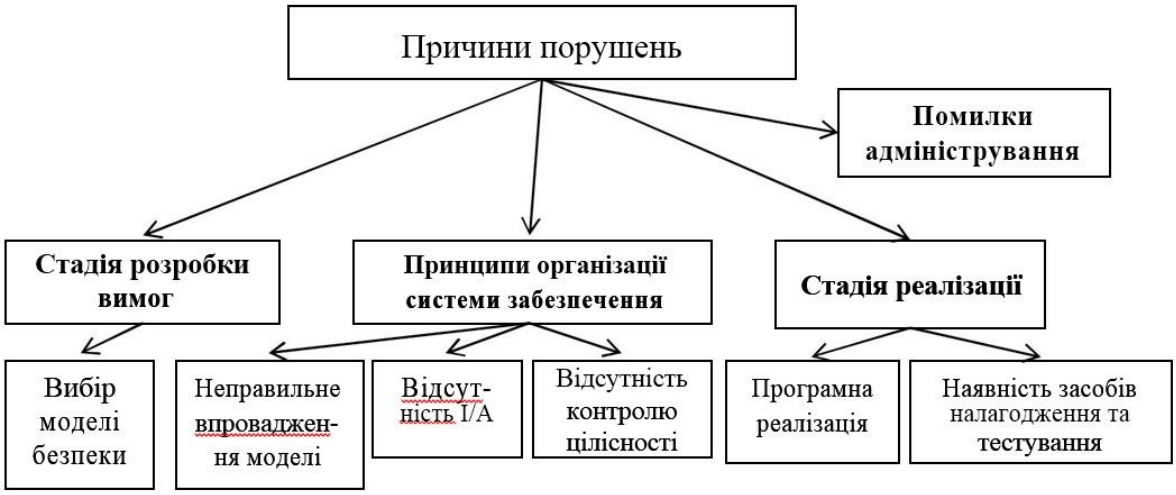

Рисунок 2.1 – Причини порушення безпеки

Вибір моделі безпеки, що не відповідає призначенню чи архітектурі АС. Модель безпеки повинна відповідати вимогам безпеки, запропонованим для АС. Сьогодні спостерігається певна невідповідність між моделями безпеки та архітектурою АС. Фактично формальні моделі безпеки існують тільки у вигляді теорії, а розробники АС змушені піддавати їх певній інтерпретації, щоб пристосувати до конкретної АС. В цьому випадку потрібно враховувати, що спотворення моделі, що виникли під час реалізації, зумовлені умовами та середовищем розробки, можуть не відповідати теоретичним положенням про стійкість. Це означає, що при виборі моделі безпеки потрібно брати до уваги специфіку архітектури, інакше, незважаючи на всі переваги моделі, гарантованого нею рівня безпеки досягти не вдасться.

Неправильне впровадження моделі безпеки. Незважаючи на цілком адекватний вибір моделі безпеки, її реалізація і застосування до архітектури конкретно ОС через властивості самої моделі чи ОС були проведені невдало.

Це означає, що в ході реалізації були втрачені всі теоретичні досягнення, отримані при формальному доведенні безпеки моделі. Звичайно неправильне впровадження моделі безпеки в систему виражається в недостатньому обмеженні доступу до найбільш важливих для безпеки систем служб і об'єктів, а також введенні різних винятків з передбачених моделлю правил розмежування доступу типу привілейованих процесів, утиліт.

Відсутність ідентифікації і/або аутентифікації суб'єктів і об'єктів. У багатьох сучасних ОС ідентифікація та аутентифікації суб'єктів і об'єктів взаємодії знаходяться на дуже примітивному рівні – суб'єкт (зловмисник) може порівняно легко видати себе за іншого суб'єкта і скористатися його повноваженнями доступу до інформації.

Відсутність контролю цілісності засобів забезпечення безпеки. У багатьох ОС контролю цілісності самих механізмів, що реалізують функції захисту, приділяється слабка увага. Багато систем допускають прозору для служб безпеки підміну компонентів. З погляду безпеки таке становище є неприпустимим.

Помилки, яких припустилися в ході програмної реалізації засобів забезпечення безпеки. Ця група причин порушення безпеки буде існувати доти, доки не з'являться технології програмування, що гарантують виробництво безпомилкових програм. Оскільки, як відомо, програми завжди мають помилки, то, очевидно, такі технології не з'являться взагалі, і помилки такого роду будуть виникати завжди.

Наявність засобів налагодження і тестування в кінцевих продуктах. Багато розробників залишають у комерційних продуктах так звані «люки», «діри», налагоджувальні можливості тощо. Причини, з яких це відбувається, цілком зрозумілі – програмні продукти стають усе складнішими, і налагодити їх у лабораторних умовах просто неможливо. Отже, для визначення причин збоїв і помилок уже в процесі експлуатації розробникам доводиться залишати у своїх продуктах можливості для налагодження і діагностики в ході експлуатації.

Помилки адміністрування. Наявність найсучасніших засобів захисту не гарантує відсутність вразливостей та потенційних порушень безпеки, тому що в будь-якій системі безпеки завжди існує людський фактор – людина, що відповідає за забезпечення безпеки, може допустити елементарну помилку, і всі зусилля розробників будуть змарновані. Помилки адміністрування є досить поширеною причиною порушень безпеки, але часто ставляться у вину розробникам системи захисту інформації.

3 МЕТОД МІНІМІЗАЦІЇ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Теорія ігор

Теорія ігор – це галузь науки про знаходження найкращого рішення між сторонами, що конфліктують. Кожна зі сторін зацікавлена в тому, щоб приховати від супротивника власні наміри, прийняття рішень в умовах конфлікту, зазвичай, відбувається в умовах невизначеності. Навпаки, фактор невизначеності можна інтерпретувати як противника суб'єкта, який приймає рішення (тим самим прийняття рішень в умовах невизначеності можна розуміти як прийняття рішень в умовах конфлікту). Зокрема, багато тверджень математичної статистики часто в теорії можна розглядадати як математичну гру.

Теорія ігор – це математичний апарат, що розглядає конфліктні ситуації, а також ситуації спільних дій кількох учасників.

Все частіше мають місце конфліктні ситуації, коли два або більше колективів (індивідуумів) мають протилежні цілі та інтереси, причому результат дії кожної із сторін залежить і від дії супротивника. Класичним прикладом конфліктної ситуації є відношення продавець – покупець. Складніші ситуації виникають, коли в суперечці інтересів беруть участь об’єднання чи коаліції.

Часто однією із сторін конфлікту є природні процеси чи явища, наприклад, погода, тобто маємо гру людини з природою. Погодними умовами людина практично не може керувати, але вона має змогу пристосовуватися до її постійних змін.

Характерними рисами математичної моделі ігрової ситуації є наявність, кількох учасників, яких називають гравцями, опис можливих дій кожної із сторін, що називаються стратегіями, визначених результатів дій для кожного гравця, що подаються функціями виграшу. Задачею кожного гравця є

знаходження оптимальної стратегії, яка за умови багатократного повторення гри забезпечує даному гравцю максимально можливий середній виграш.

Мета теорії ігор – вироблення рекомендацій щодо розумної поведінки учасників конфлікту. У теорії ігор розроблена система власних понять:

- математична модель конфлікту називається грою;
- сторони у конфлікті називаються гравцями;
- результат гри називається виграшем, програшем або нічиєю;
- правилами гри називається перелік прав і обов'язків гравців;
- ходом називається вибір гравцем однієї з передбачених правилами гри дій. Ходи бувають особисті і випадкові. Особистий хід – це персональний усвідомлений вибір дії гравця, випадковий хід – дія, що не залежить від волі гравця і визначається умовами середовища.

Залежно від кількості можливих ходів у грі, ігри поділяються на скінченні (зі скінченною кількістю можлививх ходів) і нескінченні. Деякі ігри в принципі мають вважатися скінченними, але мають так багато ходів, що належать до нескінченних.

- Стратегією гравця називається сукупність правил, що визначають вибір варіанта дій у кожному особистому ході.

Оптимальною стратегією гравця називається така, що забезпечує йому максимальний виграш. Завдання теорії ігор – виявлення оптимальної стратегії.

- Ігри, що складаються тільки з випадкових ходів, називаються азартними. Ними теорія ігор не займається. Її мета оптимізація поведінки гравця у грі, де поряд з випадковими є особисті ходи. Такі ігри називаються стратегічними.

- Гра називається грою з нульовою сумою, якщо сума виграшів усіх гравців дорівнює нулю, тобто кожен виграш за рахунок інших.

- Гра називається парною, якщо в неї грають два гравці.

- Парна гра з нульовою сумою називається антагоністичною. Теорія таких ігор найбільше розвинена. Крім того, такі ігри моделюють великий клас

реальних конфліктів. Подальші міркування будуть стосуватися саме антагоністичних ігор.

Основне припущення, на підставі якого знаходять оптимальне рішення в теорії ігор, полягає в тому, що супротивник такий же розумний, як і сам гравець.

3.2.1 Матричні ігри для двох осіб

У грі грають два гравці, зазвичай їх називають А і В. Себе прийнято ототожнювати з гравцем А. Нехай в А є m можливих стратегій: A_1, A_2,…, A_m, а в супротивника В – n можливих стратегій: B_1, B_2,…, B_n. Така гра називається грою m·n.

Позначають через $a_{i\,j}$ виграш гравця А при власній стратегії A_i і стратегії супротивника B_j. Зрозуміло, що кількість таких ситуацій може бути m·n. Гру зручно відображати таблицею, що називається платіжною матрицею, або матрицею виграшів, Таблиця 1.10. Платіжна матриця має стільки стовпців, скільки стратегій у гравця В, і стільки рядків, скільки стратегій у гравця А. На перетинанні рядків і стовпців, що відповідають різним стратегіям, стоять виграші гравця А і, відповідаю, програші гравця В.

Зведення гри до матричної форми може бути трудомістким і навіть невиконуваним завданням через невизначеність стратегій, їх значну кількість, а також складність оцінювання виграшу. Ці приклади саме й показують на ряд обмежень в даній теорії, тому що багатьох випадках задачу неможливо розв’язати методами теорії ігор.

Спочатку звернено увагу на такий факт. Виходячи з вигляду платіжної матриці, можна зробити висновок, які стратегії с свідомо невигідними. Це ті стратегії, для яких кожен з елементів відповідного рядка матриці менший або дорівнює відповідним елементам іншого якого-небудь рядка.

Таблиця 3.1 – Загальний вигляд платіжної матриці

B / A	B_1	B_2	…	B_n
A_1	a_{11}	a_{12}	…	a_{1n}
A_2	a_{21}	a_{22}	…	a_{2n}
.	.	.	…	.
.	.	.	…	.
.	.	.	…	.
A_m	a_{m1}	a_{m2}	…	a_{mn}

Кожен елемент матриці це виграш гравця А, і якщо для якої-небудь стратегії (рядка) всі виграші менші від виграшів іншої стратегії, зрозумію, що перша стратегії менш вигідна, ніж друга. Така операція відбраковування явно невигідних стратегій називається мажоруванням.

Якщо задача зведена до матричної форми, то можна порушувати питання про пошук оптимальних стратегій. Насамперед введенно поняття верхньої і нижньої ціни гри.

Нижньою ціною гри називається такий елемент матриці, для якого справедливо наступне:

$$a = \min_i \max_j a_{ij} \qquad (3.1)$$

Нижня ціна гри означає, що не зважаючи на вибір стратегії гравця В, гравець А гарантує собі виграш, не менший за а.

Верхньою ціною гри називається елемент, для якого виконується:

$$\beta = \min_j \max_i a_{ij} \qquad (3.2)$$

Верхня ціна гри - це гарантія для гравця В, що гравець А не отримає виграш, більший за β.

Точка (елемент) матриці, для якої справедливо наступне:

$$a = \beta \tag{3.3}$$

називається сідловою точкою. В сідловій точці найбільший з мінімальних виграшів гравця А точно дорівнює найменшому з максимальних програшів гравця В, тобто мінімум у якому-небудь рядку матриці збігається з максимумом у якому-небудь стовпці.

Основною метою розв'язування задач цього класу є розроблення рекомендацій щодо вибору оптимальних стратегій конфліктуючих сторін на основі застосування методичних підходів теорії ігор.

Два гравці А і В (гра двох осіб з нульовою сумою). Кожний гравець вибирає одну із можливих стратегій: позначються стратегії гравця А – A_i $(i = \overline{1,m})$, стратегії гравця В – B_j $(j = \overline{1,n})$.

Результати (плата) за всіма можливими варіантами гри задаються спеціальними функціями, які залежать від стратегій гравців, як правило, у вигляді платіжної матриці.

Нехай $\varphi_1(A_i;\ B_j) = (i = \overline{1,m};\ j = \overline{1,n})$ – виграш гравця А; $\varphi_2(A_i;\ B_j)(i = \overline{1,m};\ j = \overline{1,n})$– виграш гравця В.

Оскільки гра з нульовою сумою, то $\varphi_1(A_i;\ B_j) + \varphi_2(A_i;\ B_j) \equiv 0$

Тоді в разі, якщо

$$\varphi_1(A_i;\ B_j) = \varphi(A_i;\ B_j),$$

то

$$\varphi_1(A_i;\ B_j) = -\varphi(A_i;\ B_j).$$

Отже, мета гравця А – максимізувати величину $\varphi(A_i;\ B_j)$, а гравця В – мінімізувати її. Нехай $\varphi(A_i;\ B_j) = a_{ij}$ тобто маємо матрицю А:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

де рядки відповідають стратегіям A_i, а стовпці – стратегіям Bj.

Матриця А називається матрицею гри. Елемент цієї матриці a_{ij} – це виграш гравця А, якщо він вибрав стратегію A_i, а гравець В – стратегію B_j. Із багатьох критеріїв, які пропонуються теорією ігор для вибирання раціональних варіантів рішень, найпоширенішим є песимістичний критерій мінімаксу-максиміну. Суть цього критерію полягає у нехай гравець А вибрав стратегію A_i, тоді у найгіршому разі він отримає виграш, що дорівнює min a_{ij}, тобто навіть тоді, якщо гравець В знав б стратегію гравця А. Передбачаючи таку можливість, гравець А має вибрати таку стратегію, щоб максимізувати свій мінімальний виграш, тобто $a = \max_i \min_j a_{ij}$.

Така стратегія гравця А позначається A_{i_0} і має назву максимінної, а величина гарантованого виграшу цього гравця називається нижньою ціною гри.

Гравець В, який програє суми у розмірі елементів грального матриці, навпаки має вибрати стратегію, що мінімізує його максимально можливий програш за всіма варіантами дій гравця А. Стратегія гравця В позначається через B_{j_0} і називається мінімаксною, а величина його програшу – верхньою ціною гри, тобто $b = \min_j \max_i a_{ij}$.

Оптимальний розв’язок цієї задачі досягається тоді, коли жодній стороні невигідно змінювати вибрану стратегію, оскільки її супротивник може у відповідь вибрати іншу стратегію, яка забезпечить йому кращий результат.

Якщо, $\max_i \min_j a_{ij} = \min_j \max_i a_{ij} = \mu$ тобто, $a = b = \mu$то гра називається цілком визначеною. В такому разі виграш гравця А (програш гравця В) називається значенням гри і дорівнює елементу матриці $a_{i_0 j_0}$. Цілком визначені ігри називаються іграми з сідловою точкою, а елемент грального матриці, значення якого дорівнює виграшу гравця А (програшу гравця В) і є сідловою

точкою. В цій ситуації оптимальним рішенням гри для обох сторін є вибір лише однієї з можливих, так званих чистих стратегій – максимінної для гравця А та мінімаксної для гравця В, тобто якщо один із гравців притримується оптимальної стратегії, то для другого відхилення від його оптимальної стратегії не може бути вигідним.

3.2.2 Зведення матричної гри до задач лінійного програмування

Теорія ігор перебуває в тісному зв'язку з лінійним програмуванням, тому що кожна кінцева гра двох осіб з нульовою сумою може бути представлена як задача лінійного програмування і вирішена симплексним методом і, навпаки, кожна задача лінійного програмування може бути представлена як кінцева гра двох осіб з нульовою сумою .

Якщо гра $2 \times n$ або $m \times 2$ може бути розв’язана геометрично, то у випадку гри $3 \times n * (m \times 3)$ геометрична інтерпретація переходить у простір, що ускладнює як її побудову, так і сприйняття. У випадку ж, коли $n > 3, m > 3$ геометрична інтерпретація взагалі неможлива. Для розв'язування гри $m \times n$ використовують прийом зведення її до задачі лінійного програмування.

Нехай розглядається парна гра зі стратегіями $A_1, A_2, \dots, A_m$ для гравця А та стратегіями $B_1, B_2, \dots, B_m$ для гравця В і платіжною матрицею $(A_{ij}) = (i = \overline{1,m}; j = \overline{1,n})$. Необхідно знайти оптимальні змішані стратегії $X^* = (x_1^*, x_2^*, \dots, x_m^*)$ і $Y^* = (y_1^*, y_2^*, \dots, y_m^*)$, де $\sum_{i=1}^{m} x_i^* = 1,\ \sum_{j=1}^{n} y_j^* = 1$.

Знайдемо спочатку оптимальну стратегію гравця А. За основною теоремою теорії ігор така стратегія має забезпечити гравцеві виграш, не менший за ціну гри (поки що невідому величину) μ, за будь-якої поведінки гравця В.

Допустимо, що гравець А застосовує свою оптимальну стратегію, а гравець В - свою «чисту» j-ту стратегію B_j, тоді середній виграш гравця А дорівнюватиме:

$$a_{1j}x_1^* + a_{2j}x_2^* + \cdots + a_{mj}x_m^*. \qquad (3.4)$$

За цих обставин виграш має бути не меншим, ніж ціна гри. Отже, для будь-якого значення $j(j=\overline{1,n})$ величина має бути не меншою, ніж μ:

$$\begin{cases} a_{11}x_1^* + a_{21}x_2^* + \cdots + a_{m1}x_m^* \geq \mu; \\ a_{12}x_1^* + a_{22}x_2^* + \cdots + a_{m2}x_m^* \geq \mu; \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{1n}x_1^* + a_{2n}x_2^* + \cdots + a_{mn}x_m^* \geq \mu. \end{cases}$$

Розділивши всі обмеження на μ, отримаємо:

$$\begin{cases} a_{11}\dfrac{x_1^*}{\mu} + a_{21}\dfrac{x_2^*}{\mu} + \cdots + a_{m1}\dfrac{x_m^*}{\mu} \geq 1; \\ a_{12}\dfrac{x_1^*}{\mu} + a_{22}\dfrac{x_2^*}{\mu} + \cdots + a_{m2}\dfrac{x_m^*}{\mu} \geq 1; \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{1n}\dfrac{x_1^*}{\mu} + a_{2n}\dfrac{x_2^*}{\mu} + \cdots + a_{mn}\dfrac{x_m^*}{\mu} \geq 1. \end{cases}$$

Позначивши $\frac{x_1^*}{\mu} = t$ маємо :

$$\begin{cases} a_{11}t_1 + a_{21}t_2 + \cdots + a_{m1}t_m \geq 1; \\ a_{12}t_1 + a_{22}t_2 + \cdots + a_{m2}t_m \geq 1; \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{1n}t_1 + a_{2n}t_2 + \cdots + a_{mn}t_m \geq 1, \end{cases}$$

$t_i \geq 0(i=\overline{1,m})$.

Враховуючи умову, що $x_1^* + x_2^* + \cdots + x_m^* = 1$ отримуємо $t_1 + t_2 + \cdots + t_m = \frac{1}{\mu}$.

Необхідно зробити виграш максимальним. Цього можна досягти, коли вираз $t_1 + t_2 + \cdots + t_m = \frac{1}{\mu}$ набуватиме мінімального значення. Отже, врешті маємо звичайну задачу лінійного програмування.

Цільова функція: $\max \mu = \min \frac{1}{\mu} = \min \sum_{i=1}^{m} t_i$ за умов:

$$\begin{cases} a_{11}t_1 + a_{21}t_2 + \cdots + a_{m1}t_m \geq 1; \\ a_{12}t_1 + a_{22}t_2 + \cdots + a_{m2}t_m \geq 1; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \\ a_{1n}t_1 + a_{2n}t_2 + \cdots + \cdots . t_m \geq 1. \end{cases},$$

$t_i \geq 0 (i = \overline{1,m})$.

Розв'язуючи цю задачу симплексним методом, знаходимо значення $t_i (i = \overline{1,m})$, а також величину $\frac{1}{\mu}$ і значення $x_i^* = \mu t_i$, що є оптимальним розв'язком початкової задачі. Отже, визначено змішану оптимальну стратегію $X^* = (x_1^*, x_2^*, \ldots, x_m^*)$ для гравця А.

За аналогією можна записати задачу лінійного програмування для визначення оптимальної стратегії гравця В. З цією метою позначимо: $\frac{y_j^*}{\mu} = \mu_i (j = \overline{1,n})$. Маємо таку лінійну модель задачі: $\max F = \sum_{j=1}^{n} \mu_j$ за умов:

$$\begin{cases} a_{11}\mu_1 + a_{12}\mu_2 + \cdots + a_{1n}\mu_n \geq 1; \\ a_{21}\mu_1 + a_{22}\mu_2 + \cdots + a_{2n}\mu_n \geq 1; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}\mu_1 + a_{2n}\mu_2 + \cdots + a_{mn}\mu_n \geq 1. \end{cases}$$

$\mu_j \geq 0 (j = \overline{1,n})$.

Очевидно, що задача лінійного програмування для гравця В є двоїстою до задачі гравця А, а тому оптимальний розв'язок однієї з них визначає також оптимальний розв'язок спряженої.

Задачі теорії ігор належать до задач прийняття рішень за умов невизначеності та ризику.

Невизначеність результатів гри зумовлена кількома чинниками. По-перше, як правило, кількість можливих варіантів розвитку подій дуже велика, тому передбачити результат гри неможливо. Простою ілюстрацією такого

твердження є гра в шахи. Із-за безлічі можливих комбінацій знайти оптимальний розв'язок такої гри неможливо. По-друге, значний вплив на хід та результати гри мають випадкові чинники, дію яких передбачити неможливо, наприклад, у рулетці. По-третє, джерелом невизначеності є брак інформації щодо дій противника. Крім того, невизначеність певною мірою може стосуватися також і мети, якої прагне досягти суб'єкт. Не завжди таку мету можна виразити однозначно, а тим більше одним показником.

Зрозуміло, що коли початкові умови задачі містять значну кількість невизначених параметрів, то математичне дослідження не може дати чіткого обґрунтування раціонального розв'язку, однак і за відсутності повної визначеності кількісний аналіз дає наукову основу для прийняття рішень.

3.2 Розробка політики безпеки із використанням теорії ігор

Використання теорії ігор для розробки політики безпеки інформації обґрунтовано в роботах багатьох дослідників, в тому числі для захисту об’єктів критичної інфраструктури та протидії терористичній діяльності.

Актуальною проблемою створення політики безпеки інформації – є мінімізація витрат на її реалізацію за необхідності досягнення заданого рівня захищеності. В такій постановці, природньо моделювати інформаційне протистояння як статичну гру двох осіб: зловмисника та захисника. Очікується, що обидва гравці ведуть себе раціонально, тобто намагаються отримати максимальну вигоду для себе. Таким чином, нагородою зловмисника є збиток завданий жертві, в той час як метою захисника є забезпечення стабільної роботи системи. Маючи відомості про інформаційно–комунікаційну систему (задача з прозорою інформацією), зловмисник оперує загрозами, намагаючись завдати максимального збитку. Захиснику необхідно розподілити засоби та заходи захисту таким чином, щоб забезпечити необхідний рівень захищеності інформаційної системи, мінімізувавши витрати на реалізацію системи захисту інформації.

3.2.1 Опис системи

Об’єктом дослідження є розподілена ІКС із відкритою архітектурою, яка складається із одного компонента, що приймає участь в обробці інформації. Компонент описується набором характеристик, серед яких технологія обробки інформації, операційне середовище та інші. Вказані параметри компонента складають цінність для системи, яка буде позначатися через q.

Враховуючи особливості обчислювального середовища, компонент є вразливим до загроз із a допустимих. Допускається, що інформація про архітектуру ІКС є відкритою та відомою учасникам конфлікту. Крім того, задана ймовірність успішної реалізації загрози a проти компоненту системи c, а також ймовірність нейтралізації загрози, встановленням механізмів захисту p. Таким чином, на ефективність прийнятих зловмисником чи захисником рішення впливають випадкові фактори, що враховуються при моделюванні.

Задача полягає в побудові системи захисту інформації для описаної ІКС, які забезпечить конфіденційність, цілісність та доступність даних. Допускається, що інформація про технології обробки інформації та обчислювальне середовище є доступною і може потрапити до зловмисника.

Для вирішення поставленої задачі необхідно формалізувати систему,що підлягає захисту, в тому числі:

- провести оцінку потенційних втрат компонента q ;
- провести аналіз та створити модель порушника та атак, з урахуванням зазначених вимог, що буде включати можливі загрози a та ймовірність їх реалізації ha ;
- провести аналіз та реалізувати модель захисту де будуть обрані механізми захисту здатні протистояти зловмисникові.

Основні рішення, щодо побудови системи захисту, приймаються на етапі розробки політики безпеки. Саме тоді проводиться аналіз загроз та вразливостей, складається модель порушника та обираються механізми, що забезпечать захист від нього. Під час обрання засобів та заходів захисту доцільно використовувати математичні засоби для синтезу структури системи

захисту таким чином, щоб досягнути мінімального ризику. Результатом створення політики безпеки є формалізована модель зловмисника та сформовані вимоги до СЗІ, в тому числі обрані механізми захисту.

3.2.2 Позиційна гра “Захисник-зловмисник”

Побудова СЗІ розглядається як антагоністична гра двох гравців із повною інформацією, при чому сторони діють в умовах ризику. У такій грі ходи можуть бути детермінованими та випадковими. Детерміновані ходи є свідомим вибором стратегії дій гравців серед наявних альтернатив (варіантів рішень).

Рішення зловмисника визначає, яку розвідку чи загрозу a йому реалізовувати проти компонента c. Набір альтернатив можна представити у вигляді матриці $Y = \{y_a\}$, що складається із булевих елементів, причому $y_a = 1$ означає рішення, щодо реалізації загрози a проти компоненту c.

Вибір стратегії захисника передбачає встановлення механізму захисту $p = 1,2,...,P$ у компонент c. Набір його альтернатив будемо описувати матрицею булевих елементів $X = \{x_p\}$, причому $x_p = 1$ означає рішення, щодо встановлення механізму захисту p у компонент c.

Випадковий хід представляє собою вибір, що здійснюється під впливом випадкових факторів, а не конкретним гравцем. Набір таких факторів у теорії ігор називають «природою» – додатковим гравцем, що робить свої ходи випадково. Наприклад, під час перебору паролів існує не нульова ймовірність підбору правильного пароля або з іншої сторони, під час встановлення системи виявлення вторгнень існує ненульова ймовірність виявлення протиправних розвідувальних дій зловмисника (як то сканування портів). При цьому для кожного стохастичного ходу задається розподіл ймовірностей на множині всіх альтернатив “природи”.

Будемо вважати, що «природа» впливає на рішення, які прийняв як зловмисник так і захисник. Позначимо через h_a ймовірність успіху зловмисника під час розвідки або реалізації загрози a проти компоненту c. Тоді через d_{ap}

позначимо ймовірність виявлення або нейтралізацію загрози *a*, під час встановлення механізму захисту *p*.

Ситуація, в якій опиняються гравці в результаті своїх ходів, називається позицією. Множину всіх позицій можна розбити на такі підмножини:

- позиції, що належать зловмиснику, в кожній із яких він приймає рішення щодо вибору альтернативи серед тих, що доступні йому;

- позиції, що належать захиснику, в кожній із яких він вибирає серед наявних альтернативних варіантів.

У теорії окремо розглядають позиції із випадковими ходами, проте в запропонованій моделі випадкові ходи «природи» безпосередньо пов’язані з детермінованими ходами обох гравців і будуть розглядатися разом. Таким чином, при застосуванні кожної зі стратегій чи то зловмисником чи захисником існує ненульова ймовірність успіху (провалу) обраної стратегії в обраному обчислювальному середовищі, за заданої апріорної ймовірності успіху обраної події.

Доступно можна пояснити гру зловмисника та захисника можна з допомогою рисунка 3.1, Де зловмисник старається розвідати та проаналізувати вразливості системі, він може здійснити її пасивно або активно, тобто активно – це втручання в систему, отримання більш достовірну інформацію про вразливості, але більша ймовірність бути викритим, а пасивно – це не втручаючись у систему більш надійний варіант для захисту зловмисника, але цей варіант приносить менше інформації про систему. Захисник на даному етапі старається попередити атаку, шляхом нейтралізації вразливості.

Наступним кроком зловмисника – це здійснення атаки, на вразливе місце, при цьому порушується одна із властивостей інформації, таких як конфіденційність, цілісність або доступність. Захисник використовує засоби та заходи захисту для нейтралізації дій зловмисника.

І останнім кроком є, приховування слідів зловмисником, захисник на даному етапі вдіяти вже нічого не може.

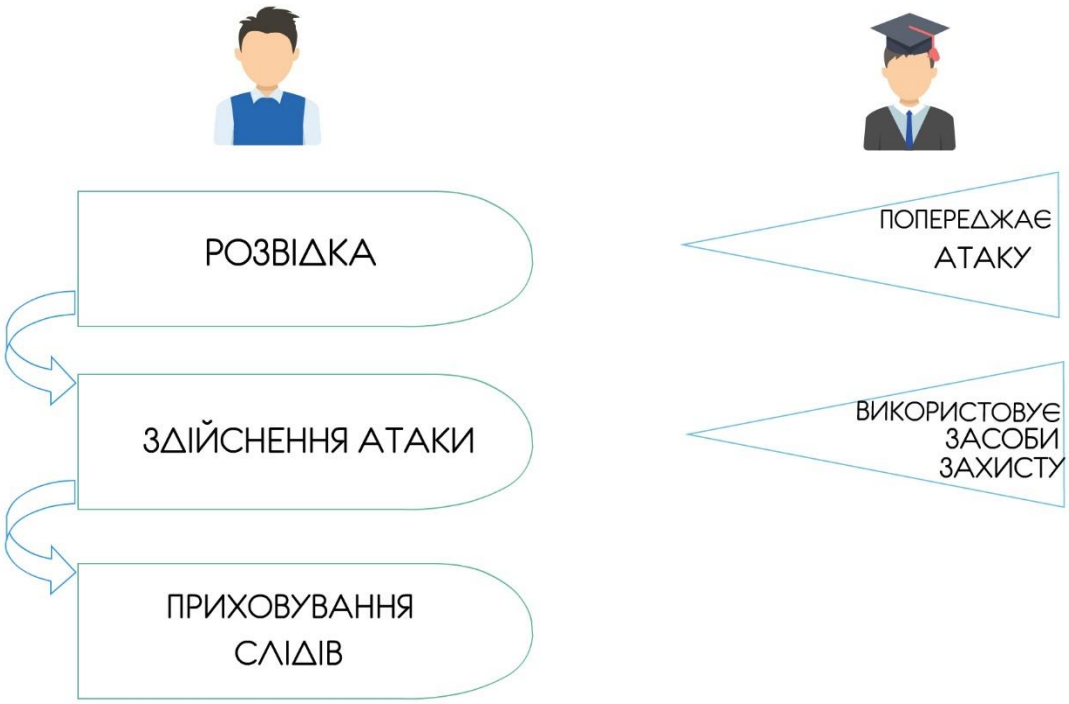

Рисунок 3.1 – Схема гри зловмисника та захисника

3.2.3 Цільова функція

Відносини між захисником та зловмисником можуть бути формалізовані з використанням функції ризику. Зловмисник завдаючи збитків системі намагається максимізувати ризик. У той же час, захисник, проти діючи зловмиснику, встановлює механізми захисту, прагнучи зменшити ризик до нуля. В умовах обмеженості фінансових та технічних ресурсів, за заданої моделі зловмисника, захиснику необхідно розподілити засоби та заходи захисту, таким чином щоб ризик в ІКС був мінімальним. У термінах теорії ігор функція ризику виступає платіжною функцією. Кількісним показником оцінювання ризиків є завданий збиток Q , що виражається у вигляді витрат та неотриманої вигоди. Таким чином значення збитку Q спричинене компоненту c еквівалентне цінності цього компонента q для функціонування системи в цілому. У подальшому будемо вважати ці величини тотожними.

В загальному вигляді відношення для функції ризику інформаційної безпеки R_a можна обчислити, перемноживши ймовірності $P^{\sim}{}_a$ реалізації загрози a та завданому збитку за реалізації цієї загрози Q. Також введемо змінну V_a , що

описує ймовірність нейтралізації загрози з використанням встановлених додаткових механізмів захисту:

$$R_a = P_{ac}^{\sim} \cdot Q \cdot (1 - V_a) \tag{3.5}$$

Однією із особливостей протистояння між захисником та зловмисником є динамічний характер, так як атаці зазвичай передує спостереження за системою та розвідка, які необхідно враховувати в моделі. Таким чином стан конфліктної ситуації може змінюватися з часом.

Як було зазначено, платіжна (цільова) функція виражається через ризик інформаційної безпеки, що зловмисник намагається збільшити, а захисник зменшити. Зловмисник обираючи стратегію дій оперує ймовірністю реалізації загроз: $P_a^{\sim} = h_a \cdot y_a$ та потенційним збитком Q=q при технічних обмеженнях на кількість одночасно реалізованих загроз L. Захисник може зменьшити ризик завдяки встановленню додаткових механізмів захисту: $V_a = \sum_p d_{ap} \cdot x_p$. Якщо $V_a = 1$, то компонент повністю захищений від загрози a , тому щоб не допустити встановлення надлишкових засобів та заходів захисту вводиться обмеження $V_a \leq 1$ Крім того, у захисника обмежені ресурси W на реалізацію механізмів захисту p , вартість кожного з яких дорівнює w_p Підставивши визначені змінні в (3.5) та врахувавши мету захисника та зловмисника можна записати цільову функцію:

$$R = \min_x \max_y \sum_{a=1}^{A} \left\{ h_a * y_a * q_c * \left[1 - \sum_{p=1}^{p} d_{ap} * x_p \right] \right\} \tag{3.6}$$

За наступних обмежень:

$$\sum_a y_a \leq L, \qquad \sum_{c,p} w_p * x_{cp} \leq W, \qquad \sum_p d_{ap} * x_{cp} \leq 1$$

$$x_p = \{0,1\}, \qquad y_a = \{0,1\},$$

За умови без етапної гри позиційна гра зловмисника та захисника розглядається як статична задача. Першим кроком розв'язання нелінійної задачі (3.6) передбачається перехід до двоїстої, шляхом введення змінної θ та зафіксувавши значення стратегій захисника x :

$$R = \min_{\theta} \sum_{a} \theta_a \ , \tag{3.7}$$

$$\theta_a \geq h_a * q * \left[1 - \sum_{p} d_{ap} * x_p\right],$$

$$\sum_{p} w_p * x_p \leq W \ , \ \sum_{p} d_{ap} * x_p \leq 1 \ , \ \theta_a \geq 0 \ ,$$

Подальший розв'язок задачі (3.7) відбувається з використанням методу гілок та границь [11]. У результаті розв'язання отримуємо оптимальний набір рішень захисника x_p та зловмисника , y_a які в теорії ігор складають рівновагу за Нешем.

В теорії ігор рівновагою Неша називають гру у якій стратегії або дії, згідно з якими кожен учасник реалізує оптимальну стратегію, передбачають дії суперників. Ця атака – це сукупність стратегій та виграшів, при якій жоден із учасників не може збільшити виграш, змінивши вибір стратегії в односторонньому порядку, коли інший учасник не змінює свій вибір.

Фахівці з теорії ігор використовують умову рівноваги Неша для аналізу стратегічної взаємодії кількох гравців. Це надає шлях для передбачення того, що відбудеться у випадку, коли кілька людей, або кілька установ приймають рішення одночасно, а результат залежить не тільки від власного рішення, але і від рішень інших. Ідея Джона Неша полягає у тому, що не можна передбачити результати вибору декількох учасників гри, аналізуючи ці рішення ізольовано одне від іншого. Натомість, потрібно запитувати, що робитиме кожен гравець, і враховувати імовірні рішення інших учасників.

Рівновага Неша була використана для аналізу ситуацій протистоянь, таких як війна або гонка озброєнь, а також дослідження того, як зменшити напруженість конфлікту шляхом повторних взаємодій. Це також було використано для вивчення граничної міри співпраці людей з різними вподобаннями, і чи будуть вони ризикувати для отримання спільного результату; використовувалось для вивчення адаптації технічних стандартів, а також явища банкової паніки і валютної кризи. Інші застосування включають транспортні потоки, організацію аукціонів, результат наданих зусиль кількома групами в навчальному процесі, регулятивне законодавство таке, як регулювання навколишнього середовища, і навіть удари пенальті у футболі.

Неформальне визначення рівноваги Неша – це набір стратегій і є рівновагою, якщо ні один гравець не може отримати більш виграшну позицію, змінюючи свою стратегію в односторонньому порядку. Щоб продемонструвати рівновагу Неша, уявімо, що кожен гравець знає стратегії інших. Припустимо, що кожен гравець запитує себе: «будучи знайомим зі стратегіями інших гравців, і розглядаючи їх як певну сталу множину, чи можу я здобути перевагу просто удосконаливши свою стратегію?»

Якщо кожен гравець дасть відповідь «Так», то в такому випадку набір стратегій не є рівновагою Неша. Але якщо кожен гравець вирішує не змінювати свою стратегію, тоді набір таких стратегій є рівновагою Неша. Тому кожна стратегія в рівновазі Неша є найкращою відповіддю на всі інші стратегії в тій рівновазі. Рівновага Неша, інколи, може виглядати не раціональною з точки зору сторонньої особи. Це може статися, тому, що рівновага Неша не є парето-оптимальною (економічний термін, який описує такий стан системи, при якому значення кожного окремого критерію, що характеризує систему, не може бути покращено без погіршення становища інших елементів).

Рівновага Неша може мати не раціональні наслідки в покрокових іграх тому, що гравці «бояться» не раціональних ходів від інших гравців. Для таких ігор під-гра ідеальної рівноваги Неша може бути більш значущою як засіб аналізу.

Неш довів, що використання змішаних стратегій в кожній грі для скінченної кількості гравців, які обирають стратегію зі скінченної множини стратегій гарантує наявність хоча б одної рівноваги Неша.

Формальний опис рівноваги Неша. Припустимо,(*S, f*) гра n осіб, де S_i – набір стратегій i-того гравця, $S = S_1 \times S_2 \times ... \times S_n$, – це множина всіх чистих стратегій, а $f = (f_i(x), ..., f_n(x))$, – набір виграшів для $x \in S$. Коли кожний гравець $i \in \{1, ..., n\}$ вибирає стратегію x_i профілі стратегій $x = (x_1, ..., x_n)$, гравець I отримує виграш $f_i(x)$. Зауважимо, що виграш залежить від усього профілю стратегій: не тільки від стратегії, обраної самим гравцем I але і від чужих стратегій. Профіль стратегій $x^* \in S$ є рівновагою по Нешу, якщо зміна своєї стратегії з x^* на x_i вигідно ні одному гравцеві I, тобто $\forall_i x_i \in S_i$: $f_i(x_i^*, x_{-i}^*)$. Коли наведена нерівність виконується строго (з > замість ≥) для всіх гравців і всіх можливих альтернативних стратегій, то рівновага класифікується як а сувора рівновага Неша. Якщо замість цього, хоч один гравець, має точну рівність між x_i^* а якоюсь іншою стратегією в множині S то рівновага класифікується як а слабка рівновага Неша.

Гра може мати рівновагу Неша в чистих або в змішаних стратегіях (в останньому випадку чиста стратегія вибирається стохастично з фіксованою ймовірністю).

3.2.4 Побудова системи захисту інформації

На першому етапі побудови СЗІ проводимо аналіз компонента *c*. Необхідно визначити цінність *q* компонента *c*, яка в подальшому буде використовуватися для оцінки можливих збитків. Успішна реалізація загрози проти компонента призведе до фінансових втрат, що еквівалентні цінності компонента для функціонування системи в цілому. За відсутності статистичних даних та фінансових звітів, припустимо, що завданий збиток *q* пропорційний збитку цілої системи.

Невід’ємним етапом створення політики безпеки є формування моделі порушника. З огляду на поставлену задачу, необхідно передбачити захист від

зовнішніх порушників з високою кваліфікацією, що оснащені необхідними програмними та апаратними засобами для віддаленої реалізації загроз ІБ та метою яких є: отримання доступу до конфіденційної інформації; отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами; нанесення збитків шляхом знищення інформаційних цінностей.

Знаючи характерні ознаки порушника та його ціль, можна обрати типові загрози інформаційній безпеці a , використовуючи які, він зможе досягнути поставленої мети Таблиця 3.2.

Таблиця 3.2 – Загрози ІБ, ймовірності їх винекнення

№	Загрози a	Ймовірності реалізації h_a
Розвідка		
1	Сканування мережі	0,6
2	Використання сканерів вразливості	0,7
3	Аналіз протоколів	0,3
Проникнення		
4	Віддалене проникнення	0,4
5	Підбір паролів	0,6
6	«Троянський кінь»	0,8
7	Підміна об’єкта	0,9

Наступним етапом розробки політики безпеки є обрання механізмів захисту, орієнтуючись на модель загроз та архітектуру обчислювального середовища. Методом експертної оцінки визначається ефективність d_{ap} кожного із механізмів захисту p проти наявних загроз a в системі, а також вартість їх реалізації w_p, Таблиця 3.3. Кожен із механізмів захисту p забезпечує певний рівень захищеності.

Таблиця 3.3 – Модель захисту

№	Механізми захисту p	Індекси загроз інформаційній безпеці *a*							Вартість w_p
		1	2	3	4	5	6	7	
1	Розмежування доступу	0,3	0,3	0,1	0,7	0,2	0,1	0,1	15
2	Ідентифікація та автентифікація	0,4	0,1	0,1	0,2	0,8	0,1	0,1	10
3	Криптографічні функції	0,3	0,2	0,1	0,1	0,3	0,2	0,1	20
4	Забезпечення цілісності	0,1	0,3	0,1	0,2	0,1	0,1	0,2	5
5	Антивірусний захист	0,1	0,4	0,1	0,1	0,1	0,8	0,1	10
6	Система виявлення вторгнень	0,7	0,9	0,3	0,2	0,1	0,3	0,8	30

Останнім етапом, є синтез структури СЗІ. Зібравши необхідні дані, можна переходити до розв’язання поставленої задачі, а саме визначення структури системи захисту інформації, яка забезпечить мінімальне значення ризику інформаційної безпеки (3.5). Безпосередньо синтез СЗІ здійснюється з використанням співвідношення (3.6), результатом якого є набір механізмів захисту $\{p\}$ для компоненту системи. Розв’язуємо цю задачу з експоненціальної складністю, тому використовуємо автоматизований математичний пакет Matlab. У таблиці 3.4 продемонстровано рішення поставленої задачі для трьох різних ситуацій – за різних витрат на СЗІ *W*. У випадку витрат, що дорівнюють 40 одиниць, ризик знижується до 17% від його значення за відсутності будь-якого захисту. У разі посилення системи захисту значення ризику знижується до 11% та 6% за витрат 700 та 100 одиниць відповідно. Для різних вихідних даних отримано набори механізмів захисту, що

забезпечую інімальний ризик при заданих обмеженнях (ресурси на побудову СЗІ). Таким чином, на прикладі побудови СЗІ для ІКС установи показано практичну придатність розробленого підходу.

Таблиця 3.4 – Встановлені механізми захисту у систему

<table>
<tr><td></td><td colspan="3">Сукупність механізмів захисту $\{x_{cp}\}$</td><td rowspan="2">Загальна вартість філіалу</td></tr>
<tr><td>Виділені ресурси (W)</td><td>40</td><td>70</td><td>100</td></tr>
<tr><td>C_1</td><td rowspan="2">6</td><td rowspan="2">2,3,4,5</td><td rowspan="2">1-6</td><td></td></tr>
<tr><td>Компонент системи (C)</td><td rowspan="2">12000</td></tr>
<tr><td>Ризик ІБ (R)</td><td>5520</td><td>2880</td><td></td></tr>
</table>

Очевидно, що коли кількість виділених ресурсів більша ніж вартість самого комплексу заходів, то це вже є задачею без обмежень і передбачає використання всіх можливих механізмів захисту.

4 СПЕЦІАЛЬНА ЧАСТИНА

4.1 Інсталяція та встановлення програми Matlab

Для того, щоб встановити Matlab на комп'ютер, потрібно вставити інсталяційний DVD диск пакету Matlab в DVD-привід комп'ютера. Автоматично запуститься майстер установки даного продукту. Якщо цього не сталося, потрібно запустити Setup.exe, розташований в кореневій директорії інсталяційного диска Matlab. Після запуску деякий час будуть розпаковуватися потрібні для установки файли і в результаті відкриється наступне вікно, рисунок 4.1:

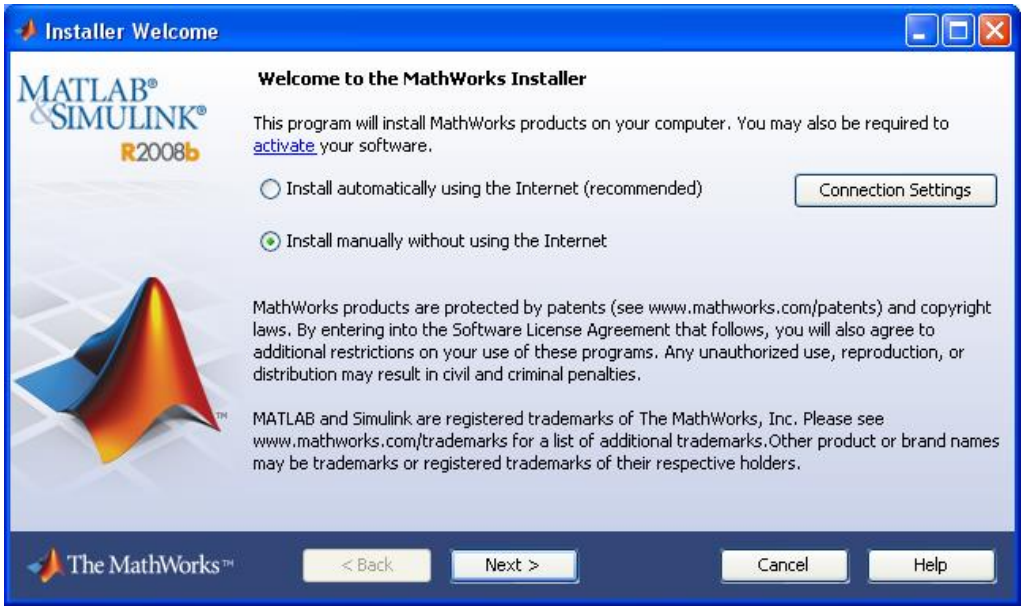

Рисунок 4.1 – Вибір встановлення програмного продукту

У цьому вікні потрібно вибрати пункт «Install manually without using the Internet» (вибіркова установка без використання Інтернет), дальше натиснути кнопку «Next>». Відкриється вікно ліцензійної угоди, рисунок 4.2:

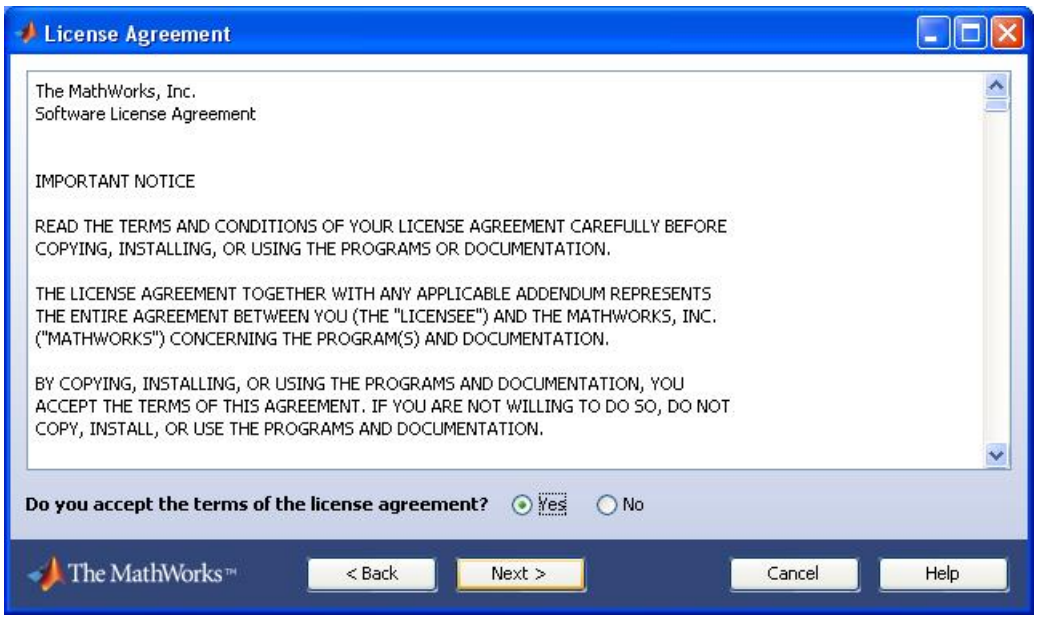

Рисунок 4.2 – Вікно ліцензійної угоди

У цьому вікні вибирається пункт «I have the File Installation Key for my license» (У мене є файл з інсталяційним ключем для моєї ліцензії) та скопіюйте цей ключ з отриманого файлу в полі під цим пунктом. Дальше потрібно натиснути кнопку «Next>». Відкриється вікно вибору установки: або за замовчуванням (Typical), або ручне налаштування (Custom), рисунок 2.3:

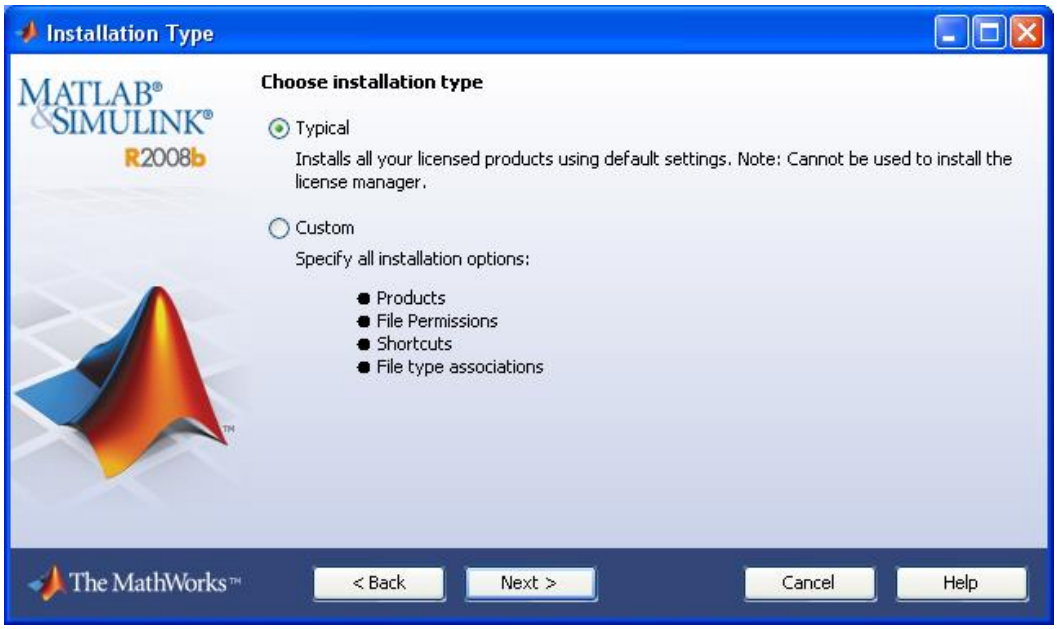

Рисунок 4.3 – Вибір налаштування программи

В цьому вікні краще вибирати пункт Typical, потім натиснути кнопку «Next>». Відкриється вікно вибору папки для установки, рисунок 4.4:

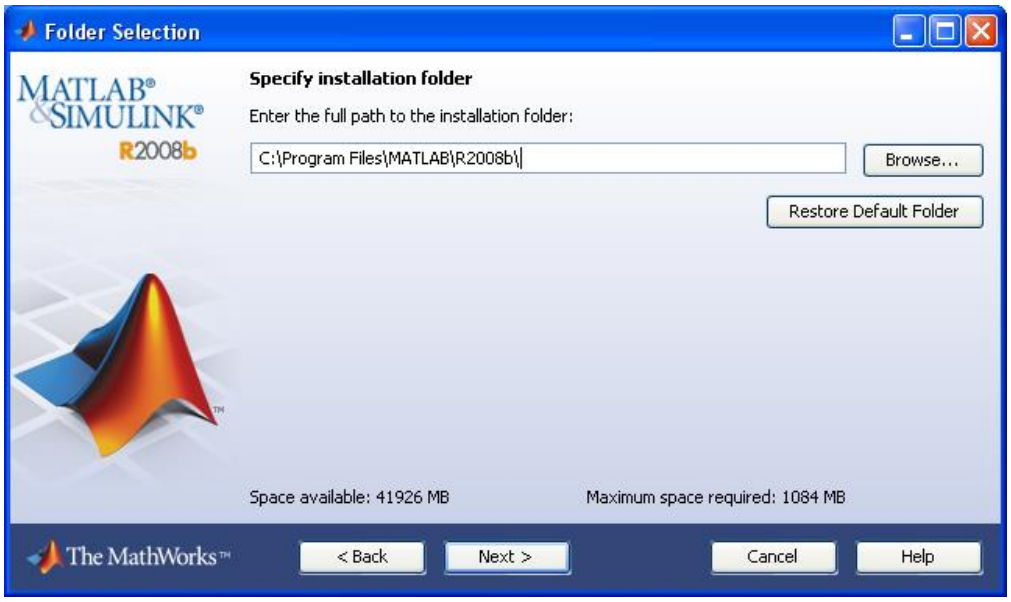

Рисунок 4.4 – Вікно вибору папки для установки програми

В цьому вікні потрібно вказати повний шлях для встановлення даного продукту, натиснути кнопку «Next>». Відкриється вікно вибору ліцензійного файлу (цей файл також буде виданий разом інсталяційним диском, він називається – license.dat), рисунок 4.5.

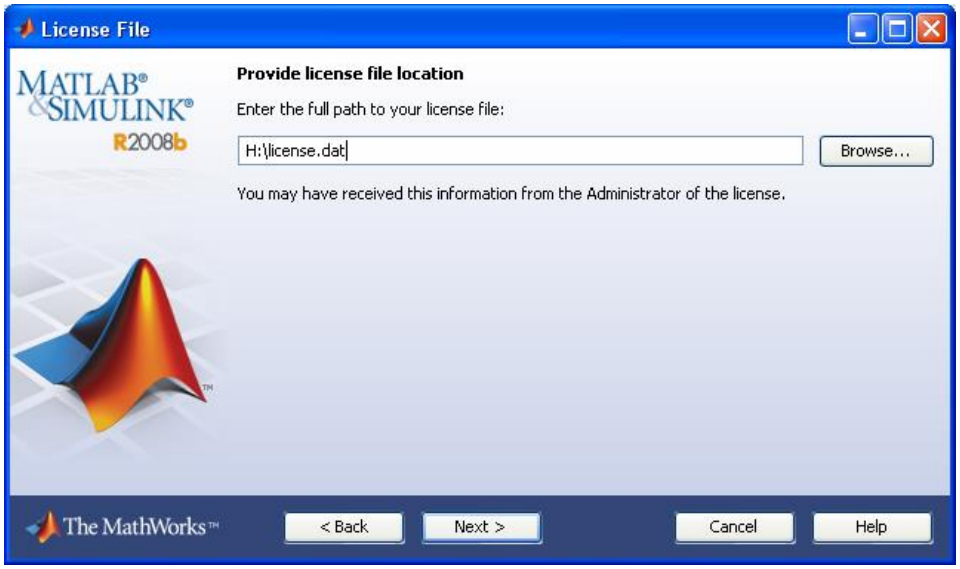

Рисунок 4.5 – Вікно вибору ліцензійного файлу

В цьому вікні вказується повний шлях до цього файлу з ліцензією, включаючи і назву самого файлу. Потрібно натиснути кнопку «Next>». Відкриється вікно установки продукту, рисунок 4.6:

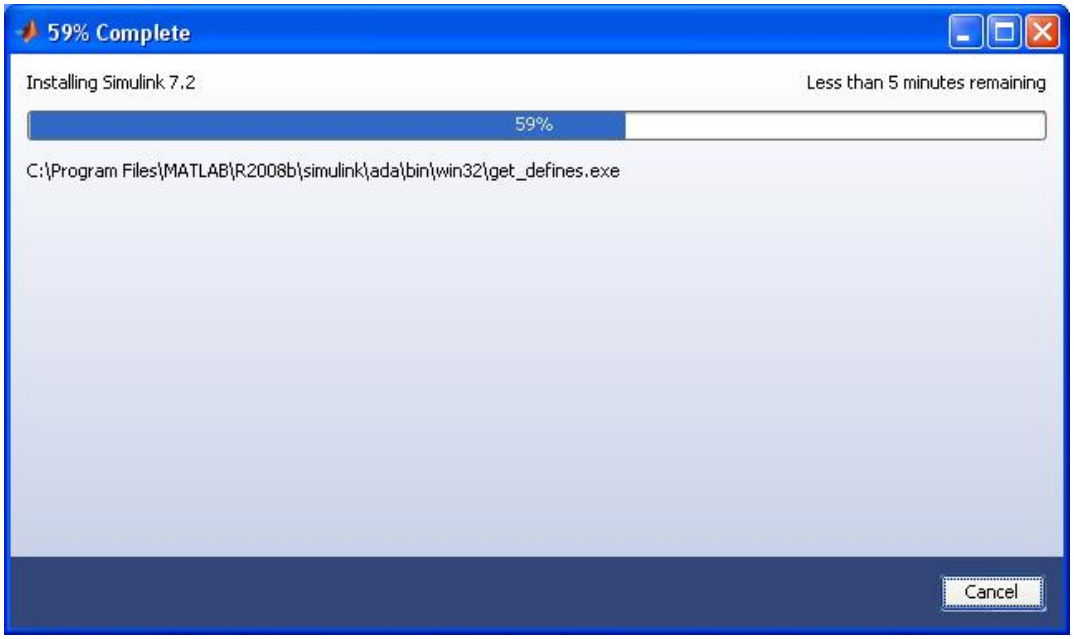

Рисунок 4.6 – Вікно встановлення програмного продукту

Після завершення процесу встановлення відкриється вікно, рисунок 2.7:

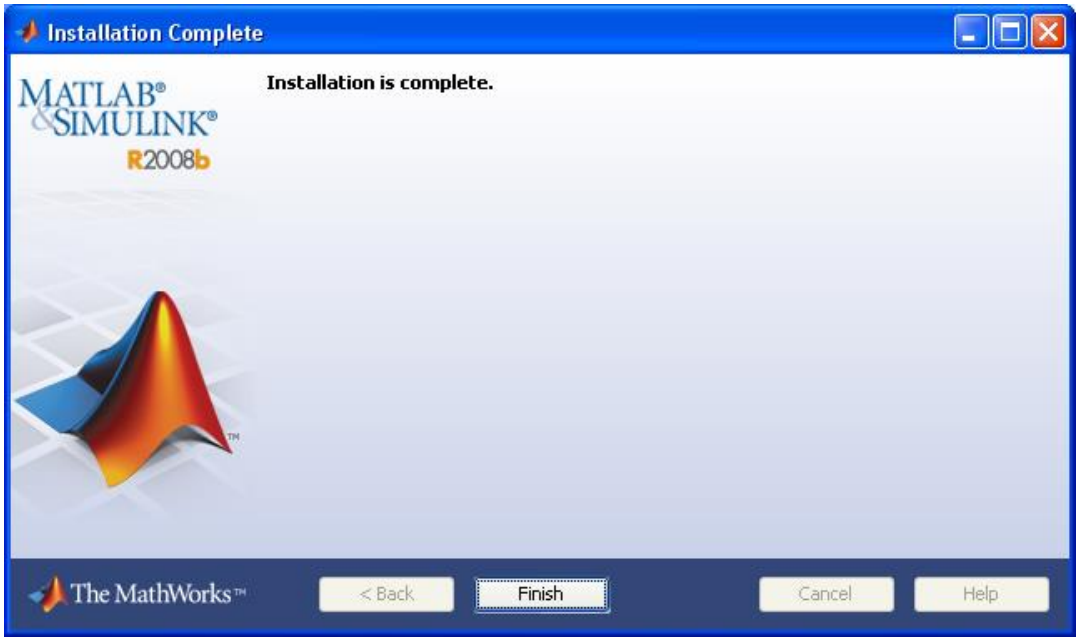

Рисунок 4.7 – Завершення встановлення програми

У даному вікні потрібно натиснути кнопку «Finish» для закриття цього вікна і завершення установки даного продукту.

4.2. Характеристика середовища Matlab та допоміжного пакету Optimization Toolbox

Matlab (скорочено від Matrix Laboratory, розроблена фірмою The MathWorks, Inc. (США, м. Нейтік, шт. Массачусетс)) – найбільш розвинена система програмування для науково-технічних розрахунків, доповнена до теперішнього часу кількома десятками більш спеціалізованих додатків, що відносяться до обчислювальної математики, обробки інформації, конструювання електронних приладів, економіки та ряду інших розділів прикладної науки.

Matlab призначений насамперед для програмування чисельних алгоритмів. Він розробляється вже більше 15 років і виник на основі більш ранніх прикладних пакетів LINPACK і EIGPACK, створених в 1970-і рр. в США, і в свою чергу вплинув на появу таких систем, як MathCad, MAPLE і Mathematica. Удосконалення системи Matlab відбувалося як у зв'язку з досягненнями в обчислювальній математиці, так і у зв'язку із змінами в архітектурі персональних комп'ютерів і розвитком загальносистемних засобів. З часом Matlab був доповнений цілим рядом вже згадуваних додатків (toolboxes), що збільшили межі його застосовності.

Matlab – система програмування високого рівня, що працює як інтерпретатор і включає великий набір інструкцій (команд) для виконання найрізноманітніших обчислень, завдання структур даних та графічного представлення інформації. Команди ці розбиті на тематичні групи, розташовані в різних директоріях системи. Зараз у системі налічується близько 800 команд, і приблизно половина з них цілком доступна починаючому користувачеві. Команди з великим можливим обсягом обчислень написані на мові програмування С, тому система виявляється майже відкритою для користувача.

Є великі можливості для виведення двовимірної і тривимірної графіки і засоби управління нею. Користувач може без особливих труднощів додавати свої команди і писати програми в термінах вже існуючих команд. Стислість і наочність програмування і виняткові можливості візуалізації результатів роблять систему дуже ефективною при пошуках і апробації нових алгоритмів, при проведенні разових розрахунків і в навчальному процесі, оскільки її можна освоювати без попереднього знайомства з основами програмування й виконувати такі складні приклади, які неможливо робити з використанням інших систем.

Робота з системою в режимі прямих обчислень носить діалоговий характер. Користувач набирає на клавіатурі вираження, що обчислюється, редагує його в командному рядку і завершує введення натисненням клавіші enter.

При цьому:

- для вказівки введення початкових даних використовується символ»;
- дані вводяться за допомогою найпростішого рядкового редактора;
- для блокування виведення обчислень деякого виразу після нього треба встановити знак; (крапка з комою);
- якщо не вказана змінна зі значенням результату обчислень, то Matlab призначає таку змінну з ім’ям ans;
- знаком привласнення є звичний математиці знак рівності =, а не комбінований знак: =, як в багатьох інших математичних системах;
- вбудовані функції (наприклад, sin) записуються малими буквами і їх аргументи вказуються в круглих дужках;
- результат обчислень виводиться в рядках висновку (без знаку»);
- діалог відбувається в стилі «задав питання – отримав відповідь».

Для вирішення оптимізаційних задач у середовищі Matlab використовується пакет оптимізації Optimization Toolbox.

Пакет оптимізації (Optimization Toolbox) – це бібліотека функцій, що розширює можливості системи Matlab в області чисельних розрахунків та

призначена для вирішення задач оптимізації і систем нелінійних рівнянь. Підтримує основні методи оптимізації функцій ряду змінних:

- безумовна оптимізація нелінійних функцій;
- метод найменших квадратів;
- вирішення нелінійних рівнянь;
- лінійне програмування;
- квадратичне програмування;
- умовна мінімізація нелінійних функцій;
- методи мінімаксу;
- багатокритеріальна оптимізація.

Цей пакет дає можливість вирішувати задачі мінімізації функцій знаходження розв'язків рівнянь, задачі апроксимації («корекції» кривих під експериментальні дані). Всі функції, які використовуються в цьому пакеті, призначені для розв'язування задач мінімізації. Тому якщо необхідно розв'язати задачу максимізації, то досить перед цільовою функцією поставити знак «мінус» і скористатися однією з наявних функцій мінімізації.

Matlab і Optimization Toolbox надають фінансовим аналітикам, інженерам та дослідникам засоби, необхідні для пошуку оптимальних та компромісних рішень, дозволяють налаштовувати та проводити діагностику задач оптимізації і швидко об'єднувати стандартні алгоритми оптимізації за своїми власними методами. Використовуючи функції результату можна зберігати параметри ітераційного процесу і створювати власні критерії зупинки розрахунку. Функції Optimization Toolbox написані на відкритій мові Matlab, що дозволяє користувачеві контролювати виконання алгоритму, змінювати вихідний код, а також створювати власні функції і алгоритми.

4.3 Функція linprog та її застосування у вирішенні задач лінійного програмування у Matlab

Для розв'язання задач лінійного програмування у пакеті оптимізації Optimization Toolbox використовується функція linprog. Вона призначена для розв'язування задачі виду:

$$f(x) = \sum_{j=1}^{n} c_j x_j = \langle c, x \rangle \to \min, \tag{4.1}$$

$$A \cdot x \le b, \tag{4.2}$$

$$Aeq \cdot x = beq, \tag{4.3}$$

$$lb \le x \le ub, \tag{4.4}$$

де *c, x, b, beq, lb, ub* – вектор-стовпчики, *A, Aeq* – прямокутні матриці, і яка має такий синтаксис:

```
x = linprog (c, A, b, Aeq, beq);
x = linprog (c, A, b, Aeq, beq, lb, ub);
x = linprog (c, A, b, Aeq, beq, lb, ub, x0);
x = linprog (c, A, b, Aeq, beq, lb, ub, x0, options);
[x, fval] = linprog(…);
[x, fval, exitflag] = linprog(…);
[x, fval, exitflag, output] = linprog(…);
[x, fval, exitflag, output, lambda] = linprog(…).
```

Розглянемо особливості параметрів exitflag, lambda, output, які використовуються в функції linprog. Так параметр exitflag приймає додатне значення, якщо ітераційний процес завершився у відповідності до заданої точності обчислень; від'ємне значення, якщо ітераційний процес не збігається до розв'язку, і 0, якщо було перевищено максимальну кількість ітерацій, яка

визначається за параметром MaxIten, або максимальну кількість обчислень значень цільової функції, яка визначається за параметром MaxFunEvals.

Параметр lambda являє собою структуру з полями, які містять множники Лагранжа для кожної групи обмежень задачі в точці x, що є результатом розв'язування поставленої задачі:

- ineqlin – для обмежень-нерівностей,
- eqlin – для обмежень-рівнянь,
- upper – для прямих обмежень типу $x \leq ub$,
- lower – для прямих обмежень типу $lb \leq x$,

При цьому ненульові елементи векторів у полях параметра lambda відповідають активним обмеженням для знайденої точки x.

Якщо в умові задачі деякі вхідні дані відсутні, то замість відповідних величин треба ставити []. Наприклад, якщо в умові задачі (2.1) – (2.4) відсутні обмеження-нерівності виду (2.2), то треба ввести A=[] і b=[].

Функція може використовувати алгоритм великої розмірності lipsol або алгоритм середньої розмірності (метод проекцій).

5 ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою дипломної роботи є розробка політика безпеки для організації з застосуванням теорії ігор та проведення оцінки точності методу для реальних даних. Середовищем розробки було обрано був обраний математичний пакет Matlab.

5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Реалізація та тестування моделі визначення авторства можна поділити на декілька етапів, що дозволяє полегшити і структурувати виконання поставленого завдання.

Основні етапи такі:

1. Пошук літературних джерел з області дослідження.
2. Обґрунтування моделі класифікації.
3. Вибір середовища розробки програмного забезпечення.
4. Розробка програми.
5. Тестування розробленої моделі на реальному датасеті.
6. Дослідження впливу на точність розмірності простору ключових слів та деяких етапів нормалізації текстових даних.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу.

Виконавцем усіх операцій по розробці програмного забезпечення є інженер-програміст.

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та їх час виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Пошук літературних джерел з області дослідження.	Інженер-програміст	27
2.	Обґрунтування моделі класифікації.	Інженер-програміст	18
3.	Вибір середовища розробки програмного забезпечення.	Інженер-програміст	9
4.	Розробка програми.	Інженер-програміст	54
5.	Тестування розробленої моделі на реальному датасеті.	Інженер-програміст	20
6.	Дослідження впливу на точність розмірності простору ключових слів та деяких етапів нормалізації текстових даних.	Інженер-програміст	12
Разом			140

Загальні затрати часу на реалізацію даної роботи становить 140 години, найбільш трудомістким є власне розробка програмного забезпечення – 54 години.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його. Заробітна плата складається з основної та додаткової оплати 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. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

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.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2019 рік», зокрема статтею восьмою мінімальна заробітна плата у погодинному розмірі становить 25,13 грн. Згідно з Єдиною тарифною сіткою розрядів та коефіцієнтів з оплати праці працівників та організацій окремих галузей бюджетної сфери установ розроблені рекомендовані тарифні розряди, що приблизно відповідають наступним межам погодинної оплати: керівник дипломної роботи – 30,00...50,00 грн./год., інженер-програміст першої категорії– 25,13...30,00 грн./год., консультант – 25,13...30,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \,, \qquad (5.1)$$

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

Оскільки всі види робіт в виконує розробник-програміст, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 25{,}13 \cdot 140 = 3518{,}2 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (5.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод} = 3518{,}2 \cdot 0{,}15 = 527{,}73 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (5.3)$$

$$В_{о.п.} = 3518{,}2 + 527{,}73 = 4045{,}93 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

- єдиний соціальний внесок ЄСВ (прибутковий податок) – 22%;
- військовий збір – 1,5%.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{оп} \cdot 0{,}235 \quad (5.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$В_{с.з.} = 4045{,}93 \cdot 0{,}235 = 950{,}79 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці наведено у таблицю 5.2.

Таблиця 5.2 – Розрахунки витрат на оплату праці

з/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Відрахування $Ф_{ОП}$, грн.	Всього витрати на плату праці, грн. (6=3+4+5)
		Тарифна ставка, грн.	Кількість відпрацьованих год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1.	Програміст (розробник)	25,13	140	3518,2	527,73	950,79	4996,72

З таблиці розрахунки витрат на оплату праці видно що всього витрати на плату праці становить 4996,72 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{ві} = q_i \cdot p_i \,, \tag{5.5}$$

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

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum М_{ві} \,. \tag{5.6}$$

Розрахунки занесемо у таблицю 5.3.

Таблиця 5.3 – Розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Один. виміру	Норма витрат	Ціна за один., грн.	Затрати матер., грн.	Транс-портно-заготівель-ні витрати, грн.	Загальна сума витрат на матер., грн.
1. Основні матеріали						
Використання мережі Internet	години	120	–	120	–	120
MathType subscription	шт.	1	1325,93 грн.	1325,93 грн.		1325,93 грн.
2. Допоміжні витрати						
Папір формату А4	шт.	160	0,3	48	–	48
Разом:						1373,93

Загальні матеріальні витрати на Internet і Папір формату А4 становить 1373,93 грн.

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S \,, \qquad (5.7)$$

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 1,68грн.

Потужність комп'ютера для створення дипломної роботи – 80 Вт, кількість годин роботи обладнання згідно таблиці 5.1 –150 години.

Тоді,

$$З_в = 0{,}08 \cdot 140 \cdot 1{,}68 = 18{,}82 \text{ грн.}$$

Згідно формули затрати на електроенергію де необхідна потужність множиться на кількість годин на реалізацію розробки і множиться на вартість кіловат-години електроенергії що в висновку дорівнює 18,82 грн.

5.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їхнього повного відновлення.

Для визначення амортизаційних використовується формула:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (5.8)$$

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 %).

Для даної дипломної роботи засобом розробки є комп'ютер. Його вартість становить 18000 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 18000 \cdot 5\% / 100\% = 900{,}00 \text{ грн.}$$

Оскільки робота виконувалась 140 години, а в місяць є 196 робочих годин, то амортизаційні відрахування будуть становити:

$$A = 900{,}00 \cdot 140 / 196 = 642{,}86 \text{ грн.}$$

Згідно формули для визначення амортизаційних де $Б_В$ множиться $Н_А$ і ділиться на 100% амортизація розробки становить 642,86 грн.

5.6 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.

$$Н_в = В_{о.п.} \cdot 0{,}2 \ldots 0{,}6 \,, \qquad (5.9)$$

де $Н_в$ – накладні витрати.

Отже, накладні витрати:

$$Н_в = 4045{,}93 \cdot 0{,}2 = 809{,}19 \text{ грн.}$$

Накладні витрати згідно розрахунку формули, становить 809,19 грн.

5.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці $B_{о.п}$	4045,93	51,61%
Відрахування на соціальні заходи $B_{с.з}$	950,79	12,15%
Матеріальні витрати $З_{м.в}$	1373,93	17,53%
Витрати на електроенергію $З_{в}$	18,82	0,25%
Амортизаційні відрахування $А$	642,86	8,21%
Накладні витрати $Н_{в}$	809,19	10,15%
Собівартість $С_{в}$	7841,52	100,00%

Собівартість ($С_{в}$) роботи розрахуємо за формулою:

$$С_{в} = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_{в} + А + Н_{в} \quad (5.10)$$

Отже, собівартість роботи дорівнює:

$$С_{в} = 4045,93+950,79+1373,93+18,82+642,86+809,19= 7841,52 \text{ грн.}$$

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 7841,52 грн.

5.8 Розрахунок ціни науково-дослідної роботи

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

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ) \tag{5.11}$$

де $P_{рен.}$ – рівень рентабельності, 30 %, $ПДВ$ – ставка податку на додану вартість, (20 %).

Звідси ціна на роботу складе:

$$Ц = 7841{,}52 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 12232{,}77 \text{ грн.}$$

Загальний розрахунок ціни програмного продукту становить 12232,77 грн.

5.9 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 (E_p) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = \frac{П}{C_B}, \tag{5.12}$$

де $П$ – прибуток; C_B – собівартість.

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

$$П_{пл} = Ц - С_в \ . \quad (5.13)$$

Розраховуємо плановий прибуток:

$$П_{пл} = 12232,77 - 7841,52 = 4391,25 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{С_в} \ . \quad (5.14)$$

Тоді,

$$E_р = 4391,25/ 7841,52 = 0,56.$$

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

$$T_р = \frac{1}{E_р} \ , \quad (5.15)$$

Термін окупності дорівнює:

$$T_р = 1 / 0,56 = 1,79 \text{ р.}$$

Згідно формул плановий прибуток від розробки становить 4391,25 грн., економічна ефективність дорівнює 0,56 а термін окупності становить 1,79 роки що вважається доцільним та економічно вигідним.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

6.1.1 Характеристика дій безпосереднього керівника робіт та роботодавця у випадку настання нещасного випадку на виробництві

При настанні нещасного випадку на виробництві, на нього повинні реагувати багато учасників посттравматичного ефекту. У першу чергу, це безпосередній керівник та роботодавець підприємства. Порядок проведення розслідування та ведення обліку нещасних випадків, професіональних захворювань і аварій на виробництві затверджений постановою КМУ від 30.11.2011 р. № 1232.

Керівник якнайшвидше має організувати надання першої медичної допомоги потерпілому. При потребі керівник має забезпечити доставку потерпілого до медичного пункту. Керівник зобов’язаний розібратися у тому, що трапилося, та бути присутнім при госпіталізації. Він має діяти від імені Компанії перед будь якими третіми особами. Якщо інцидент стався на території Компанії, то потрібно прикласти максимально зусиль для знаходження свідків. Якщо інцидент стався поза межами Компанії, то керівник має записати паспортні дані, номери телефонів та машин. Також керівник має повідомити про інцидент роботодавця. Якщо обстановка та стан робочого місця не наштовхує на небезпеку інших працівників, то потрібно місце, яке призвело до нещасного випадку зберегти до прибуття комісії.

Після отримання повідомлення про нещасний випадок роботодавець повинен протягом години через засоби зв’язку повідомити відповідні органи, а також протягом доби відправити повідомлення про інцидент на паперовому носії. У обов’язки роботодавця також входить утворити незалежну комісію та організувати розслідування інциденту[20].

У склад комісії має входити:

Голова Комісії: керівник служби охорони праці Компанії.

Члени Комісії: керівник структурного підрозділу, в якому стався нещасний випадок; уповноважений трудового колективу з питань охорони праці; спеціаліст санепідемстанції (у разі гострих професійних отруєнь (захворювань).

Якщо постраждалий потрапив у лікарню, роботодавець має надає письмовий запит до лікувального закладу з проханням видати висновок про ступінь тяжкості травми.

Якщо стався груповий нещасний випадок, який закінчився смертю або тяжкими тілесними пошкодженнями, то роботодавець повинен повідомити відповідний місцевий орган державного нагляду за охороною праці, місцевий орган державної виконавчої влади, прокуратуру за місцем знаходження Компанії та Держнаглядохоронпраці. Якщо інцидентом являється отруєння, то роботодавець має також повідомити санепідемстанцію. Якщо люди загинули від гострого професійного отруєння, то роботодавець має повідомити МОЗ.

Якщо розслідування закінчилося, то роботодавець повинен на протязі доби затвердити три примірники акту по форма Н-5. Якщо нещасний випадок визнано пов’язаний із виробництвом то складається сім примірників акту про нещасний випадок на виробництві по формі Н-1, які складаються Комісією з розслідування нещасного випадку. У такому випадку, потерпілому або його родині будуть виплачуватися всі необхідні витрати та відшкодовуватися отримана шкода, передбачені законодавством, за рахунок кошті Фонду соціального страхування від нещасних випадків на виробництві та профзахворювань.

Один примірник акту Н-1 та Н-5, разом із матеріалами розслідування роботодавець має зберігати не менше 45 років, а якщо реорганізації чи ліквідації Компанії документи повинні передаватися правонаступнику або до державного архіву. Решта примірників актів роботодавець розсилає адресатам Комісією з розслідування нещасного випадку.

6.1.2 Аналіз основних особливостей стандарту OHSAS 18001 щодо ведення та управління документацією з охорони праці

OHSAS 18001 – це британський стандарт в якому описується розробка та впровадження систем управління охороною здоров'я і безпекою праці на підприємстві. OHSAS - це абревіатура від англійського «Occupational Health and Safety Management Systems» - що так і перекладається «Система управління гігієною та охороною праці».

У цьому стандарті описані вимоги щодо гігієни та безпеки роботи, для того щоб, організація могла покращити свою діяльність та зменшити ризики нещасного випадку . У стандарті немає вимог щодо розробки системи управління. Вона містить у собі вимоги щодо гігієни і безпеки роботи, аніж безпека продукції та наданих послуг.

З допомогою стандарту OHSAS 18001 організація може забезпечити безпечні умови роботи, знизить кількість нещасних випадків і відповідати законодавству.

Стандарт OHSAS 18001 має багато переваг, до яких відноситься [22]:

Скорочення кількості нещасних випадків і професійних захворювань.

Скорочення періоду простоїв і пов’язаних із ними витрат, у томи числі щодо страхування.

Більш ефективне управління ризиками для здоров’я та виробничої безпеки.

Покращення позитивного іміджу компанії в результаті прихильності до охорони праці та забезпечення виробничої безпеки.

Підвищення лояльності ділових партнерів і розширення кола нових клієнтів.

Стандарт OHSAS 18001 також містить у собі схему дій, заходи управління факторами, що впливають на виникнення небезпечних ситуацій.

Порядок управління документацією з охорони праці містить кілька розділів [23]:

Розділ «Область застосування».

Розділ «Термін та визначення».

Розділ «Позначення та скорочення».

Розділ «Вимоги».

У розділ «Область застосування» мають входити вимоги щодо управління документацією та дія має розповсюджуватися на всі підрозділи. У документації мають проходити зміни якщо є нові затвердженні, скасовані чи введені в дію документи, надходження нового документа щодо управління охороною праці в організації, або ж надходження відповідних вказівок або розпоряджень від керівництва.

У розділі «Термін та визначення» мають бути описані найчастіше вживані терміни з їхніми визначеннями.

Розділ «Позначення та скорочення» містить у собі абревіатури з їхніми визначеннями та скорочення.

У розділі «Вимоги» описаний порядок управління документацією з охорони праці. Порядок має свої положення та визначає реалізацію:

На підприємстві встановлюється певна ієрархія документації: Положення про систему управління охороною праці.

Процедурні документи з описом операцій, які оформлюються у визначеній формі.

Інструктивні документи.

Записи та інша супутня документація (колективний договір, програма заходів з управління, плани роботи підприємства з питань, суміжних із забезпеченням охорони праці, службові записки, переліки, реєстри, запити та відповіді на них тощо).

У записи та іншої документації з охорони праці можна включати акти про нещасні випадки та професійні захворювання, додаткові матеріали щодо інциденту, протоколи нарад, результати перевірки знань з охорони праці, картки видачі індивідуального захисту, звіти, результати атестації робочих місць, оцінювання ризиків, аудит та матеріали перевірок керівництвом.

Ведення записів дозволяє аналізувати результативність, ефективність впровадження системи управління та вибрати заходи щодо вдосконалення, виявляти причини та проаналізувати невідповідності, створити свій метод одержання достовірної інформації.

Записи мають вестися як і на паперових, так і на електричних носіях для подальшого аналізу та при необхідності бути підтвердженими у юридичних осіб. Основним нюансом є те, що записи не можуть бути зміненими.

Якщо організація буде виконувати вимоги та відповідати створеному OHSAS 18001, то це автоматично знизить ризик бути оштрафованими або потрапити під правову відповідальність і судові розгляди, якщо виникнуть нещасні випадки. Впровадження OHSAS 18001 – це довгострокова стратегія щодо безпеки працівників.

6.2 Безпека в надзвичайних ситуаціях

6.2.1 Оцінка надійності захисту виробничого персоналу і її послідовність

Якщо оцінювати надійсність захисту робочого персоналу, то потрібно брати до уваги те, що надзвичайні ситуації можуть призвести до втрати працездатності, важкого ураження тіла або смерті людей [26].

Надійність захисту персоналу може показати, наскільки стійке підприємство до надзвичайних ситуацій у мирний час.

Для ефективного захисту людей потрібно укривати персонал у захисних спорудах та дотримуватися таких умов:

Захисні споруди повинні забезпечувати захист для всього робочого персоналу.

Захисні споруди повинні забезпечувати захист від усіх видів надзвичайних ситуацій.

Захисні споруди мають мати систему життєзабезпечення на всю тривалість перебування.

ЗС мають не далеко розміщуватися від робочих місць, щоб робітники вчасно могли укрилися.

Весь персонал має знати правила дії при сигналах про НС.

Показник надійності захисту виробників можна взяти коефіцієнт надійності захисту К_(Н.З.), який показує яка кількість робітників надійно захищена.

Коефіцієнт надійності виробників визначається на основі кількох показників, які показують загальну підготовленість об'єкту до завдань захисту.

Оцінка надійності захисту персоналу проводиться у наступній послідовності:

Інженерний захист робітників визначається за формулою:

$$К_{(інж.зах.)}=К_{(інж.зах.)}/N \quad (6.1)$$

де К_(інж.зах.) – частина персоналу працюючої зміни, що може своєчасно укритися в ЗС з достатнім захистом та системою життєзбезпечення;

N– чисельність найбільшої працюючої зміни.

Визначається система сповіщення, та час донесення сигналу сповіщення до робітників. Показником сповіщення є коефіцієнт:

$$К_СП=К_СП/N \quad (6.2)$$

Вивчається дії робочого персоналу після отримання сигналу сповіщення. Визначається коефіцієнтом навченості:

$$К_НАВЧ=К_{(НАВЧ.)}/N \quad (6.3)$$

Визначається готовність сховища до прийому робітників. Для цього потрібно визначити час, за який сховища, які використовуються у подвійному призначення можуть бути підготовленні до прийому людей (заповнюється

запас їжі, води, перевірка герметичності та функціонування систем життєдіяльності). Потрібно порівняти фактичний час підготовки сховища з потрібним часом для підготовки сховища. Для оцінки надійності будуть включатися лише сховище для яких:

$$Ч\_(гот.фак.)/Ч\_(гот.пот.) < 1 \quad (6.4)$$

Показником надійності захисту з урахуванням готовності є коефіцієнт готовності:

$$К\_гот = К\_гот/N \quad (6.5)$$

На основі окремих показників визначається коефіцієнт надійності захисту робітників та службовців КН.З.за мінімальним значенням окремих показників:К_(інж.зах.), К_СП., К_НАВЧ, К_гот.

Після аналізу результатів, можна визначити слабкі місця об’єкту захисту та шляхи, які покращать показники надійності захисту.

У висновках потрібно вказувати:

- Надійність захисту робітників та службовців.
- Необхідність покращення захисних споруд та заходи для підвищення надійності.
- Приміщення, які можна використовувати під захисні споруди.
- Кількість та тип захисних споруд, що швидко зводяться.
- Заходи надійного захисту персоналу чергової зміни.
- Заходи з повного забезпечення персоналу.
- Заходи покращення умов зберігання, профілактики та ремонту ЗІЗ.
- Заходи забезпечення об’єкту в умовах Р. Х. Б. З.

6.2.2 Забезпечення безпеки життєдіяльності при роботі з ПК

На сьогоднішній день комп’ютери широко застосовуються і всіх областях діяльності людини. Під час роботи з ПК на людину впливає ряд небезпечних та шкідливих факторів: електромагнітних полів, інфрачервоного випромінювання, шум і вібрація, статична електрика та ін.

При роботі з комп’ютером напружуються, перш за все, зір і м’язи рук при роботі з ПК. Також не велика розумова та нервово-емоційна нагрузка. Тому потрібно щоб робоче місце максимально відповідало вимогам.

Для зменшення зорової напруги, освітлення повинне бути змішаним. Коефіцієнт природного освітлення (КЕО) повинне бути не нижче ніж 1,5%, а при середньому зоровому навантаженні – не менше ніж 1%. В якості джерел штучного освітлення зазвичай використовуються люмінесцентні лампи типу ЛБ або ДРЛ, які попарно об'єднуються у світильники.

Залежно від орієнтації вікон потрібно використовувати такі кольори стін і підлоги:

- Вікна орієнтовані на південь – стіни потрібно закрашувати в зеленувато-блакитного або світло-блакитного колір, а підлога має бути зеленою.

- Вікна орієнтовані на північ – стіни світло-оранжевого або оранжево-жовтого кольору, а підлога – червонувато-оранжева.

- Вікна орієнтовані на схід – стіни мають мати жовто-зелене забарвлення, а підлога зелена або червонувато-оранжева.

- Вікна орієнтовані на захід – стіни покрашені в жовто-зелений або голубувато-зелений, а підлога – зелена або червонувато-оранжева.

Щоб не було болю та дискомфорту у спині потрібно щоб робоче крісло повторювало форму спини. Положення спинки крісла повинна забезпечувати нахил тіла від 97-121°. Під час напруженої роботи потрібно кожної години робити перерву тривалістю 15 хв та виконувати легкі вправи для розслаблення.

Клавіатуру слід робити окремої від екрану і рухомий. Зусилля натиску на клавіші повинно лежати в межах 0,25 - 1,5 М, а хід клавішею - 1-5 мм.

Для уникнення сутулості потрібно екран дисплея розміщати перпендикулярно до напрямку погляду. Нахил екрану має бути від -15 до +20° по відношенню до нормального його положення. Якщо монітор без захисного екрану, то в такому випадку монітор має бути розміщений на відстані витягнутої руки. Найкорисніша відстань від екрана до краю столу – 20 – 115 см.

Щоб уникнути ураження електричним струмом потрібно правильно розміщувати устаткування і кабелі, використовувати скриту електромережу, надійні розетки. Потрібно регулярно чистити комп'ютер від пилу та бруду. Щоб уникнути іскріння потрібно рідше виймати штепсельні вилки з розеток.

Дуже важливим є постачання свіжого повітря у приміщення, тому потрібно використовувати системи механічної вентиляції і кондиціонування, а також природну вентиляцію.

Рівень шуму для місця математика-програміста, інженера та операторів відеоматеріалів не повинен перевищувати 50 дБА. При підвищеному рівні шуму потрібно використовувати звукопоглинаючі матеріали. Для пониження вібрації встановлюються устаткування на спеціальні фундаменти або віброізолятори.

Якщо у приміщенні використовується більше ніж один комп'ютер, то на користувача можуть впливати випромінювання від інших робочих зон. В такому випадку потрібно використовувати спеціальні фільтри і користувач має розміщуватися від інших дисплеїв не менше ніж на один метр.

7 ЕКОЛОГІЯ

7.1 Аналіз сучасних програмних продуктів для обробки великих масивів екологічної інформації

Оперативна, якісна і точна обробка великих масивів статистичної інформації може бути виконана лише з використанням сучасних засобів обчислювальної техніки. Наявність потужних, надійних і разом з тим простих в експлуатації програмних продуктів статистичного аналізу звільняє дослідника від рутинних операцій, розширює сферу застосування статистичних методів в різних галузях людської діяльності, сприяє появі якісно нових можливостей статистичного аналізу і моделювання даних. Використання пакетів прикладних програм це єдиний реальний практичний інструмент розв'язування задач багатофакторного кореляційно-регресійного та аналізу в багатовимірному просторі.

Сучасний ринок програмних продуктів пропонує різноманітні пакети програм для статистичної обробки даних. Всесвітньо відомі статистичні пакети для комплексної обробки даних: BMDP, SPSS, SAS, Systat, Minitab, S-Plus, Statgraphics Statistica та інші.

Використання згаданих пакетів програм дає змогу автоматизувати процес статистичного дослідження в таких напрямах:

- створення файлів даних і таблиць;
- групування даних;
- графічний аналіз даних;
- розрахунок варіаційних характеристик вибіркових сукупностей;
- побудова рядів розподілу;
- аналіз рядів динаміки і прогнозування їх майбутніх рівнів;
- кореляційно-регресійний аналіз;
- багатомірний аналіз.

З 1995 р. Світовим лідером на ринку статистичного програмного забезпечення визнається інтегрована система Statistical для Windows (версія 5.0), розроблена фірмою Stat Soft. Перша версія програми з'явилася у 1991р. для операційної системи MS-DOS і була новим напрямом розвитку статистичного програмного забезпечення. В ній реалізовано графічно-орієнтований підхід до статистичного аналізу даних, суть якого полягає в отриманні всебічного візуального представлення інформації на всіх етапах статистичної обробки даних.

Багатофункціональна, графічно орієнтована на обробку масових даних система Statistica відповідає основним стандартам Windows (динамічний обмін даними з іншими додатками, підтримка основних операцій з буфером обміну, робота в мережевому середовищі та інші).

Передусім це стандарти користувацького інтерфейсу — MDI, використання буфера-обміну, механізму динамічного зв'язку (DDE) з іншими додатками; система підтримує всі операції, реалізовані за допомогою методу Drag-and-Drop — «Перетягти та опустити», включаючи автозаповнення, інші.

Складніші процедури обробки даних у системі Stratgraphics виконує спеціалізований модуль Data Management — «Управління даними», а для обробки великих масивів даних або даних з довгими текстовими значеннями застосовують процедури Megafile Manager Data — «Менеджера метафайлів».

Система Stratgraphics працює з чотирма типами документів. Це:

- електронна таблиця Spreadsheet, призначена для введення і перетворення первинних даних;
- електронна таблиця Scrollsheet — для виведення результатів аналізу;
- графік — для візуалізації результатів обробки та аналізу даних; звіт — файл у формі RTF (розширений текстовий формат), в якому зберігається текстова, числова і графічна інформація.

Усі статистичні процедури системи розбито на окремі модулі, кожен з яких об'єднує групу логічно зв'язаних між собою статистичних методів і в

рамках конкретної моделі забезпечує повний і всебічний аналіз закономірностей.

Модуль Multiple Regression — «Множинна регресія» включає:

- вичерпний набір засобів множинної лінійної і нелінійної регресії,
- багатофакторного прогнозування,
- аналіз залишків і викидів,
- тестування гіпотез регресійного аналізу.

Модуль Time Series/Forecasting — «Часові ряди і прогнозування» об'єднує процедури аналізу закономірностей динаміки: тенденцій розвитку і коливань, різні методи згладжування рядів, описування трендів, описування сезонної декомпозиції, методи авторегрсійного аналізу, методи прогнозної екстраполяції.

Система Statistica включає модуль Anova/Manova — «Дисперсійний аналіз», увесь арсенал методів багатовимірного аналізу (кластерний, дискримінантний, факторний аналіз, факторне шкалювання, канонічні кореляції).

Особливе місце посідає модуль Sepath — «Моделювання взаємозв'язків системами структурних рівнянь».

Зазначені модулі покривають практично весь спектр сучасних методів статистичного дослідження і моделювання. Запуск модуля здійснюється через перемикач модулів — Module Swither. У кожному модулі робота починається із «Стартової панелі», де відкривається файл первинних даних, вибирається процедура обробки даних і визначаються відповідні їй параметри.

У системі Statistica реалізовано принцип постійного логічного підказування. Якщо користувач не може визначитися щодо наступного кроку діалогу, через команду Enter система сама спрямує до відповідного діалогового вікна. Якщо виникають складнощі з вибором параметрів обчислювальної процедури, вони задаються системою «за умовчуванням».

Використання сучасних комп'ютерних технологій обробки даних, перетворюють статистичний аналіз, моделювання та прогнозування в захоплююче дослідження закономірностей навколишнього світу.

7.2 Вимоги до моніторів (ВДТ) та ПЕОМ

Конструкція монітора (відео термінального пристрою - ВДТ) повинна забезпечувати можливість фронтального спостереження екрана шляхом повороту корпуса в горизонтальній площині навколо вертикальної осі в межах ± 30 ° і у вертикальній площині навколо горизонтальної осі в межах ± 30 ° з фіксацією в заданому положенні. Дизайн моніторів повинен передбачати фарбування в спокійні м'які тони з дифузійним розсіюванням світла. Корпус монітора і ПЕОМ, клавіатура повинні мати матову поверхню одного кольору з коефіцієнтом відображення 0,4 - 0,6 і не мати блискучих деталей, здатних створювати відблиски.

Конструкція ВДТ повинна передбачати наявність ручок регулювання яскравості і контрасту, що забезпечують можливість регулювання яскравості і контрасту, що забезпечують можливість регулювання цих параметрів від мінімальних до максимальних значень.

ВДТ і ПЕОМ повинні забезпечувати потужність експозиційної дози рентгенівського випромінювання в будь-якій точці на відстані 0,05 м. від екрана і корпуса монітора при будь-яких положеннях регулювальних пристроїв не повинна перевищувати 7,74 х10 А / кг, що відповідає еквівалентній дозі, рівної 0,1 мбер / год (100 мкР / год). В таблиці 7.1 наведено межі параметрів ВДТ.

Таблиця 7.1 - Візуальні ергономічні параметри ВДТ і межі їх змін

Найменування параметрів	Межі значень параметрів	
	Мінім.	Макс.
Яскравість знака (яскравість фону), кд / кв. м. (вимірювана в темряві)	35	120
Зовнішня освітленість екрана, лк	100	250
Кутовий розмір знака, кут. Мін.	16	60

1. Оптимальним діапазоном значень візуального ергономічного параметра називається діапазон, в межах якого забезпечується безпомилкове зчитування інформації при часі реакції людини - оператора, що перевищує мінімальний, встановлений експериментально для даного типу ВДТ, не більше, ніж в 1,2 рази.

2. Допустимим діапазоном значень візуального ергономічного параметра називається діапазон, при якому забезпечується безпомилкове зчитування інформації, а час реакції людини - оператора перевищує мінімальний, встановлений експериментально для даного типу ВДТ, не більше, ніж у 1,5 рази.

3. Кутовий розмір знака - кут між лініями, що з'єднують крайні точки знака по висоті і очей спостерігача. Кутовий розмір знака визначається за формулою: a = arctg (h / 2 l), де h - висота знака, l - відстань від знака до ока спостерігача.

Дані, наведені в таблиці 7.2, підлягають коригуванню у міру введення в дію нових стандартів, що регламентують вимоги і норми на візуальні параметри ВДТ.

Таблиця 7.2 - Нормовані візуальні параметри відеодисплейних терміналів

№ п/п	Найменування параметрів	Значення параметрів
1	Контраст (для монохромних ВДТ)	Від 3: 1 до 1,5: 1
2	Нерівномірність яскравості 2 / елементів знаків,%	не більше ± 25
3	Нерівномірність яскравості 2 / робочого поля екрану,%	не більше ± 20
4	Формат матриці знаку для великих літер і цифр, (для відображення діакритичних знаків і малих літер з нижніми виносними елементами формат матриці повинен бути збільшений зверху чи знизу на 2 елементи зображення)	не менше 7 * 9 елементів зображення не менше 5 * 7 елементів зображення
5	Відношення ширини знака до його висоти для великих літер	від 0,7 до 0.9 (допускаєтьсявід 0,5 до 1,0)
6	Розмір мінімального елемента відображення (пікселя) для монохромного ВДТ, мм	0,3
7	Кут нахилу лінії спостереження, град.	не більше 60 град нижче горизонталі
8	Кут спостереження, град.	не більше 40 град. від нормалі до будь-якій точці екрану дисплея
9	Допустиме горизонтальне зміщення однотипних знаків,% від ширини знака	не більше 5
10	Допустиме вертикальне зміщення однотипних знаків,% від висоти матриці,	не більше 5

ВИСНОВКИ

У даній роботі було розглянуто і проаналізовано підхід до вирішення проблеми побудови системи захисту інформації за умови обмеженості ресурсів та розроблено алгоритм мінімізації ризиків на основі методів експертної оцінки, теорії ігор та математичного програмування.

В результаті виконання дипломної роботи було:

- проведено літературних джерел в області досліджень;
- досліджено математичні підходи для формування політики безпеки;
- розглянуто модель загроз та порушника;
- створено математичну модель у формі гри конфліктуючих сторін – захисника та зловмисника;
- запропоновано метод мінімізації ризиків в залежності від виділених ресурсів.
- проведено вибір компонентів системи захисту організації для практичної задачі на основі оцінок ризиків та ефективності тих чи інших засобів захисту, доступних в інтернеті.

Крім того в роботі в спеціальній частині описано середовище розробки Matlab та функції, які використовуються для розв’язку задач математичного програмування.

В розділі "Обґрунтування економічної ефективності" проведено оцінку основних показників економічної ефективності проекту.

В підрозділі "Охорона праці" висвітлено питання, що стосуються стандарту OHSAS 18001 та дій керівництва у разі нещасного випадку на виробництві. В підрозділі "Безпека життєдіяльності" описано надійність захисту персоналу та питання безпеки життєдіяльності при роботі з ПК

В розділі "Екологія" проведено аналіз сучасних програмних продуктів для обробки великих масивів екологічної інформації та наведено вимоги до моніторів.

Використання математичного апарату теорії ігор, у тому числі максимінної стратегії, забезпечує отримання мінімального гарантованого значення ризику інформації, що відрізняє розроблений підхід від методів експертної оцінки.

Розроблений підхід є гнучким, що дозволяє змоделювати поведінку порушників різного типу.

БІБЛІОГРАФІЯ

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. — К.: BHV, 2009. — 608 с.

2. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності ін- формації в комп'ютерних системах від несанкціоно- ваного доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р., № 22

3. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р., № 22.

4. ISO/IEC27035. Information technology. Security techniques. Information security incedent management.–2011.–78p.

5. LandollD. The security risk assessment handbook: a complete guide for performing security risk assessments /Douglas J.Landoll. –BocaRaton: Auerbach Publications, 2016.–504p.

6. Rittinghouse J.W. Business continuity and disaster recovery for infosec managers / JohnW. Rittinghouse,J amesF.Ransome. –Oxford:Elsevier,2015.–408p.

7. SpeddingL. Business risk management handbook: a sustainable approach / Linda Spedding, Adam Rose.–Oxford:Elsevier,2018.–768p.

8. Андрианов В.В. Обеспечение информационной безопасности бизнеса/ В.В.Андрианов, С.Л.Зефиров, В.Б.Голованов.–М.:ЦИПСиР,2016.–373с.

9. БалашовП.А.Оценкарисковинформационнойбезопасностинаосновене четкойлогики/П.А.Балашов,В.П.Безгузиков,Р.И.Кислов//[Електроннийресурс]. –режимдоступу:http://www.nwaktiv.ru/textstat2/index.html

10.Рябинин И.А. Научная Школа «Моделирование и Анализ Безопасности и Риска в Сложных Системах» и ее смысл // Труды четвертой Международной науч- ной школы МА БР 2004, июнь 22–25, 2004. — 650 с.

11.Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2013. No

1 (49). – С.15-26.

12.Владимирцев А.В., Марцынковский О.А. Использование метода экспертных оценок при анализе и оценке рисков системы менеджмента.– Ассоциация по сертификации «РусскийРегистр» – Санкт-Петербург: 2017.– 425с.

13.Гарасим Ю.Р. Аналіз систем захисту, які мають властивість живучості /Ю.Р.Гарасим// Військово-технічнийзбірник.–2016.No1(4).–С.87–95.

14.Гарасим Ю.Р. Забезпечення живучості та неперервності функціонування систем захисту інформації /Ю.Р.Гарасим, В.А.Ромака, М.М.Рибій//Вісник Нац.ун-ту “Львівськаполітехніка” “Автоматика, вимірювання та керування”. –2014.– No741.– С.105-112.

15.Дубинин Е.А. Оценка относительного ущерба безопасности информационной системы: монография /Е.А.Дубинин, Ф.Б.Тебуева, В.В.Копытов. –М.:ИЦРИОР:НИЦИНФРА-М,2014.–192с.

16.Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки /О.А.Замула, В.І.Черниш// Системи обробки інформації:збірнихнауковихпраць.–Х.:ХУПС,2014.–Вип.2(92).–С.53-56.

17.ЗамулаА.А., СевериновА.В., КорниенкоМ.А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации. – Наука І техніка Повітряних Сил Збройних Сил Україні, 2017,– No2(15).–С.47-52

18.Родіонов А.М. Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем // Інформаційні технології та комп’ютерна інженерія. — 2008. — № 1 (11). — С. 170–175.

19.Глушак В.В., Новіков О.М. Метод проектування систем захисту інформації з використанням детермінованої гри «захисник-зловмисник» // Наукові вісті НТУУ «КПІ». — 2011. — № 2. — С. 46–53.

20.Архипов А.Е. Технологии експертного оценивания в задачах защиты информации // Інформаційні технології та комп’ютерна інженерія: міжнар. наук.- техн. журн. — 2005. — № 1. — С. 89–94.

21.Понтрягин Л.С. Линейная дифференциальная игра убегания // Труды Матема- тического института АН СССР, Т. 112. — 1971. — М.: Наука. — С. 30–63.

22.Ishai Menache, Eitan Altmany Battery-State Dependent Power Control as a Dynamic Game // Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops. — 2008. — WiOPT 2008. 6th International Symposium on. — Berlin. — P. 242–250.

23.Порядок проведення розслідування та ведення обліку нещасних випадків, професіональних захворювань і аварій на виробництві затверджений постановою КМУ від 30.11.2011 р. № 1232

24.ДСТУ 2293-93. Система стандартів безпеки праці. Терміни та визначення / уклад. М. В. Панфонюк. – Київ: Вікторія, 2008. – ISBN 448 с. – 966-598-148-X.

25.OHSAS 18001:2007 - Occupational Health and Safety Management System http://www.producao.ufrgs.br/arquivos/disciplinas/103_ohsas_18001_2007_ing.pdf

26. Білявський Г.О. Основи загальної екології: підр. для студ. природ. факультетів вищ. навч. закл. / Білявський Г.О. , Падун М.Н., Фурдуй Р.С. 2-е вид., зі змінами. К.: Либідь, 1995.- 368с. ISBN 5-325-00640-1.

27. Білявський Г. О. Основи екології: підручник для студ. вищих навч. закладів / Г. О. Білявський, Р. С. Фурдуй, І. Ю. Костіков. К. : Либідь, 2004. - 408 с. ISBN 966-06-0289-8.

28.Запольський А.К. Основи екології: підр. для студ. техн. технол. спец. вищ. навч. закл. / А. К. Запольський, А.І. Салюк; за ред. К.М. Ситника. К.: Вища школа, 2001.- 358с. ISBN 966-642-059-7.