Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Ковальчука Данила Володимировича*

академічної групи *125м-22-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Синтез системи підтримки прийняття рішень для оцінки інформаційних загроз в ІКС гіпермаркету*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.ф.-м.н., проф. Гусєв О.Ю.			
розділів:				
спеціальний	ст.викл. Начовний І.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Ковальчуку Данилу Володимировичу* **академічної групи** *125м-22-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Синтез системи підтримки прийняття рішень для оцінки інформаційних загроз в ІКС гіпермаркету*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Постановка задачі	02.11.2023
Розділ 2	Спеціальний розділ	16.11.2023
Розділ 3	Економічний розділ	30.11.2023

Завдання видано _____ Гусєв О.Ю.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Ковальчук Д.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 104 с., 27 рис., 7 табл., 5 додатків, 30 джерел.

Об'єкт дослідження: інформатизація процесу прийняття рішення з метою підвищення його ефективності.

Мета кваліфікаційної роботи: підвищення ефективності роботи систем підтримки прийняття рішень шляхом впровадження сучасних інформаційних технологій на комерційних підприємствах.

У розділі «Стан питання. Постановка задачі» проведено аналіз специфіки комерційних підприємств, виконано аналіз нормативно-правової бази у сфері захисту інформації, виконана характеристика підприємства, категоріювання об'єктів, розроблена модель порушника та виконано постановку задачі.

У спеціальній частині визначено необхідність розробки системи підтримки прийняття рішень, надані методи і технології систем підтримки прийняття рішень, розглянуто практичне застосування різних технологій при вирішенні задачі вибору, виконано синтез методів підтримки прийняття рішень для вибору найбільш актуальної загрози інформації з моделі загроз для АСЗ на прикладі мережі будівельних гіпермаркетів.

В економічному розділі виконано розрахунок економічного ефекту від впровадження системи в регіональний офіс комерційного підприємства.

Наукова новизна очікуваних результатів полягає у використанні інформаційних технологій, методів прийняття рішень і можливого застосування системи підтримки прийняття рішень на практиці у комерційних підприємствах.

ЗАХИСТ ІНФОРМАЦІЇ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, МОДЕЛЬ ЗАГРОЗ.

THE ABSTRACT

The explanatory note: 104 pages, 27 pictures, 7 tables, 5 appendices, 30 sources.

The object of study: informatization of the decision-making process with the aim of improving its effectiveness.

The purpose of the qualification work: to increase the effectiveness of the systems of support of decision-making through the introduction of modern information technologies for business.

The first part of the study analyzes the specificity of commercial enterprises, the analysis, gives analysis of normative-legal base in the sphere of information protection, gives enterprise characteristics and categorization of objects, develops the model of the intruder, and explains the problem statement.

The special part determines the need to develop systems of support of decision-making, presents the methods and technologies of systems of support of decision-making, considers the practical application of various technologies in solving the problem of selection, evaluates the synthesis methods of decision support for selecting the most relevant threat information from a threat model for AC3 on the example of network of construction hypermarkets.

The economic part calculates the economic benefits from implementation of the developed system at the central office of business.

Scientific novelty of the expected results consists in usage of information technologies, methods of decision-making and possible use of the system support decision making in practice at the commercial enterprises.

PROTECTION OF INFORMATION, INFORMATION SECURITY MANAGEMENT SYSTEM, DECISION SUPPORT MANAGEMENT SYSTEM, THREAT MODEL.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІБ – інформаційна безпека;

ІТ – інформаційні технології;

ІКС – інформаційно-комунікаційна система;

ІКТ – інформаційні та комунікаційні технології;

ІСУ – інформаційні системи управління;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НПБ – нормативно-правова база;

НСД – несанкціонований доступ;

ОС – операційна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

РСО – режимно-секретний орган;

САО – системи автоматизації офісу;

СЗП – система збалансованих показників;

СУІБ – система управління інформаційною безпекою;

СППР – система підтримки прийняття рішень;

УІС – управлінські інформаційні системи;

DSS – decision support system

ISM – information security management;

KPI – key performance indicators;

ROSI – return on security investment.

ЗМІСТ

ВСТУП

Проблема вибору при прийнятті рішень присутня абсолютно у всіх сферах діяльності сучасної людини. Люди повинні приймати рішення в будь-якому місці і в будь-який час. Під час війни, в політиці, в управлінні бізнесом, при виборі автомобіля або квартири і в тисячах інших випадків. Прийняте рішення, очевидно, має бути найкращим з представлених альтернатив, однак розглянути всі аспекти і деталі, які можуть впливати на вибір в ухваленні рішення, неможливо без сторонньої допомоги. Звичайно, є винятки, але витрати і зусилля для обробки такої кількості інформації будуть величезними. Між тим, неоптимальність прийнятих рішень веде до значних втрат можливостей і ресурсів. І втрати тим більше, чим складніше ситуація.

Прагнення до підвищення оптимальності прийнятих рішень призвело до створення науки, яка носить назву «Теорія прийняття рішень». Основним завданням при прийнятті рішення є вибір з варіантів, кращих для досягнення певної мети, або ранжування різних варіантів з точки зору їх впливу на досягнення цієї мети, незалежно від тієї області, в якій приймається рішення. Інакше кажучи, закони прийняття рішень єдині для всіх предметних областей.

Постійний розвиток інформаційних технологій призвів до створення машинних систем, спеціально призначених для прийняття рішень. Людина і комп'ютер чудово доповнюють один одного. Машинний комплекс чудово справляється з сортуванням всіляких альтернатив, а людина добре розбирається в цілях і оцінках підсумкових рішень. Все це підготувало ґрунт для створення систем підтримки прийняття рішень.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз організації і управління інформаційною безпекою у мережах будівельних гіпермаркетів

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності складають підходи. Підхід передбачає певну послідовність дій на підставі конкретного плану. Вони можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють наступні рівні:

1) фізичний;
2) програмно-технічний;
3) управлінський;
4) технологічний;
5) рівень користувача;
6) мережевий;
7) процедурний.

Більш детальніше розглянемо управлінський рівень. На цьому рівні здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління. До таких стадій належать: прийняття рішення по визначенню області та контексту інформаційної загрози і

складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній, соціальній та інших сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у нижчих організаційних ланках системи управління; виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Для забезпечення ефективної роботи в ринкових умовах та кваліфікованого керування підприємствами винятково важливо є їх чітка і повна класифікація за певними ознаками.

Виділимо кілька основних критеріїв, за якими слід відносити організацію до того чи іншого типу (рисунок 1.1).

Нижче розглянемо детальніше особливості кожного типу підприємств.

За метою і характером:

– комерційні - мета - одержання прибутку; створюються у формі господарських товариств і суспільств, виробничих кооперативів, державних і муніципальних унітарних підприємств;
– некомерційні - не мають за мету одержання прибутку і не розподіляють отриманий прибуток між учасниками (суспільні чи релігійні об'єднання, благодійні фонди, споживчі кооперативи, некомерційні партнерства й інші організації).

За правом власності:

– приватні - належать окремим громадянам на правах приватної власності і з правом наймання робочої сили; підприємства, що

базуються на приватній власності, але тільки на особистій праці (праці членів родини);

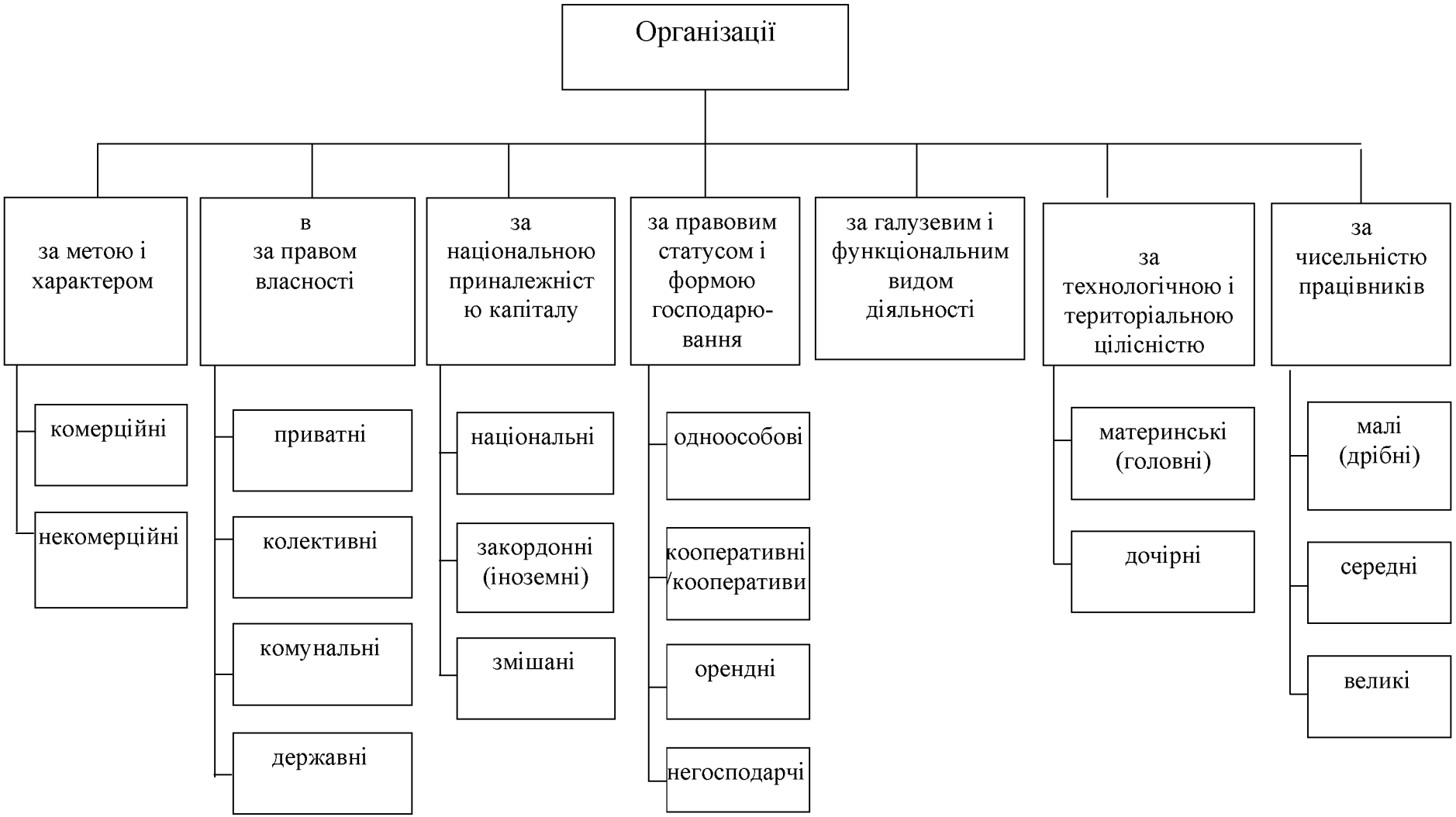

Рисунок 1.1 – Класифікація організацій

– колективні - базуються на власності трудового колективу, а також на власності кооперативу, або іншої статутної чи суспільно громадської організації;
– комунальні - засновані на базі власності відповідної територіальної громади;
– державні - засновані на державній власності (також казенні підприємства, що не підлягають приватизації).

За національною приналежністю капіталу:

– національні - капітал належить підприємцям своєї країни;
– закордонні (іноземні) - капітал є власністю іноземних підприємців (фірм) чи частково у тій частині, що забезпечує їм необхідний контроль. Створюються у формі філій дочірніх фірм і реєструються в країні за місцезнаходженням;
– змішані - капітал належить підприємцям (фірмам) двох чи декількох країн; їхня реєстрація здійснюється в країні одного з засновників такого підприємства.

За правовими статусом і формою господарювання:

1) одноособове підприємство - є власністю однієї людини чи членів родини; несе відповідальність за свої обов'язки всім майном (капіталом). Може бути зареєстроване як самостійне чи як філія іншого підприємства (іншої фірми). Форму одноособових підприємств мають переважно невеликі фірми за чисельністю працівників;
2) кооперативні підприємства (кооперативи) - добровільні об'єднання громадян з метою спільного ведення господарської чи іншої діяльності. Їх характерною ознакою є особиста участь кожного в спільній діяльності, використанні власного чи орендованого майна;
3) орендні підприємства - оренда складається в тимчасовому (на договірній основі) володінні і користуванні майном, необхідним орендарю для здійснення підприємницької діяльності;

4) господарчі товариства є об'єднаннями підприємців:

- повні - товариство, всі учасники якого займаються спільною підприємницькою діяльністю і несуть солідарну відповідальність по

  зобов'язаннях підприємства усім своїм майном;
- з обмеженою відповідальністю – товариства, котрі мають статутний фонд, розділений на частини; розмір їхній визначається статутними документами. Учасники цього суспільства несуть відповідальність у межах їхнього внеску;
- командитні - товариства, що, поряд із членами з повною відповідальністю, включає одного і більше учасників, відповідальність яких обмежується особистим внеском у майно такого суспільства;
- акціонерні - головним атрибутом товариства служить акція (цінний папір без установленого терміну звертання, що свідчить про майнову участь акціонера в статутному фонді суспільства; підтверджує членство в ньому і право на одержання частини прибутку у виді дивіденду і на участь у розподілі майна при ліквідації товариства). Акціонерні товариства бувають двох видів: відкритого типу, акції яких поширюються шляхом відкритої підписки і купівлі-продажу на фондових біржах, та закритого типу, акції яких можуть поширюватися тільки між його засновниками.

За галузевим і функціональним видом діяльності - при визначенні галузевої приналежності підприємство відносять до тієї чи іншої галузі, виходячи з того виду діяльності, що на момент реєстрації є переважним.

За технологічною і територіальною цілісністю:

– материнські (головні) - контролюють інші фірми, дочірні компанії; володіють контрольним пакетом їх акцій;

– дочірні - юридично самостійні організаційні утворення, що здійснюють комерційні операції і складають звітний баланс.

За чисельністю працівників:

– малі (дрібні) - у промисловості і будівництві - до 200 чол.; в інших галузях виробничої сфери - до 50 чол.; науці і науковому обслуговуванню - до 100

чол.; галузях невиробничої сфери - до 25 чол.; роздрібній торгівлі - до 15 чол. Мікропідприємствами є суб'єкти малого підприємництва із чисельністю працівників до 10 чол. і розміром виручки від продажу продукції (надання послуг) до 250 тис. грн. на рік;

– середні - в промисловості і будівництві - до 300 чол.; в інших галузях виробничої сфери - до 100 чол.; науці і науковому обслуговуванню - до 200 чол.; галузях невиробничої сфери - до 50 чол.; роздрібній торгівлі - до 30 чол.;

– великі - в промисловості і будівництві - від 300 чол.; в інших галузях виробничої сфери - від 100 чол.; науці і науковому обслуговуванню - від 200 чол.; галузях невиробничої сфери - від 50 чол.; роздрібній торгівлі - від 30 чол.

За основу вибору методики оцінки ефективності візьмемо комерційне підприємство.

Відповідно до Господарського кодексу України (далі ГК) комерційна діяльність — це самостійна, ініціативна, систематична, на власний ризик господарська діяльність, що здійснюється суб'єктами господарювання (підприємцями) з метою отримання прибутку. Суб'єктами підприємницької діяльності (підприємцями) можуть бути громадяни України, інших держав, не обмежені законом у правоздатності або дієздатності.

Умови заняття торгівельною діяльністю, основні вимоги до торговельно-виробничої мережі і торговельного обслуговування населення встановлені постановою Кабінету Міністрів України «Про затвердження

Порядку провадження торговельної діяльності та правила торговельного обслуговування населення».

Торгівля в даному випадку розглядається як вид господарської діяльності, яка забезпечує перехід товарної маси із сфери виробництва до споживача. Торговельна діяльність розглядається в двох аспектах. В першому випадку – це галузь народного господарства, до якої належать усі суб'єкти господарювання, торгові посередники, незалежно від того, мають вони чи ні право власності на товари.

У другому випадку під словом «торгівля» розуміють процес або дію, маючи на увазі продаж, зміну власника товару. Комерцією (торгівлею) займаються майже всі підприємства: виробничі, оптові і роздрібні.

Ст. 263 ГК України визначає господарсько-торговельну діяльність як таку діяльність, що здійснюється суб'єктами господарювання у сфері товарного обігу, спрямована на реалізацію продукції виробничо-технічного призначення і виробів народного споживання, а також допоміжну діяльність, яка забезпечує їх реалізацію шляхом надання відповідних послуг.

Комерційна діяльність в Україні регулюється Законами України "Про захист прав споживачів", "Про споживчу кооперацію", "Про зовнішньоекономічну діяльність", "Про забезпечення санітарного та епідемічного благополуччя населення", "Про лікарські засоби", "Про якість і безпеку харчових продуктів та продовольчої сировини", іншими актами законодавства.

Детально загальні правила здійснення торговельної діяльності регулює підзаконний нормативно-правовий акт «Порядок заняття торговою діяльністю і правила торгівельного обслуговування населення», затверджений постановою Кабінету Міністрів України від 15.06.2006 р. № 833. Цей «Порядок і правила» визначають загальні умови здійснення торговельної діяльності, основні вимоги до торговельної (торговельно-виробничої) мережі і торговельного обслуговування громадян.

Законодавство України про інформацію складають Конституція України, законодавчі акти про окремі галузі, види, форми і засоби інформації, міжнародні
договори та угоди, ратифіковані Україною, принципи і норми міжнародного права.

Основним законодавчим актом в області інформаційної безпеки в Україні є закон України «Про інформацію», який встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

Закон «Про захист персональних даних» займає своє місце в системі національного законодавства, це визначається тим, що він є базовим законом в сфері захисту персональних даних фізичних осіб в Україні. Зазначене обумовлено рядом особливостей захисту персональних даних. По-перше, їх несанкціонований збір, обробка та розповсюдження можуть бути використані на шкоду людині, а також суспільству і державі. По-друге, участь України в міжнародному обміні інформацією, в міжнародних проєктах, які засновані на використанні нових інформаційно-комунікаційних технологій, зокрема, Інтернет, в різних секторах економічної, соціальної і науково-технічної діяльності, вимагає захисту персональних даних при їх автоматизованій обробці, в умовах гармонізації правових норм, що діють в Україні, з європейськими стандартами.

Інформаційна безпека в державному, банківському та комерційному секторах України має забезпечуватися згідно з положеннями ДСТУ ISO/IEC 27001:2010 «Інформаційні технології. Методи і засоби досягнення інформаційної безпеки. Системи управління інформаційною безпекою.

Вимоги (ISO/IEC 27001:2010, IDT)» (далі ДСТУ 27001), який надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків. СУІБ забезпечує вибір адекватних і пропорційних засобів контролю та захисту інформації і, тим самим, довіру зацікавлених сторін.

Проблема вдосконалення державної інформаційної політики є однією із пріоритетних. Якщо розглядати в Україні діяльність щодо захисту інформаційно

комунікаційних систем, то наявна нормативна база у сфері захисту інформації відповідає світовим підходам до їх проєктування, виробництва, оцінювання та експлуатації. Концепція Національної безпеки України визначає загрози національній безпеці та основні напрями державної політики національної безпеки України щодо інформаційної сфери. Прийняті також документи, які складають нормативну базу в цій сфері: Національна програма інформатизації, Указ Президента "Про міри по забезпеченню інформаційної безпеки держави", Закон України "Про державну таємницю", Положення "Про технічний захист інформації" та інші.

Однак наявність відповідної нормативної бази – це тільки перший крок в напрямку забезпечення належного рівня безпеки в цій сфері. Найбільш важливим є реалізація та впровадження необхідних заходів щодо здійснення політики інформаційної безпеки і особливо захисту інформації.

Інформаційна безпека відіграє важливу роль у формуванні процесу впровадження нових інформаційних технологій в усі сфери життя суспільства та людства в цілому. Широкомасштабне використання обчислювальної техніки та комунікаційних систем, збільшення обсягів інформації, що обробляється та поширення кола користувачів приводить до якісно нових можливостей несанкціонованого здобуття інформації.

Виділимо основні проблеми сфери захисту інформації:

- незавершеність організаційно-правової і нормативно-юридичної бази, а також не довершене створення нормативних і методичних документів із захисту інформації від витоку по технічним каналам і т.п.;
- різке підвищення злочинності підприємств шляхом розвідки через розміщення на територіях, які охороняються, різних комерційних структур, підприємств і т.п.;
- значна зношеність матеріально-технічної бази проведення робіт, особливо контрольно-вимірювальної апаратури, засобів обчислювальної техніки, зв'язку, оргтехніки;
- відсутність достатнього фінансування на створення систем захисту і сучасних засобів захисту інформації, значне зниження рівня захищеності за рахунок скорочення фінансування робіт на підтримку засобів захисту.

Останнім часом в умовах тотального впровадження інформаційних технологій вирішити проблеми інформаційної безпеки важко через такі причини:

- інформація відносно просто копіюється дублюванням раніше створених
- інформаційних продуктів;
- у зв’язку з швидким розвитком обчислювальної техніки значно ускладнено можливості контролю і запобігання несанкціонованому отриманню й використанню інформації з обмеженим доступом.
- різноманітність апаратних і програмних засобів формування, передачі, перетворення, відображення і зберігання інформації при впровадженні інформаційних технологій збільшує потенційні можливості формування нових каналів її витоку і порушення цілісності;
- ефективна охорона інформації може бути досягнута тільки шляхом створення системи безпеки інформації, що реалізує державну політику, здійсненням управлінської, адміністративно-господарської і

виробничої діяльності, підготовки кадрів відповідної кваліфікації та інших видів діяльності.

Саме через відсутність та недостатню впровадженість або втрату актуальності системи захисту інформації на підприємстві виникають різного рівня витоки інформації. Тому на основі нормативних документів та стандартів інформаційної безпеки є необхідною розробка системи показників, за допомогою яких можна контролювати стан СУІБ.

Система управління інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності критичної інформації, забезпечення неможливості несанкціонованого доступу до критичної інформації, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей.

Найбільш значущою метою системи управління інформаційної безпеки комерційних організацій є захист бізнес-інтересів компанії з максимальним показником повернення інвестицій в інформаційну безпеку (ROSI). Також однією

з основних цілей такої системи інформаційної безпеки є гарантія майнових прав та інтересів клієнтів та партнерів. У той же час заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією в компанії, оскільки це може поставити під загрозу розвиток організації.

1.2 Характеристика підприємства

В якості об'єкта інформаційної діяльності обраний регіональний офіс будівельно-господарських гіпермаркетів «Епіцентр К». Це – товариство з обмеженою відповідальністю, що має у своєму підрозділі мережу будівельно-господарських гіпермаркетів. Акт обстеження підприємства знаходиться в Додатку Б.

Згідно Додатку Б «Акт обстеження ТОВ «Епіцентр К», на даному підприємстві циркулює загальнодоступна та конфіденційна інформація.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Виходячи з цього та згідно з НД ТЗІ 1.6-005-2013 (п. 5.7), ОІД відноситься до четвертої категорії.

1.3 Рекомендації зі створення служби захисту інформації

Для забезпечення впровадження, функціонування СУІБ та контролю за функціонуванням СУІБ наказом має бути призначений керівник СУІБ або його заступник, який відповідає за питання інформаційної безпеки та в оперативному підпорядкуванні якого знаходиться підрозділ інформаційної безпеки. Керівник СУІБ повинен мати повноваження долучати до впровадження та функціонування СУІБ усіх потрібних фахівців і, в першу чергу, керівників підрозділів – власників бізнес-процесів.

Беручи до уваги інформаційні потоки ТОВ «Епіцентр К», інформація яка наведена в Додатку Б, та згідно з НД ТЗІ 3.7-003-2005 (п. 5.10) для організації робіт зі створення КСЗІ в ІКС необхідно створити службу захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД ТЗІ 1.4-001-2000.

Метою створення СЗІ є організаційне забезпечення завдань керування комплексною системою захисту інформації в АС та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в АС, проєктування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в АС.

Наказ на створення СЗІ знаходиться в Додатку Б.

1.4 Категоріювання об’єктів

Об’єкти, на яких здійснюється обробка технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов’язковому категоріюванню.

Категоріювання об’єктів проводиться комісією з категоріювання установи-власника (розпорядника, користувача) об’єкта.

Комісія з категоріювання визначає ступень обмеження доступу до інформації, яка обробляється технічними засобами та/або озвучується на об’єкті, та з урахуванням цього ступеня встановлює категорію об’єкта. Встановлена категорія зазначається в Акті категоріювання об’єкта, який складається комісією з категоріювання за результатами її роботи та впроваджує його.

За результатами роботи комісії складаються акти довільною форми, в яких наводяться зазначені відомості, раніше встановлена категорія та прийняте рішення про категоріювання. Акти затверджуються керівником організації (Додаток Б).

1.5 Розробка моделі порушника

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз яка розглянута у другої частині для інформації та моделі порушника (згідно п.4.1).

Модель порушника – це абстрактний формалізований або неформалізований опис порушника, рівня його повноважень, ресурсних можливостей, використовуваних ним програмних і (або) технічних засобів з метою реалізації загроз для інформації.

Об'єктом захисту на підприємстві ТОВ „Епіцентр К” є конфіденційна, а також відкрита інформація, яка зберігається на сервері підприємства та циркулює у мережі.

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Порушники класифікуються за рівнем

можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього та також доповнює:

- перший рівень визначає найнижчий рівень можливостей проведення діалогу з КС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проєктування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник — це фахівець вищої кваліфікації, який має і використовує повну інформацію про комп'ютерну мережу і КЗЗ.

Джерела загроз поділяються на 3 основні групи:

1 Антропогенні - виступають об'єкти-користувачі, дії яких можуть бути кваліфіковані як умисні чи випадкові злочини. Тільки в цьому випадку можна говорити про заподіяння шкоди. Ця група найбільш обширна і становить найбільший інтерес з точки зору організації захисту, так як дії об'єкта-користувачів завжди можна оцінити, спрогнозувати і вжити адекватних заходів.

2 Техногенні - спрямовані від технічних засобів обробки інформації, що оточують людину та можуть впливати на компоненти ІКС чи інформаційні ресурси.

3 Стихійні - Стихійні джерела загроз інформації характеризуються не тільки тим, що їх ні як неможливо передбачити до появи, або можливо передбачити, але неможливо уникнути. Такі джерела загроз не піддаються прогнозуванню та заходи, щодо захисту від них повинні застосовуватися завжди.

Класифікація джерел загроз наведена у таблиці 1.1.

Таблиця 1.1 – Класифікація джерел загроз

Позначення	Визначення категорії	Рівень загрози
Антропогенні джерела загроз		
Внутрішні по відношенню до АС		
ПВ1	Технічний персонал, обслуговуючий приміщення, у яких знаходиться АС	1
ПВ2	Персонал, що безпосередньо працює з АС, але не має доступу до інформації	2
ПВ3	Персонал, що безпосередньо працює в АС та має доступ до інформації	3
Зовнішні по відношенню к АС		
ПЗв1	Будь-які особи, що знаходяться за межами КЗ	1
ПЗв2	Відвідувачі	2
ПЗв3	Конкуренти	4
ПЗв4	Кримінальні структури	3
ПЗв5	Зловмисники (хакери)	2
Специфікація за мотивами здійснення порушення		
Позначення	Мотив порушника	Рівень загрози

Позначення	Визначення категорії	Рівень загрози
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок	4
Специфікація порушника за рівнем кваліфікації та обізнаності щодо АС		
Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Знає особливості систем контролю доступу на об’єкт	3
К2	Знає структуру, функції та механізми систем захисту інформації	4
Специфікація порушника за часом дії		
Позначення	Характеристика можливостей порушника	Рівень загрози
В1	В неробочій час, під час планових перерв працівників та інші	2
В2	Під час функціонування підприємства	3
В3	Як під час перерв, так і під час функціонування	4
Специфікація порушника за місцем дії		
Позначення	Характеристика можливостей порушника	Рівень загрози
Д1	Без доступу до контрольованої зони	1
Д2	З доступом до контрольованої зони, але без доступу до приміщень	2
Д3	Усередині приміщень, але без доступу до автоматизованої системи	3

Продовження таблиці 1.1

Позначення	Визначення категорії	Рівень загрози
Д4	Від робочих станцій та персональних комп'ютерів співробітників компанії	4
Техногенні джерела загроз		
Позначення	Характеристика	Рівень загрози
Т1	Засоби зв’язку	1
Т2	Мережі інженерних комунікацій	2
Т3	Неякісні технічні засоби обробки інформації	3
Т4	Неякісні програмні засоби обробки інформації	3
Т5	Допоміжні засоби (відео спостереження, охоронна сигналізація, пожежна сигналізація)	2
Стихійні джерела загроз		
Позначення	Характеристика	Рівень загрози
С1	Пожежа	3
С2	Урагани, Паводок	2
С3	Непередбачувані обставини	1
С4	Інші форс-мажорні обставини	1

Використовувані позначення:

1 – рівень загрози малий, практично неможливий (ймовірність у 0-30% випадків);

2 – рівень загрози невеликий, але в окремих випадках можливий (ймовірність у 30-50% випадків);

3 – загроза можлива в 50% випадків;

4 – дуже велика ймовірність виникнення загрози порушення (ймовірність у 50-80% випадків);

5 – загроза неминуча так як ймовірність прямую до 100 (ймовірність у 80-90% випадків).

На основі наведеної у таблиці 1.1 класифікації антропогенних джерел загроз, необхідно створити модель порушника за мотивом, кваліфікацією, часом та місцем дії. З урахуванням функціональних особливостей ТОВ "Епіцентр К", а також його цільової аудиторії, представлена модель порушника підприємства (табл. 1.2).

Таблиця 1.2 - Модель порушника підприємства

Порушник	ПВ1	ПВ2	ПВ3	ПЗв1	ПЗв2	ПЗв3	ПЗв4	ПЗв5
Мотив	М1,2	М2,3	М2, 3	М3	М3	М3	М3,4	М3, 4
Кваліфікація	К1	К2	К2	К1	К1	К1	К1	К2
Час дії	В1	В2	В2	В3	В2	В3	В3	В3
Місце дії	Д2,3	Д4	Д4	Д1,2	Д3,4	Д3,4	Д1	Д1

1.6 Профіль захищеності для інформаційної системи

Згідно НД ТЗІ 2.5-005-99 дана автоматизована система відноситься до класу «3», тому що це розподілений багатомашинний багатокористувачевий комплекс, що обробляє інформацію різних категорій конфіденційності і має доступ через незахищене середовище.

Для даної АС був обраний стандартний функціональний профіль захищеності, з підвищеними вимогами до забезпечення цілісності, доступності і конфіденційності оброблюваної інформації.

3.КЦД.1 - {КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

КД-2 (базова довірча конфіденційність);

КО-1 (повторне використання об'єктів);

КВ-1 (мінімальна конфіденційність);

ЦД-1 (мінімальна довірча цілісність);

ЦО-1 (відкат);

ЦВ-1 (мінімальна цілісність при обміні);

ДР-1 (недопущення використання ресурсів);

ДВ-1 (відновлення після збоїв);

НР-2 (реєстрація);

НІ-2 (одиночна ідентифікація й автентифікація);

НК-1 (односпрямований достовірний канал);

НО-1 (Розподіл обов'язків адміністраторів);

НЦ-2 (КЗЗ із функціями диспетчера доступу);

НТ-2 (самотестування при старті);

НВ-1 (автентифікація джерел даних).

1.7 Постановка задачі

Виходячи з результатів аналізу організації та управління інформаційною безпекою на комерційних підприємствах, а також необхідністю в ефективному управлінні інформаційною безпекою, що можливе при наявності правильно організованої і функціонуючої системи управління інформаційною безпекою та контролю її процесів, необхідно вирішити наступні задачі:

1) моделювання загроз інформації для автоматизованої системи класу 3 на прикладі регіональної мережі будівельних гіпермаркетів;

2) подання методів і технологій систем підтримки прийняття рішень;

3) розгляд практичного застосування різних технологій при вирішенні задачі вибору;

4) здійснення синтезу технології з представлених альтернатив СППР для вибору найбільш актуальної загрози інформаційної безпеки з моделі загроз для автоматизованої системи класу 3.

1.8 Висновок

Масштаби застосування інформаційних технологій набули таких масштабів, що поряд із проблемами продуктивності, надійності і стійкості функціонування комп'ютерних систем, гостро постає проблема захисту циркулюючої в системах інформації від несанкціонованого доступу. Інформація в багатьох організаціях стає ключовим ресурсом, а інформаційна безпека - справою стратегічної важливості.

Система управління інформаційною безпекою є сучасним процесом забезпечення безпеки інформаційних ресурсів організації, яка побудована на кращих світових практиках. Її впровадження необхідно аби забезпечити об'єднання всіх захисних засобів, що застосовуються на підприємстві, у єдиний адекватний реальним загрозам і керований комплекс, що дозволяє досягати корпоративних цілей інформаційної безпеки на рівні всього підприємства.

Розроблена система управління інформаційною діяльністю потребує постійного контролю та вдосконалення.

Досягнення заданих цілей можливо у ході вирішення таких основних завдань, як визначення відповідальних за інформаційну безпеку, розробка спектра ризиків інформаційної безпеки та проведення їх експертних оцінок, розробка політик і правил доступу до інформаційних ресурсів, розробка системи управління ризиками інформаційної безпеки, у тому числі методи їх оцінки, контролю інформаційної безпеки на підприємстві та системи показників, регулюючих стан системи.

2 СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Методи оцінки загроз безпеці інформації

2.1.1 Аналіз існуючих методів

Аналіз загроз інформаційній безпеці дозволяє виділити складові сучасних загроз – їх джерела та рушійні сили, способи і наслідки реалізації. Аналіз виключно важливий для отримання всієї необхідної інформації про інформаційні загрози, визначення потенційної величини збитку, як матеріальної, так і нематеріальної, і вироблення адекватних заходів протидії.

При аналізі загроз інформаційної безпеки використовуються три основні методи (рисунок 2.1):

Рисунок 2.1 – Основні аналітичні методи оцінки загроз

Розглянемо наведені методи детальніше.

Пряма експертна оцінка. Метод експертних оцінок заснований на тому, що параметри загроз задаються експертами. Експерти визначають переліки параметрів, що характеризують загрози інформаційної безпеки, і дають суб'єктивні коефіцієнти важливості кожного параметра.

Статистичний аналіз – це аналіз інформаційних загроз на основі накопичених даних про інциденти інформаційної безпеки, зокрема, про частоту виникнення загроз певного типу, їх джерела та причини успіху або неуспіху реалізації. Наприклад, знання частоти появи загрози безпеки інформації дозволяє визначити ймовірність її виникнення за певний проміжок часу.

Для ефективного застосування статистичного методу потрібна наявність досить великий за обсягом бази даних про інциденти. Потрібно відзначити ще одну вимогу: при використанні об'ємних баз необхідні інструменти узагальнення даних і виявлення в базі вже відомої та нової інформації.

Факторний аналіз заснований на виявленні факторів, які з певною ймовірністю ведуть до реалізації загроз і тим або іншим негативних наслідків. Такими факторами можуть бути наявність привабливих для злочинців інформаційних активів, уразливості інформаційної системи, високий рівень вірусної активності в зовнішньому середовищі і т.д. Оскільки на сучасні інформаційні системи впливають безліч факторів, зазвичай використовується багатофакторний аналіз.

При аналізі загроз інформаційної безпеки найбільш ефективно застосовувати комплекс різних аналітичних методів. Це значно підвищує точність оцінки.

Найбільш вдалим рішенням з оцінки загроз є створення моделі загроз, яка може бути описана багатьма способами, найчастіше використовується табличне представлення моделі загроз, але також популярні способи математичного опису та використання наочних схем.

2.1.2 Вибір методу оцінки загроз

В даній роботі був обраний комплексний метод аналітичної оцінки загроз інформаційній безпеці підприємств. Модель загроз представлена у вигляді таблиці 1.3.

2.1.3 Розробка моделі загроз

Мета розробки моделі загроз – виявлення та первинний аналіз пріоритетних напрямків побудови системи захисту інформації, відокремлення незначущих та встановлення взаємозв’язків можливих каналів витоку інформації з обмеженим доступом.

Види інформації з обмеженим доступом, яка може бути в приміщенні РСО, виходячи з фізичної природи середовища виникнення та поширення небезпечних сигналів:

– електромагнітні сигнали, що виникають під час роботи технічних засобів, обробці інформації за допомогою ПЕОМ, веденні переговорів засобами зв'язку;

– акустичні сигнали, які виникають під час роботи технічних засобів, веденні переговорів засобами зв'язку;

– наявність паперових носіїв, на яких надруковано інформацію з обмеженим доступом або інших матеріальних носіїв таємної інформації;

– дії робітників об'єкту.

– модель загроз повинна включати (згідно п.4.5):

– генеральний та ситуаційний (Додаток Б) плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;

– схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІзОД;

– оцінку шкоди, яка передбачається від реалізації загроз.

Загрози можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Необхідно розробити модель загроз інформаційної безпеки для автоматизованої системи класу 3 на прикладі підприємства ТОВ «Епіцентр К». Модель загроз вказано у таблиці 2.1.

Таблиця 2.1 – Модель загроз підприємства

Загроза	Ймовірність реалізації	Збиток від реалізації	Рівень реалізації загрози	Вразливість	Методи протидії
Техногенні загрози					
1 Збій в системі електропостачання	0,5	0,5	0,2	цілісність, доступність	Використання пристроїв неперервного електропостачання
2 Знищення (руйнування) інформації	0,2	1	0,8	цілісність, доступність	Резервне копіювання
3 Старіння носіїв інформації	0,2	0,5	0,2	цілісність, доступність	Резервне копіювання, оновлення бази носіїв
4 Модифікація інформації при передачі по каналах зв'язку і комунікації	0,2	0,75	1	цілісність	Використання контрольних сум
Загрози при стихійних лихах					
1 Знищення (руйнування)					
Приміщень	0,2	1	1	цілісність, доступність	Страхування, системи протипожежної безпеки
Технічних засобів обробки інформації	0,3	1	0,8	цілісність, доступність	Страхування, системи протипожежної безпеки
Носіїв	0,3	1	0,8	цілісність,	Страхування,

Загроза	Ймовірність реалізації	Збиток від реалізації	Рівень реалізації загрози	Вразливість	Методи протидії
інформації				доступність	системи протипожежної безпеки, вогнестійкі сейфи
2Зникнення інформації в засобах обробки,при передачі	0,5	0,75	1	цілісність, доступність	Резервне копіювання, використання підтверджень про отримання
Антропогенні загрози					
1 Знищення					
Електронної інформації	0,8	1	0,8	цілісність, доступність	Резервне копіювання
Носіїв інформації (паперові, магнітні, оптичні)	0,5	1	0,6	цілісність, доступність	Контроль доступу у приміщення, система відеоспостереження, облік носіїв,резервне копіювання
Програмного забезпечення	0,5	1	0,6	цілісність, доступність	Резервне копіювання, розмежування прав доступу для користувачів системи
Засобів обробки інформації	0,5	1	0,6	цілісність, доступність	Контроль доступу у приміщення, система відеоспостереження, облік засобів обробки інформації
2 Крадіжка					
Носіїв інформації (паперові, магнітні, оптичні)	0,8	1	0,8	Конфіденцій-ність, доступність	Контроль доступу у приміщення, система відеоспостереження, облік носіїв,резервне копіювання
Інформації (читання та несанкціоноване копіювання)	0,9	1	1	конфіденцій-ність, доступність	Контроль доступу у приміщення, система відеоспостереження,

Загроза	Ймовірність реалізації	Збиток від реалізації	Рівень реалізації загрози	Вразливість	Методи протидії
					облік носіїв, криптографічний захист
засобів доступу (ключі та паролі)	0,75	1	1	конфіденційність, цілісність, доступність	Використання антивірусного програмного забезпечення, криптографічних засобів захисту, контроль доступу у приміщення
3 Порушення встановленого режиму доступу	0,75	1	1	конфіденційність, цілісність, доступність	Охорона приміщень, система контролю доступу
4 Порушення нормальної роботи (переривання) пропускної здатності каналів зв'язку	0,6	1	0,8	доступність	Використання міжмережевих екранів, аналіз трафіку
5 Помилки при використанні програмного забезпечення	0,6	0,75	0,8	цілісність, доступність	Резервне копіювання даних, підвищення кваліфікації працівників
6 Шкідливе програмне забезпечення	0,75	1	0,6	конфіденційність, цілісність, доступність	Використання міжмережевих екранів, антивірусного програмного забезпечення, криптографічних засобів захисту
Технічні канали витоку інформації					
1 ПЕМВ засобів	0,25	1	0,8	конфіденцій-	Використання

Продовження таблиці 2.1

Загроза	Ймовірність реалізації	Збиток від реалізації	Рівень реалізації загрози	Вразливість	Методи протидії
обробки інформації				ність	генераторів ЕМ шуму, екранування приміщень
2 Наводки на лінії електроживлення	0,25	1	0,8	конфіденцій-ність	Використання генераторів шуму, фільтри
3 Несанкціонований знімання інформації	0,4	1	0,6	конфіденцій-ність	Система контролю доступу у приміщення, перевірки наявності закладних пристроїв
4 Акустичні канали	0,6	1	0,6	конфіденцій-ність	Використання генераторів шуму, звукоізоляція, екранування
5 Оптичні канали	0,6	1	0,6	конфіденцій-ність	Контроль доступу, захист прозорих поверхонь (вікна, двері) за допомогою жалюзі

Пояснення до таблиці 2.1.

Класифікація ступенів впливу на інформаційний ресурс:

І Критична - збитки від реалізації загроз призведуть до краху роботи суб'єкта або до дуже значних матеріальних втрат.

ІІ Середня - збитки від реалізації загроз призведе до деяких матеріальних або моральних втрат, якщо не будуть зроблені деякі дії.

ІІІ Незначна - збитки від реалізації загроз приносить скоріше моральний збиток, може бути використана тільки в певних ситуаціях.

Шкала оцінювання ймовірності реалізації загроз:
0 … 0.24 – дуже низька ймовірність (Незначна);
0.25 …0.49 – низька ймовірність ;

0.5 … 0.74 – середня ймовірність;
0.75 … 1 – висока ймовірність.
Шкала оцінювання рівня збитку від реалізації загроз:
0 … 0.24 – незначні, або відсутні;
0.25 …0.49 – низький рівень (Незначна);;
0.5 … 0.74 – середній рівень (Середня);
0.75 … 1 – високий рівень збитку, можливі критичні ситуації (Критична).

Перелік актуальних загроз з середнім та високим рівнем ризику:

1) несанкціоноване підключення до безпровідної мережі;

2) вплив на співробітників;

3) запуск файлів, що містять віруси, що впливають на ОС;

4) підбір автентифікаційних даних користувачів;

5) розголошення, передача атрибутів доступу;

6) неавторизована модифікація, читання чи видалення інформації у базі даних;

7) неавторизована модифікація, читання чи видалення електронних документів;

8) запуск експлойтів, що використовують вразливості мережевих служб;

9) запуск ОС з зовнішнього носія;

10) читання важливої інформації з паперових носіїв та екранів персональних комп'ютерів;

11) запуск експлойтів, що використовують вразливості ОС;

12) крадіжка ноутбуків;

13) перехоплення інформації, що надаються мережевими службами, використання вразливості протоколів передачі даних;

14) пошкодження носіїв інформації внаслідок пожару;

15) знищення чи псування носіїв інформації, крадіжка носіїв інформації.

2.2 Актуальність дослідження СППР

Питання вибору тієї чи іншої технології, з метою прийняття рішень є вкрай важливим. В основі кожної з систем підтримки прийняття рішень лежить той чи інший математичний метод рішення задачі. Таким чином, розгляд інформаційних технологій в СППР неможливо без освітлення застосовуваних у них методи. Існує ряд певних методів використовуваних при прийнятті рішення в СППР, які можуть бути віднесені до методів інформаційних технологій. Їх опис і застосування можна зустріти у різних джерелах по даній темі, однак чітка і структурована інформація про порівняння даної групи методів між собою і розгляд рішення практичних завдань в рамках одного дослідження відсутній - це обумовлює актуальність даної теми.

2.2.1 Інструментарій і методи дослідження

Дослідження будується на розгляді двох методів підтримки прийняття рішень за допомогою інформаційних технологій. Метод аналітичних мереж (МАС) і метод Експертної СППР (PURr). Розглядаються системи використовують цим методи, а також приклад розгортання ЕСППР в хмарній платформі.

Для вирішення задачі вибору альтернативи BI-платформи з точки зору методу аналітичних мереж використовується система «SuperDecisions», що знаходиться у вільному доступі, а з точки зору застосування методу PURr - «Експертна система підтримки прийняття рішень». Результатом дослідження є порівняння методів і оцінка отриманих результатів при вирішенні завдань.

2.2.2 Системи підтримки прийняття рішень

Говорячи про системи підтримки прийняття рішень, в першу чергу, має сенс визначитися з поняттям. Незважаючи на факт стрімкого розвитку і повсюдного впровадження СППР, на поточний момент немає чітко сформульованого поняття системи підтримки прийняття рішень як такої.

Формулювання визначення цілком і повністю залежить від думки автора. Однак сучасні системи підтримки прийняття рішень можуть бути охарактеризовані як системи, спрямовані на вирішення завдань повсякденної управлінської діяльності, які також є інструментом, створеним з метою надати допомогу особам, які приймають рішення. За допомогою систем підтримки прийняття рішень проводиться вибір альтернатив серед деяких неструктурованих і слабоструктурованих завдань, в тому числі і багатокритеріальних.

Згідно основного поняття Система Підтримки Прийняття Рішень (СППР) (англ. Decision Support System, DSS) - це комп'ютерна автоматизована система, метою якої є допомога особам, які приймають рішення в складних умовах для повного і об'єктивного аналізу предметної діяльності.

Перші введені поняття визначень систем підтримки прийняття рішень (на початку 70-х) зводилися до наступних трьох моментів:
1 Вміння працювати з неструктурованими і слабоструктурованими завданнями;
2 Інтерактивні автоматизовані (іншими словами, реалізація яких заснована на базі комп'ютера) системи.

Остання версія визначення не відображає кілька важливих моментів, наприклад, участь самого комп'ютера у створенні системи підтримки прийняття рішень. Як було сказано вище, зараз немає чітко сформульованого і загальноприйнятого визначення системи підтримки прийняття рішень. Основна проблема полягає в тому, що конструкція системи ключовим чином залежить від типу задачі, для рішення якої вона була створена, а також від наявних даних, інформації і навіть від користувачів цієї системи. Однак можна охарактеризувати СППР посилаючись на загальновизнані частини СППР. СППР - це «сукупність процедур по обробці даних і думок, що допомагають керівникові в прийнятті рішень, заснована на використанні моделей».

Велика кількість дослідників під системами підтримки прийняття рішень розуміють - «інтерактивні комп'ютерні системи, які допомагають особі, що приймає рішення, використовувати дані та моделі для розв'язання слабо структурованих або важко формалізованих завдань». Для більш точного визначення поняття систем підтримки прийняття рішень, має сенс розглянути місце СППР серед інформаційних систем у цілому. Розглядаючи СППР через призму процесів прийняття рішень, можна виділити три типи підтримки рішень:1. Інформаційна; 2. Модельна; 3. Експертна.

Всі три типи, що реалізуються в СППР, є інформаційними системами, покликаними допомогти у вирішенні неструктурованих завдань. На рисунку 2.2 наведена структура, функції технологічних блоків і основні операції системи підтримки прийняття рішень.

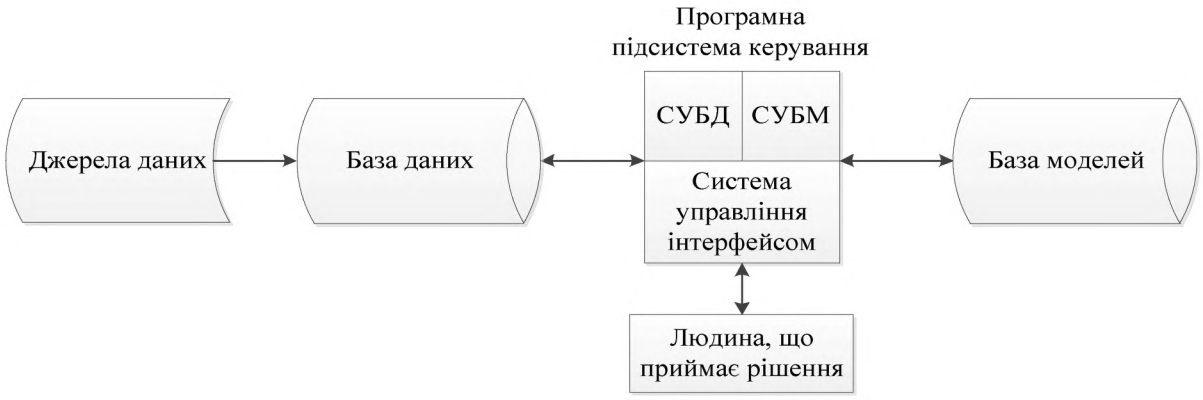

Рисунок 2.2 - Структура СППР

Основними компонентами інформаційної технології підтримки прийняття рішень є база даних, програмна підсистема і база моделей. Система управління базою даних (СКБД), система управління базою моделей (СУБМ) і система управління інтерфейсом входять до складу програмної підсистеми (рисунок 2.3).

Рисунок 2.3 - СППР щодо існуючих ІС

В результаті видно, що інформаційна підтримка прийнятих рішень заснована на двох «китах»:

1 Інформаційні системи управління (ІСУ) - набір різних інструментів для збору, зберігання і обробки інформації про діяльність підприємства, що є єдиним цілому - системою.

2 Системи автоматизації офісу (САО) - системи, що організують підтримку процесу комунікації як всередині підприємства, так із зовнішніми джерелами, заснованої на базі засобів передачі та роботи з інформацією (рисунок 2.4).

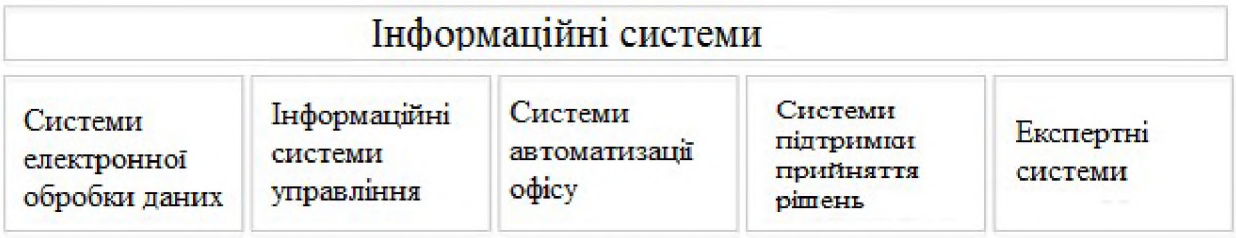

Рисунок 2.4 - Різновиди інформаційних систем

Беручи до уваги визначення і поняття, наведені вище, можна зробити висновок, що системи підтримки прийняття рішень конструктивно відрізняються від традиційних систем. СППР спрямовані на конкретного

користувача, на наявні у нього знання та інтуїцію, на його систему цінностей. Немаловажним фактором також є наявний у користувача досвід.

Важливо розуміти, що сам процес прийняття рішень носить суб'єктивний характер - цей факт є основою СППР. Іншими словами, це означає, що користувач цілком автономна, і діє він, спираючись тільки на власні знання і досвід. Очевидно, що на розсуд самого користувача можуть бути залучені сторонні консультанти та експерти. Таким чином, система лише допомагає користувачеві знайти ті рішення, які представляються йому найкращими на основі яких-небудь даних, але які, водночас, без допомоги системи дуже важко або неможливо було б знайти з причини високої складності розв'язуваної задачі.

Сучасні СППР - це результат багатьох досліджень, таких як:

- бази даних (Data Base) і бази знань (Data Knowledge);
- штучного інтелекту (Artificial Intelligence);
- інтерактивних комп'ютерних систем;
- методів імітаційного моделювання.

Як результат, СППР виникли завдяки злиття управлінських інформаційних систем (УІС) і систем управління базами даних (СУБД).

Нинішні системи підтримки прийняття рішень використовують у своєму арсеналі такі основні технології:

- сховища даних (Data Warehouse);
- інструменти оперативною (в реальному часі) аналітичної обробки інформації (On-Line Analytical Processing);
- інструменти вилучення даних (Data Mining), текстів (Text Mining) і візуальних образів (Image Mining).

Однією з найважливіших особливостей сучасних систем підтримки прийняття рішень є відсутність можливості оптимізації і ранжирування значень груп показників на основі їх повної сукупності, з-за неможливості існуючих математичних методів здійснювати дані операції. Сучасні методи

вимагають попереднього приведення всіх критеріїв до єдиної числової оцінки.

Способів приведення до єдиної числової оцінки існує досить багато, і той з них, що буде обраний у звичайно підсумку, може відчутно вплинути на результати ранжирування і оптимізації в негативному плані. Необхідно брати до уваги той факт, що користувач, який повністю відповідає високим вимогам професіоналізму у своїй галузі, абсолютно не обов'язково повинен вміти розбиратися в тому, які алгоритми використовується в СППР. Отже, всі рішення, прийняті розробником в ході процесу проєктування системи, потенційно можуть впливати на вибір альтернатив. Причому контролювати цей вплив користувач не в змозі.

Описаний вище принциповий недолік традиційних СППР, що спираються лише на формальні методи згортки, в сучасних системах зведений до мінімуму. Це досягається за рахунок зіставлення між собою можливих значень груп показників. Здійснюється цей процес користувачем в діалозі з системою, а значення зіставляються відповідно переваг користувача. В результаті отримуємо функцію переваг, сформовану в системі як результат таких зіставлень користувачем. У подальшому на її основі здійснюються операції ранжування та оптимізації. У підсумку, формальні методи згортки критеріїв замінено процедурою визначення переваг. При цьому результати процедури виявлення переваг відображають унікальний підхід користувача до задачі і не піддаються впливу з боку розробника.

Характеристики СППР.

Згідно E. Turban , СППР володіє наступними властивостями:

1 Системи підтримки прийняття рішень використовують і дані, і моделі;

2 Системи підтримки прийняття рішень спрямовані менеджерам в якості помічника в процесі прийняття рішень у питанні слабоструктурованих і неструктурованих завдань;

3 Системи підтримки прийняття рішень тільки підтримують, а не замінюють вироблення альтернатив менеджерами;

4 Мета системи підтримки прийняття рішень - підвищення ефективності рішень.

E. Turban висунув припущення про список характеристик ідеальної системи підтримки прийняття рішень. На думку E. Turban ідеальна СППР володіє наступними характеристиками:

1 СППР взаємодіє з слабоструктурованими рішеннями;

2 СППР може бути використана особами приймають рішення різного рівня;

3 СППР може бути адаптована для групового або індивідуального використання;

4 СППР дозволяє підтримувати як взаємозалежні, так і послідовні рішення;

5 СППР здатна підтримувати три фази процесу рішення: інтелектуальну частину, створення і сам вибір;

6 СППР дозволяє враховувати різні методи і стилі рішення, що безумовно буде корисним при розв'язанні задачі групою осіб;

7 СППР повинна бути гнучкою і спроможною до адаптації до змін і організації, і її зовнішнього оточення;

8 СППР максимально проста в експлуатації і модернізації;

9 СППР підвищує ефективність процесу прийняття рішення;

10 СППР дозволяє ОПР управляти процесом прийняття рішень з використанням комп'ютера, але не навпаки;

11 СППР здійснює підтримку еволюційного використання і здатна легко адаптуватися до мінливих вимог;

12 СППР може бути легко створена, якщо також легко може бути сформульована логіка її конструкції;

13 СППР здатна підтримувати моделювання;

14 СППР здатна використовувати знання.

Класифікації СППР:

На рівні з поняттям, для систем підтримки прийняття рішень також відсутня загальноприйнята класифікація. Різні автори висувають різні теорії про класифікації.

На рівні користувача поділяє системи підтримки прийняття рішення на три типи:

- пасивні;
- активні;
- кооперативні;

Пасивна СППР - це система, що допомагає процесу ухвалення рішення, але не має можливості виносити пропозицію, яка саме з рішень варто приймати. Активна СППР - це система, навпаки, має можливість робити пропозицію, яке з доступних рішень слід вибрати. А кооперативна СППР дозволяє особі, що приймає рішення, доповнювати та вдосконалювати рішення, які пропонує система, посилаючи після цього внесені зміни в систему для перевірки. У відповідь, СППР також доповнює та покращує рішення і знову посилає їх користувачеві. Цей процес триває в циклі до моменту отримання погодженого вирішення.

На концептуальному рівні відрізняє системи, з керованих ними об'єктів:

- керовані повідомленнями (Communication-Driven DSS);
- керовані даними (Data-Driven DSS);
- керовані документами (Document-Driven DSS);
- керовані знаннями (Knowledge-Driven DSS);
- керовані моделями (Model-Driven DSS).

Коротко охарактеризуємо кожну з систем.

Система, керована повідомленнями (Communication-Driven DSS) - система, здатна підтримувати групу користувачів, які здійснюють роботу над виконанням однієї загальної задачі. Системи, керовані даними (Data-Driven

DSS) - системи, спрямовані на роботу з даними (також Data-oriented DSS), які орієнтуються в основному на доступ і маніпуляцію з якимись даними. Системи, керовані документами (Document-Driven DSS) - системи, що здійснюють управління, пошук, а також маніпуляції з наявною неструктурованою інформацією, заданої в різних формах. Системи, керовані знаннями (Knowledge-Driven DSS) - системи, що забезпечують рішення завдань у формі фактів, правил, процедур. Нарешті системи, керовані моделями (Model-Driven DSS) - це системи характеризуються доступ і маніпуляції з математичними моделями (наприклад: імітаційні, фінансові). Необхідно також відзначити, що деякі OLAP систем, здатні виконувати складний аналіз даних, можуть бути класифіковані як клас Гібридних систем, які здатні забезпечувати і моделювання, пошук і обробку даних.

На технічному рівні розрізняються системи всього підприємства і настільні системи. Система підприємства - це система, яка має сполучення з великими сховищами інформації і здатна обслуговувати деяку кількість менеджерів даного підприємства. Настільна система - це невелика система, спроєктована для обслуговування лише одного користувача і його комп'ютера.

У різних джерелах можна зустріти й інші теорії про класифікації СППР (Hevner і Power, Holsapple і Whinston Golden, Alter). Увагу варто звернути на чудову (для свого часу) класифікацію Alter'a, суть якої полягає в розбитті всіх систем підтримки прийняття рішень на 7 різних класів, проте в даний час цю класифікацію можна назвати застарілою.

Також системи підтримки прийняття рішень можуть бути класифіковані на основі тих даних, з якими вони працюють. Умовно системи можуть бути розділені на оперативні та стратегічні. Оперативні системи - системи, спроєктовані для негайного реагування на зміни, що відбулися будь-яких умов у ситуацію на даний момент часу при управлінні фінансово-господарськими процесами підприємства. Стратегічні системи - це системи,

спрямовані на аналіз великих обсягів різнорідної інформації, одержуваної з різних джерел. Основною метою цих систем підтримки прийняття рішень є знаходження оптимальних альтернатив розвитку бізнесу підприємства з урахуванням впливу на неї різних факторів: стан цільових ринків компанії, зміни в законодавстві, зміни ринків капіталів та фінансових ринків та інші.

Системи першого типу (тобто оперативні) були названі як «Інформаційні Систем Керівництва (Executive Information Systems EIS). Такі системи є набором кінцевих звітів, створених на основі деяких даних з транзакционной ІС компанії, в ідеалі реально відображають в режимі «online» головні аспекти фінансової і виробничої діяльності. Для системи характерні наступні властивості:

- звіти ґрунтуються на стандартних для організації запитах; кількість звітів невелика;

- ІСР демонструють звіти в максимально зручному вигляді; поряд з таблицями і діловою графікою - різні мультимедійні можливості;

- ІСР спрямовані на конкретний вертикальний ринок; управління ресурсами, маркетинг, фінанси.

Системи другого типу (стратегічні) - це системи, що передбачають досить глибоку опрацювання інформації. Стратегічні системи спеціально перетворені таким чином, щоб їх було зручно використовувати в процесі прийняття рішень. Невід'ємним компонентом систем підтримки прийняття рішення цього рівня є якісь правила прийняття рішень, які на основі агрегованих даних, дозволяють менеджерам компанії обґрунтовувати свої рішення, а також знижувати ризики. Системи другого типу останнім часом отримали активний розвиток. Технологічно дані системи будуються на засадах багатовимірного представлення та аналізу даних (OLAP).

При створенні СППР можна також використовувати Web-технології. В даний час СППР на основі Web-технологій для ряду компаній є синонімами

СППР підприємства. Приклад рішення СППР з використанням Web-технології буде розглянуто далі.

2.3 Методи підтримки прийняття рішень на основі інформаційних технологій

Сучасні інформаційні системи інтелектуальної підтримки процесів розробки і реалізації управлінських рішень (Системи підтримки прийняття рішень - СППР) являють собою системи, що максимально пристосовані до рішення задач повсякденній управлінській діяльності, є інструментом, покликаним надати допомогу особам, що приймають рішення (ОПР). З допомогою систем підтримки прийняття рішень може здійснюватися вибір рішень деяких неструктурованих, а також слабоструктурованих завдань, в тому числі і багатокритеріальних. При цьому під багатокритеріальністю розуміється оцінка прийнятих рішень не за однією, а за сукупністю кількох показників (критеріїв), що розглядаються в один момент часу. Інформаційна складність полягає в необхідності обліку досить великих обсягів даних, яка практично нездійсненна без допомоги сучасної обчислювальної техніки. У даних умовах кількість можливих рішень, зазвичай, досить велике, і вибір оптимального з них без всебічного аналізу швидше за все призведе до грубих помилок.

Система підтримки рішень (СППР вирішує дві основні задачі:

- вибір найкращого рішення з безлічі можливих (оптимізація);
- упорядкування можливих рішень за переваги (ранжування).

В обох задачах першим і найбільш принциповим моментом є вибір сукупності критеріїв, на основі яких в подальшому будуть оцінюватися і зіставлятися можливі рішення (будемо називати їх також альтернативами). Система СППР допомагає користувачеві зробити такий вибір.

Умовно СППР можна класифікувати за методами вирішення певних проблем. Розглянемо методи прийняття рішень на основі інформаційних технологій: методи застосовувана в СППР.

Для підтримки прийняття рішень за допомогою інформаційних технологій, включаючи аналіз і вироблення альтернатив, у СППР використовуються велика кількість методів. Наприклад:

1) інформаційний пошук;

2) інтелектуальний аналіз даних;

3) витяг (пошук) знань у базах даних;

4) міркування на основі прецедентів;

5) імітаційне моделювання;

6) генетичні алгоритми;

7) штучні нейронні мережі;

8) методи штучного інтелекту.

Таку класифікацію методів можна охарактеризувати як «спосіб досягнення мети». В якості порівняння з такою класифікацією доцільно розглянути методи і моделі, представлені в СПР, згруповані за наступними напрямами:

1 Методи прийняття рішення з використанням принципу Більшості: PUR1 - PUR12;

2 Принципу Парето: PRT1 - PRT12;

3 Багатоцільової оптимізації: OTNUST, USTUP, ABSUST;

4 З використанням принципу Байєса: BAJES, BAJNOEXP, BAJPOR, BAJPRI0R, BAJPORPR, LAPLAS, LAPLP0R;

5 Методи прийняття рішення в динамічній постановці: BELMAN, MARKON, MARKBS;

6 В умовах повної невизначеності: WALD, WALDPOR, OPTIMIST, OPTIMPOR, HURWICZ, SAVAGE, BRAUN, HURWPOR.

Проте постійне прагнення людства до зниження витрат у всіх можливих формах призвело до впровадження СППР у хмарні технології. Стрімкий розвиток даної сфери, а також її актуальність підштовхує встановити «Web-based» СППР осібно від інших і порівняти її з позицій переваг і недоліків.

Розглянемо Метод аналітичних мереж» в якості порівнянного (на прикладі ППО SuperDecisions) с web-based системою «Експертна система підтримки прийняття рішень» (EDSS).

2.3.1 Особливості методу аналітичних мереж

МАС (Метод аналітичних мереж) - більш загальна форма методу аналізу ієрархій (МАІ), що використовується в умовах мульти-критериальності. МАІ структурує рішення проблеми в ієрархію з метою визначення критерію вибору і альтернативи, в той час як МАС структурує його в якості аналітичної мережі, і потім використовують систему парних порівнянь для вимірювання ваги компонентів структури, і, нарешті ранжує альтернативи у вирішенні.

Існує багато проблем, вирішення яких не може бути прийнято з допомогою МАІ. Наприклад, коли відбувається взаємодія елементів на високому рівні з елементів більш низького рівня і їх залежності повинні бути прийняті до уваги. МАС надає рішення для проблем, які не можуть бути структуровані ієрархічно. Визначення значення критерію важливо не тільки для альтернатив; як і в ієрархії важливості самих альтернатив визначає важливість критеріїв. Тому дуже багато проблем можуть бути змодельовані з використанням діаграми «мережа».

Мережеві моделі не повинні показувати ієрархічну структуру, що означає, що вони не повинні бути лінійними зверху вниз. Насправді МАС використовує мережу якій немає необхідності вказувати рівні взагалі. Тому термін «рівень» в МАІ замінюється терміном «кластер». Мережева модель має підключення типу «цикл»: кластери елементів і петлі, які з'єднують кластери самим до себе. Цей вид моделі називаються системами зі зворотним зв'язком. На практиці, багато проблем пов'язані з рішенням зворотного зв'язку.

Хоча МАС і МАІ схожі в порівняльній фазі, відмінності у фазі все таки є. У МАС, шкала відносин пріоритетних векторів, отриманих з матриць

попарних порівнянь не синтезується лінійно, як в MAI. Також там немає вимоги, що кожен елемент кластера впливає на елемент в іншому кластері. У цьому випадку, ці елементи дають нульове значення за їх внесок. А суперматриця, яка складається з шкал відносин пріоритетних векторів, отримана із матриць попарних порівняння і нульових векторів, повинна бути стохастичною для отримання значущих результатів. Кожен блок векторів-стовпців зважуються на пріоритет відповідного кластера, їх елементи відображаються вертикально на лівій стороні матриці і горизонтально у верхній частині матриці. Щоб переконатися, що ця матриця є стохастичною можна порівняти самі кластери, які знаходяться на лівій по відношенню до їх впливу на кожен кластер на самому верху. Отримані пріоритети кластерів потім використовуються для ваг кластерів по відношенню до відповідного кластеру на самому верху.

Загалом, алгоритм MAC включає в себе наступні етапи:

1 Проєктування мережевої структури задачі;

2 Обчислення ваг всіх елементів кожного з компонентів (за допомогою матриці попарних порівнянь - як і в MAI) відповідно до їх впливу на інші компоненти;

3 Перевірка узгодженості введених даних;

4 Формування суперматриці з векторів;

5 Приведення суперматриці до стохастичного увазі (зважування блоків на відповідні ваги у разі відсутності стохастичності);

6 Зведення суперматриці в граничну ступінь;

7 Отримання результату в першому стовпці суперматриці.

Таким чином, аналіз ієрархій (MAI) є способом прийняття рішень, що включає в себе якісні фактори. У цьому методі шкали коефіцієнтів виходять з порядкових шкал, які отримують з окремих суджень за якісним факторам використання матриці парних порівнянь. Аналітичний Метод мереж (MAC) також використовує матрицю попарних порівнянь для отримання

співвідношення масштабів. Різниця між цими двома способами з'являється в моделюванні завдання та обчислення остаточних пріоритетів альтернатив з співвідношень ваг отриманих раніше. MAI моделює прийняття рішення проблеми з допомогою однонаправленої ієрархічного відносини між елементами рішення. Однак MAC дозволяє проводити більш складні взаємозв'язки між елементами рішення.

Як приклад практичного використання метод аналітичних мереж (MAC) буде розглядатися програма SuperDecisions.

Програма SuperDecisions використовується для прийняття рішень з залежністю і зворотним зв'язком. Вона реалізує метод аналізу ієрархій (MAI), і метод аналітичний мереж (MAC). Обидва методи використовують одну фундаментальну формулу - процес визначення пріоритетів на основі винесення висновків по парах елементів, або отримання пріоритетів шляхом нормалізації прямих вимірювань. В MAI елементи розташовані у вигляді ієрархічної структури з метою опис критеріїв вибору альтернатив, MAC елементи зібрані в групи, одна з яких містить альтернативи, які містять інші критерії або інші елементи рішення. У MAC немає конкретного елемента мети, а пріоритети визначаються в рамках відносного впливу кожного з ознак на альтернативи. Кластери розташовані в мережі і мають зв'язок між елементами. Іноді зв'язку розташовуються в кілька рівнів, наприклад, коли завдання розпадається на переваги, можливості, витрати і ризики. Більшість методів прийняття рішень в тому числі і MAI припускають незалежність між критеріями і альтернативами, або одним з критеріїв, або однією з альтернатив. MAC немає подібних обмежень.

2.3.2 Особливості Веб-СППР (WB-DSS)

Хмарні обчислення відкривають доступ до обчислювальних ресурсів, які будуть доступні тільки на вимогу. Еластичність, ефективність і скорочення витрат приваблюють багато підприємства розглянути варіант міграції додатків в хмару. Веб-системи підтримки прийняття рішень (WB-DSS) є

системам підтримки прийняття рішень, які доступні в віддалено через мережу Інтернет. Вони мають не поступаються настільним системам кордону функціоналу. Однак мають характерні ознаки, що відрізняють їх від настільних аналогів:

- доступність в інтернеті;

- підтримка приватних осіб / клієнтів / працівників / менеджерів / груп у процесі прийняття рішень, незалежно від їх фізичного місцезнаходження або часу;

- використання даних, баз знань, документів і моделей які мають можливість звернутися до величезного розмаїття великих груп користувачів;

Основними відмінностями веб-версії систем підтримки прийняття рішень від настільних аналогів є кілька дуже вагомих ознак. В першу чергу - доступність глобальної аудиторії. При розміщенні на віддаленому сервері доступність до ресурсів обмежується лише фантазією розробників і гаманцем власника, оскільки обчислювальні потужності, розташовані в «хмарах» приведуть до певних витрат.

Іншою важливою ознакою є простота використання. Такі системи спрямовані на зниження навантаження на ОПР і не вимагають додаткового навчання роботи з системою - інтуїтивно зрозумілий інтерфейс дозволяє швидко приступити до роботи.

Вагомим чинником також є безпека. Проблеми безпеки можуть обмежити застосування WB-DSS чутливих областях. У таких випадках WB-DSS вимагає додаткових компонентів для запобігання загроз безпеки і помилки в різних точках обміну інформацією.

В цілому, той факт, що WB-DSS доступні через Web, створює як можливості так і проблеми, які, однак, зазвичай не присутні в настільних версіях СППР.

Тим не менш, разом з дискусіями про порівнянні веб-і настільних систем підтримки прийняття рішень виникають суперечки і так званої міграції настільних систем у веб-платформи.

Системи підтримки прийняття рішень, які були призначені для роботи на робочому столі, можуть бути доступні в інтернеті з метою зробити їх більш широко доступними для широкої аудиторії. Як приклад вже існуючих діючих прикладних СППР у веб-версії можна навести два випадки:

1 Expert Choice (www.expertchoice.com);

2 EXSYS (www.exsys.com).

Expert Choice використовується, щоб зробити вибір між декількома альтернативами, заснованими на множині критеріїв прийняття рішень і різних атрибутів. Наприклад, можна використовувати Expert Choice у виборі будинку серед безлічі, ґрунтуючись на відповідних атрибутах (наприклад, місце розташування, кількість кімнат, розмір ділянки), а також в цілях оцінки альтернатив (наприклад, купівля кращого будинку в межах бюджету). Expert Choice була розроблена на основі методу аналізу ієрархій (AHP), а також може бути використана при наявності декількох учасників, які беруть участь у прийнятті рішення. Цей інструмент був доступний задовго до популярності в Інтернеті. Зараз же веб-версія доступна як окремий інструмент під назвою «Expert Choice decision portal «(ECDP), розроблена тільки для використання через мережу Інтернет.

EXSYS використовується для розробки експертних систем для надання консультативних послуг особам, які приймають рішення. Експертна система може бути визначена як "система, яка використовує людські знання використовуються комп'ютером, щоб вирішити проблеми зазвичай вимагають людського досвіду". Як і Expert Choice, EXSYS також використовувалася для підтримують прийняття рішень до початку широкого використання в Інтернеті. Цей продукт став одним з перших, що здійснили перехід до веб-версії.

Переходи великих гравців на ринку СППР мають вагомі причини.

З одного боку, переваги переходу до Web здаються незаперечними:

- веб-доступ до СППР економить витрати на установку програми, тому що він встановлений централізовано і доступний з декількох місць. Таким чином, веб-сервери замінюють ще і мережеві сервери для цих систем;

- веб-доступ знижує витрати на технічне обслуговування системи, модель оновлення, оновлення даних та інші зміни, які можуть статися в системі, що розвивається з плином часу.

- особи, які приймають рішення і споживачі мають більш широкий доступ до системи, тому що вона доступна з будь-якого комп'ютера в будь-який час.

Таким чином, веб-доступ здатний зберегти витрати на встановлення, обслуговування та оновлення системи. Це, в свою чергу, збільшує доступ до системи для введення даних, а також для спільного вирішення поставлених завдань.

2.3.3 Впровадження ЕСППР в MS Azure

Для оцінки ефективності міграції програми в хмарну платформу на практиці, розгорнемо «Експертну систему підтримки прийняття рішень» в одній з хмарних платформ.

В якості платформи для впровадження програми «Експертна система підтримки прийняття рішень» була выбрата MS Azure.

MS Azure - хмарна платформа, за допомогою якої можна розміщувати в «хмарних» датацентрах Microsoft і «віртуально»-необмежено масштабувати програми. Windows Azure реалізує модель Platform as a service (PaaS), коли платформа надається клієнтові як сервіс. Платформа Windows Azure надає можливість розробки і виконання програм і зберігання даних на серверах, розташованих в розподілених дата-центрах.

Інтерфейс програми представляє собою повністю закриту для користувача систему, управління якої здійснюється з консолі адміністратора (рисунок 2.5).

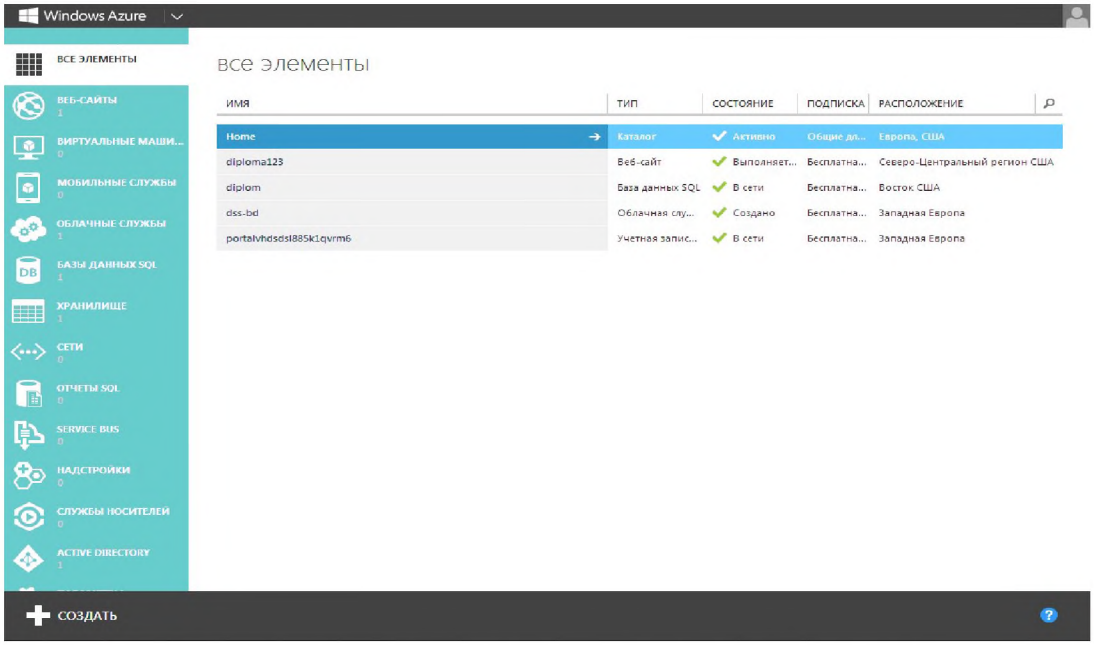

Рисунок 2.5 - Веб платформа MS Azure

Розгортання системи відбувається після створення Бази даних SQL і підключення сховища (наприклад, DropBox) з вмістом самої системи. Варто відзначити, що всі здійснювані операції інтуїтивно зрозумілі завдяки наочного інтерфейсу. Розгортання відбувається через новостворений веб-сайт та підключення бази даних через ADO.NET. (Частина фреймфорка .NET, що надає доступ до даних для додатків, заснованих на Microsoft .NET. Не є розвитком більш ранньої технології ADO, а є самостійною технологією)

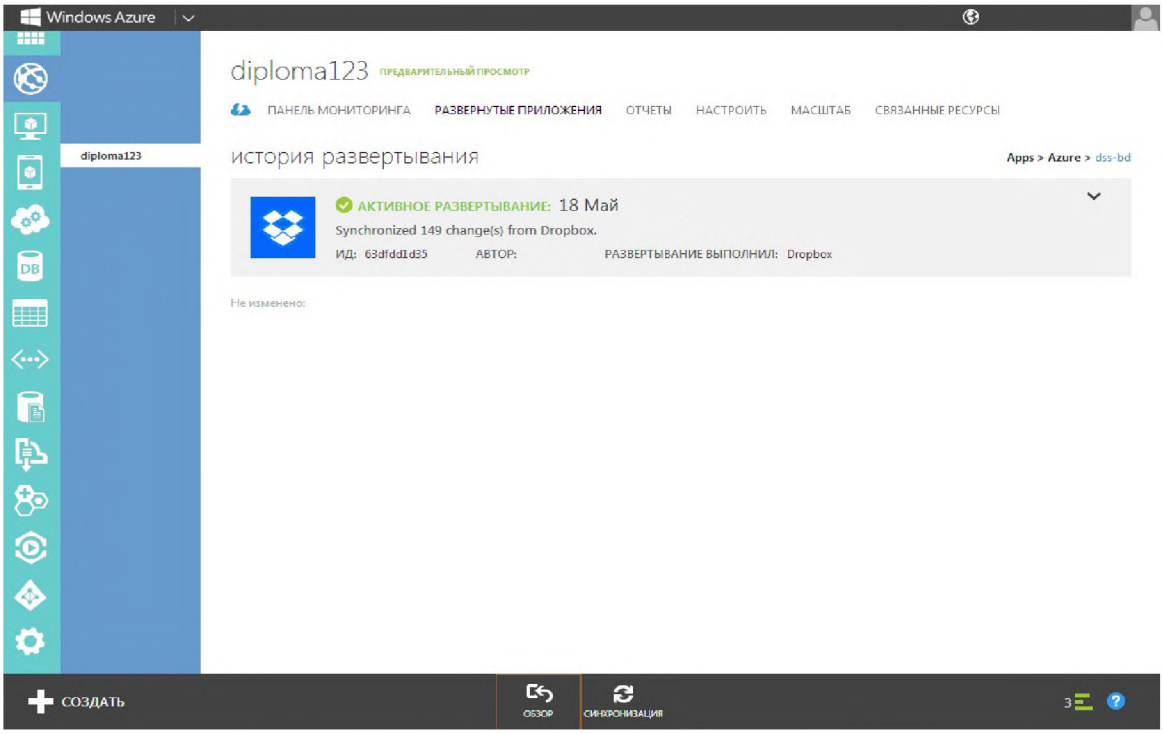

Рисунок 2.6 - Веб-платформа MS AZURE

У результаті виконаних дій, на створений сайт розгорнута «Експертна система підтримки прийняття рішень», готова вирішувати завдання вибору з допомогою більш ніж 25 методів.

За великим рахунком, на цьому всі труднощі щодо розгортання системи підтримки прийняття рішень в «хмарі» закінчуються. Безумовно, витрати на розробку функціональної частини самої системи вимагають великих ресурсів - і людських, і матеріальних, проте сам процес впровадження, або «міграції» досить простий і не витратний, що робить цей клас систем підтримки прийняття рішень потенційно привабливим для підприємств, як великих, так і дрібних, мають обмежені бюджети на розвиток IT-стратегій.

2.4 Синтез СППР для моделювання загроз інформацій для автоматизованої системи класу 3

В результаті постійних доробок існуючих методів рішення завдань систем підтримки прийняття рішень за допомогою інформаційних технологій, дуже великий спектр завдань. Для демонстрації ефективності СППР, розглянемо актуальні завдання вибору найбільш актуальної загрози

інформації з моделі загроз для автоматизованої системи класу 3, що дозволяє в першу чергу звернути увагу на необхідну загрозу безпеки. Приклад наведено на інформаційних загрозах будівельно-господарчого гіпермаркету «Епіцентр К».

Ознаки порівняння:

1 Ймовірність реалізації загрози - під ймовірністю реалізації загрози розуміється визначений експертним шляхом показник, що характеризує, наскільки вірогідним є реалізація конкретної загрози безпеки для даної системи в складних умовах обстановки;

2 Збиток від реалізації - це критерій який показує які втрати може понести підприємство після реалізації загрози та зможе взагалі функціонувати;

3 Рівень реалізації загрози - це критерій який показує необхідний рівень можливостей порушника для реалізації загрози;

4 Критерії інформації що порушуються при скоєні загрози (конфіденційність).

5 Критерії інформації що порушуються при скоєні загрози – це (цілісність).

6 Критерії інформації що порушуються при скоєні загрози (конфіденційність).

Вихідні дані, що необхідні для мого розрахунку були представлені в таблицях 2.2 та 2.3. (Таблиця 2.2 - Вихідні дані для розрахунку вірогідності загрози та таблиця 2.3 - Значимість оцінок)

Таблиця 2.2 - Вихідні дані для розрахунку вірогідності загрози

Признаки / Загроза	Ймовірність реалізації	Збиток від реалізації	Рівень реалізації загрози	Порушення конфіденційності	Порушення цілістності	Порушення доступності
Знищення (руйнування) інформації	0,2	1	0,8	0	1	1
Модифікація інформації	0,2	0,75	1	0	1	0
Порушення встановленого режиму доступу	0,75	1	1	1	1	1
Помилки при використанні ПЗ	0,6	0,75	0,8	0	1	1
Шкідливе ПЗ	0,75	1	0,6	1	1	1

В таблиці 2.2 коефіцієнти розташовані в порядку зростання від 0 (нижнього) до 1 (високого) .

Таблиця 2.3 - Значимість ознак

Ознаки	Збиток від реалізації	Ймовірність реалізації	Рівень реалізації загрози	Порушення конфіденційності	Порушення цілісності	Порушення доступності	Разом
Коефіцієнти значення	25	10	20	15	15	15	100

2.4.1 Рішення задачі за допомогою методу аналітичних мереж

Для вирішення даної задачі методом аналітичних мереж використовуємо програму SuperDesicions, спеціалізоване програмне забезпечення для моделювання аналітичних мереж і розрахунку пріоритетів.

Мережа буде складатися з 3 компонентів (в термінології програми – кластерів), з яких «Мета» є компонентом джерелом, а «Альтернативи» - компонентом – стоком. Центральну роль відіграє кластер «Ознаки», містить 6 ознак на основі яких будуватиметься рішень даної задачі (рисунок 2.7).

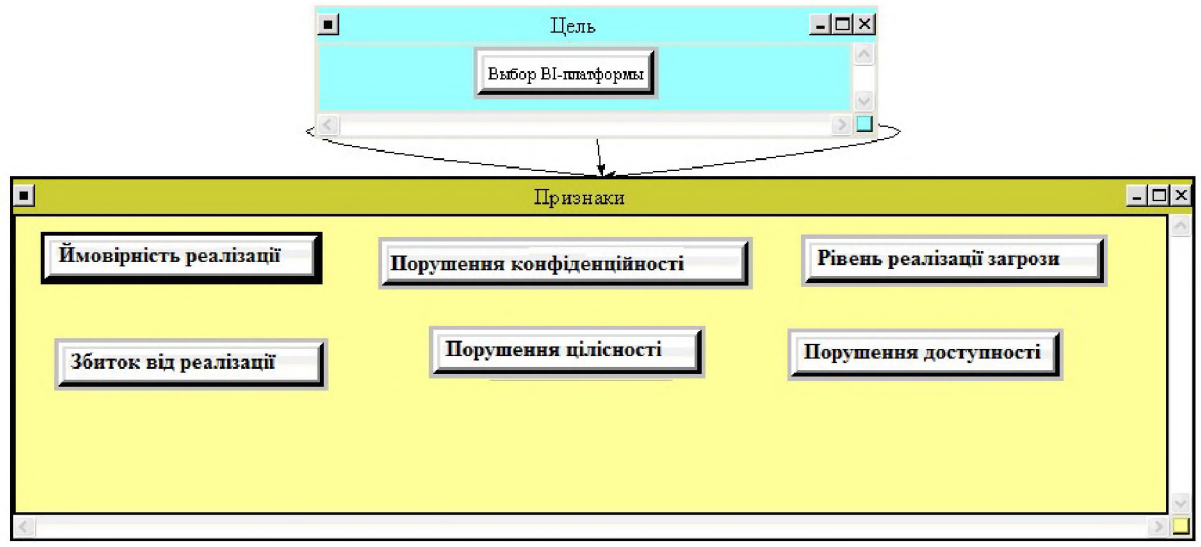

Рисунок 2.7 - Структура завдання

Кластер містить всі ознаки 6 ознак, описані в умовах задачі. Кластер «Альтернативи» містить 5 загроз інформаційної безпеки для автоматизованих систем класу 3, з яких ОПР належить зробити вибір, ґрунтуючись на представлених програмою рекомендаціях.

Приймемо, що кожна з ознак пов'язана з кожною з альтернатив певних коефіцієнтів. Відповідно, кожна з альтернатив пов'язана з ознаками з допомогою коефіцієнтів значущості.

Після створення структури, для кожної виділеної взаємозв'язку необхідно ввести попарні порівняння. Система SuperDecisions дозволяє здійснювати введення різними способами (рисунок 2.8 - рисунок 2.12):

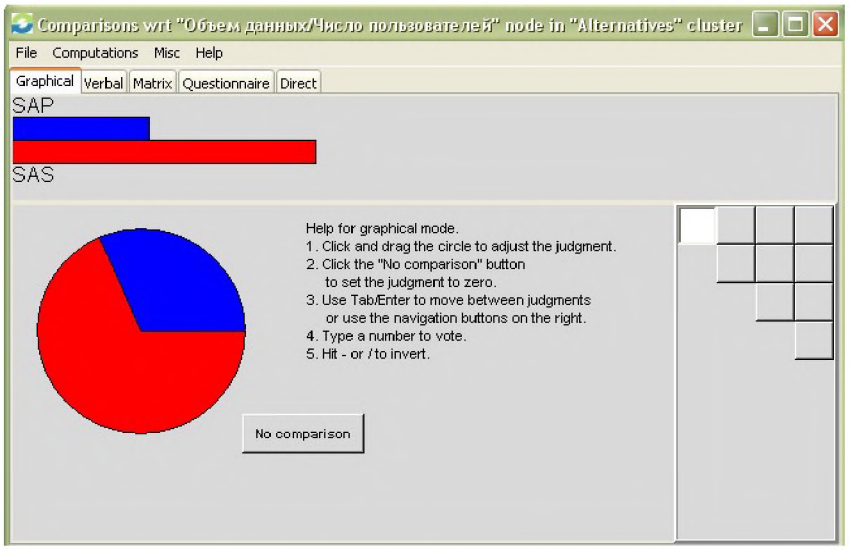

Рисунок. 2.8 - Графічний спосіб введення попарних

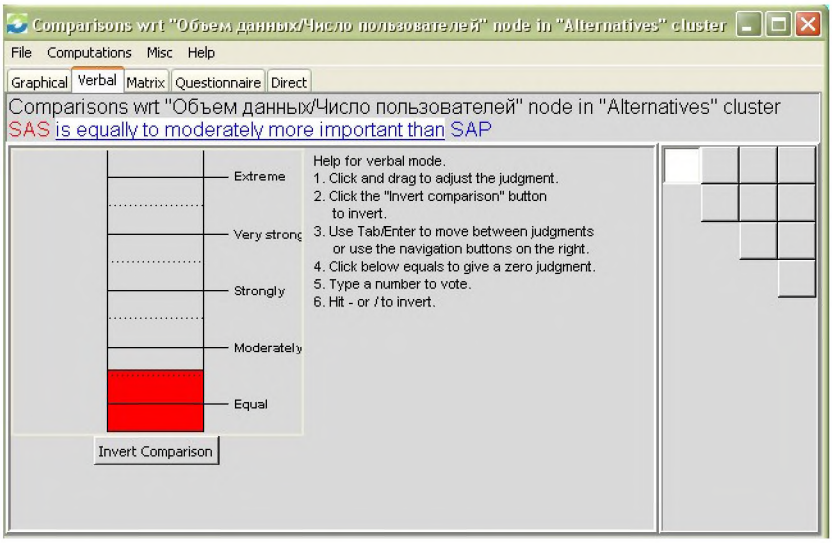

Рисунок 2.9 - Вербальний спосіб введення попарних порівнянь

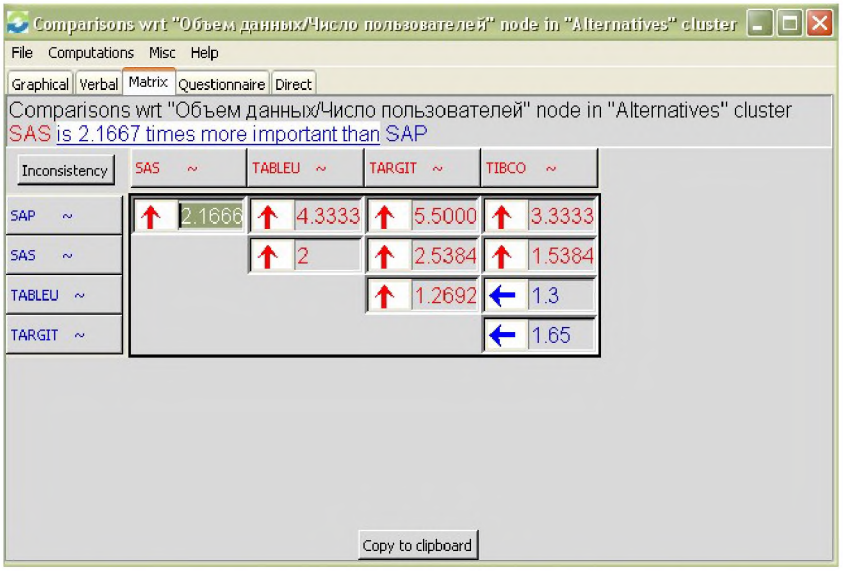

Рисунок 2.10 - Матричний спосіб введення попарних порівнянь

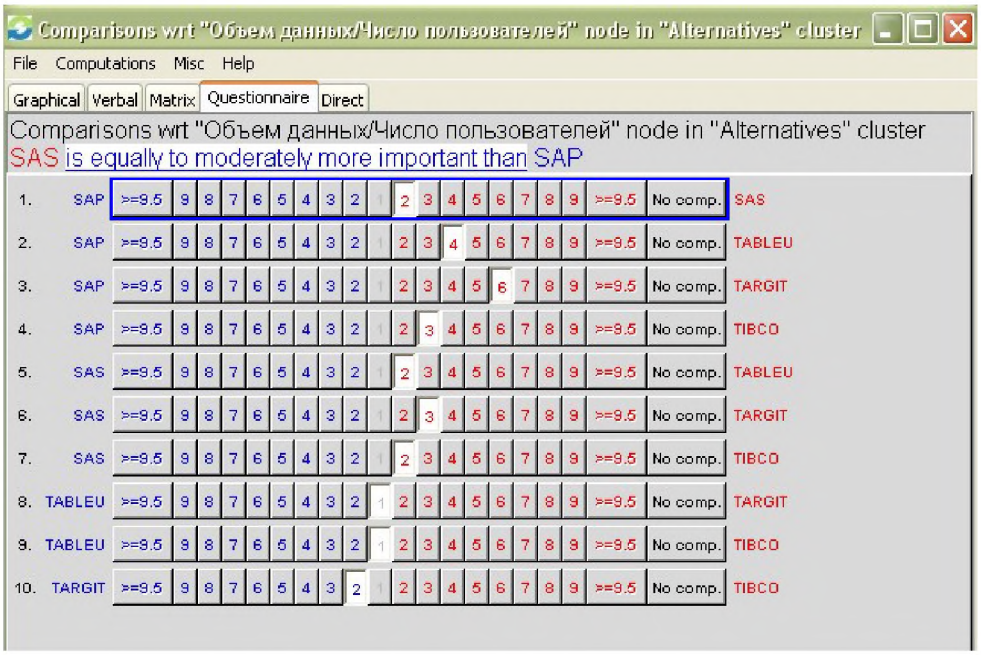

Рисунок 2.11 - Опитувальний спосіб введення попарних порівнянь

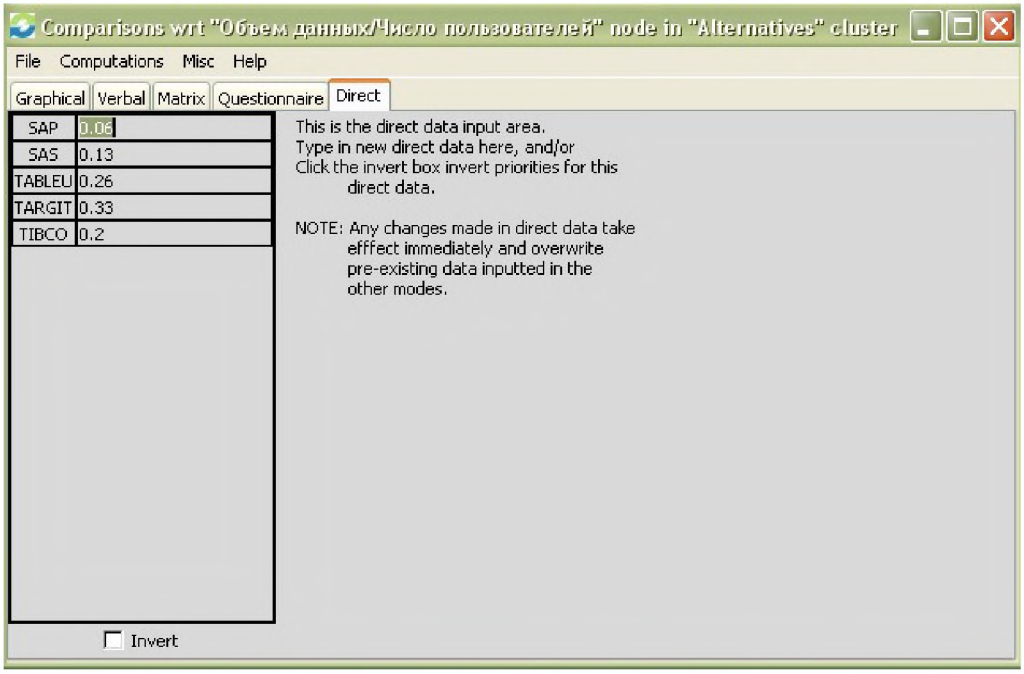

Рисунок 2.12 - Прямий спосіб введення попарних порівнянь

Так як вихідні дані представлені у вигляді кількісних оцінок, доцільно перевести оцінки, відносини до загальної суми для введення останнім, прямим способом введення.

Також програма дозволяє переглядати вектор відносної значущості різних елементів завдання.

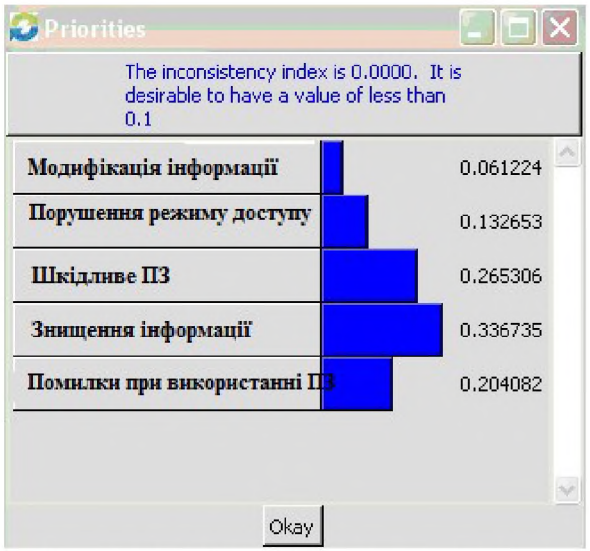

Рисунок 2.13 - Пріоритети ознак

На Рисунку 2.13 представлено вплив ознаки «Збиток від реалізації» на представлені альтернативи. Найбільший вплив ознака впливає на загрозу знищення (руйнування) інформації і шкідливе програмне забезпечення. У верхній частині вікна представлений показник узгодженості, значення якого не повинно перевищувати значення рівне 0,1.

Всі значення пріоритетів доступні в окремому вікні програми. Ознака №1 – "Збиток від реалізації" має найбільший пріоритет, що відповідає вихідним значенням завдання (рисунок 2.14).

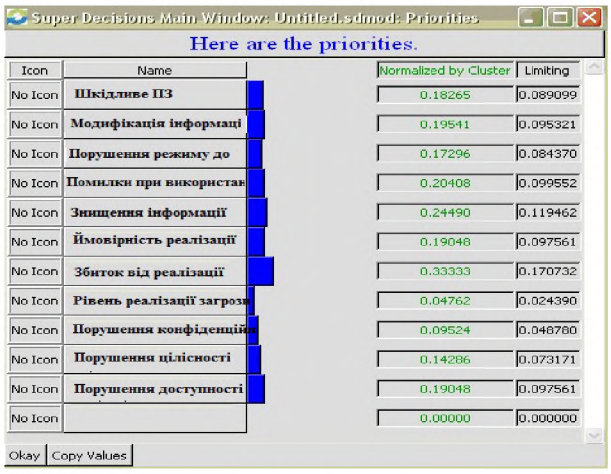

Рисунок 2.14 - Всі пріоритети

Після введення та перевірки значень необхідно сформувати суперматрицю з отриманих власних векторів відносної значущості. Інтерфейс програми дозволяє побудувати суперматриці:

Не зважена суперматриця зображена на рисунку 2.15

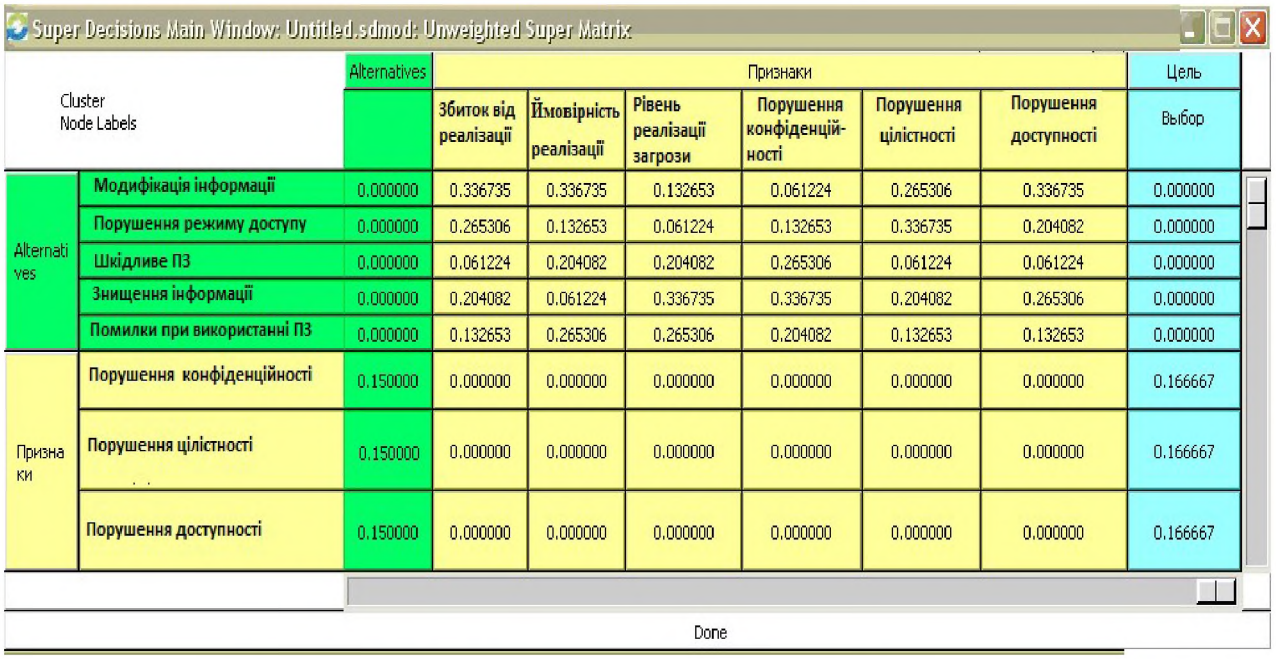

Рисунок 2.15 - Не зважена суперматрица

Зважена матриця, що містить пріоритети з матриць попарних порівнянь помножені на ваги блоків суперматриці (рисунок 2.16):

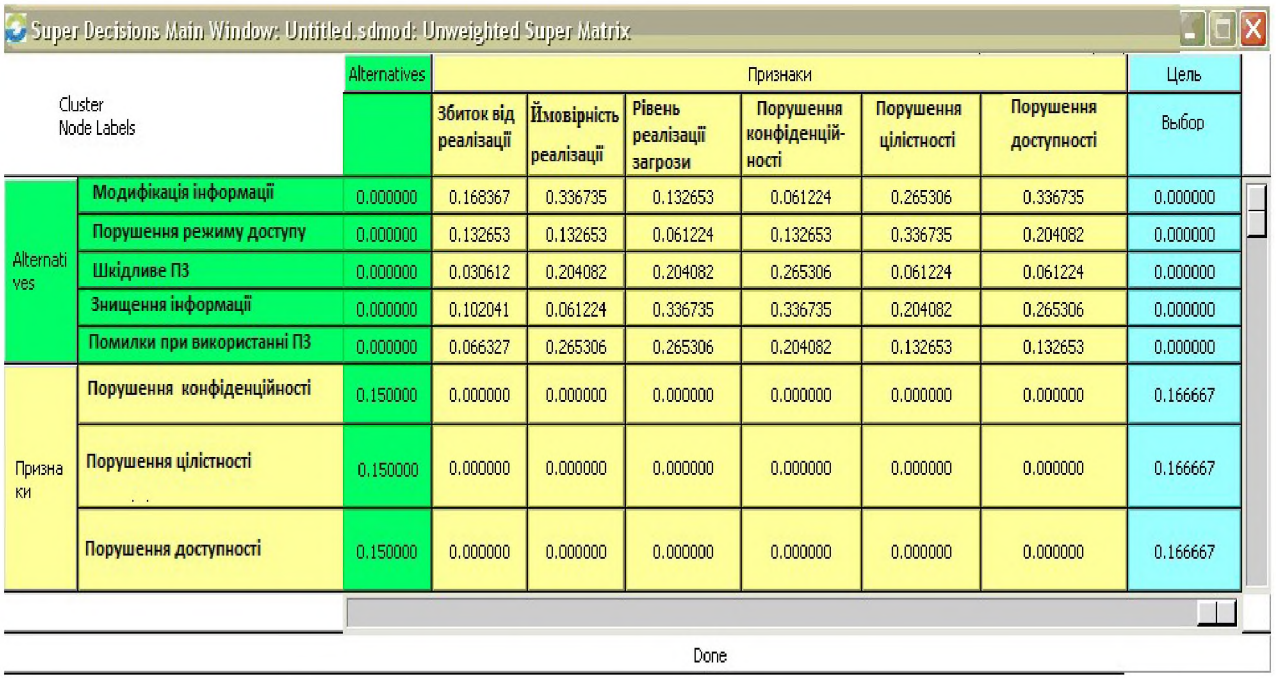

Рисунок 2.16 - Зважена суперматриця

Гранична суперматриця представлена (зважена суперматриця приведена до стохастичного увазі і зведена в граничну ступінь) нижче на рисунку 2.17.

Super Decisions Main Window: Untitled.sdmod: Limit Matrix

Cluster Node Labels		Alternatives	Признаки						Цель
			Збиток від реалізації	Ймовірність реалізації	Рівень реалізації загрози	Порушення конфіденцій-ності	Порушення цілістності	Порушення доступності	Выбор
Alternatives	Шкідливе ПЗ	0.119462	0.119462	0.119462	0.119462	0.119462	0.119462	0.119462	0.119462
	Помилки при використанні ПЗ	0.099552	0.099552	0.099552	0.099552	0.099552	0.099552	0.099552	0.099552
Признаки	Визуализация данных	0.048780	0.048780	0.048780	0.048780	0.048780	0.048780	0.048780	0.048780
	Интеграция внутри BI платформы	0.097561	0.097561	0.097561	0.097561	0.097561	0.097561	0.097561	0.097561
	Интеграция с внешними приложениями	0.073171	0.073171	0.073171	0.073171	0.073171	0.073171	0.073171	0.073171
	Порушення конфіденційності	0.170732	0.170732	0.170732	0.170732	0.170732	0.170732	0.170732	0.170732
	Порушення цілістності	0.097561	0.097561	0.097561	0.097561	0.097561	0.097561	0.097561	0.097561
	Порушення доступності	0.024390	0.024390	0.024390	0.024390	0.024390	0.024390	0.024390	0.024390

Done

Рисунок 2.17 - Гранична суперматрица

В якості результатів рішення задачі отримуємо графічне представлення значень пріоритетів досліджуваних альтернатив.

• стовпець Raw обчислений з суперматриці;

• стовпець Normals = нормалізований стовпець Raw;

• стовпець Ideals = елементи стовпця Raw / максимальний елемент цього стовпця.

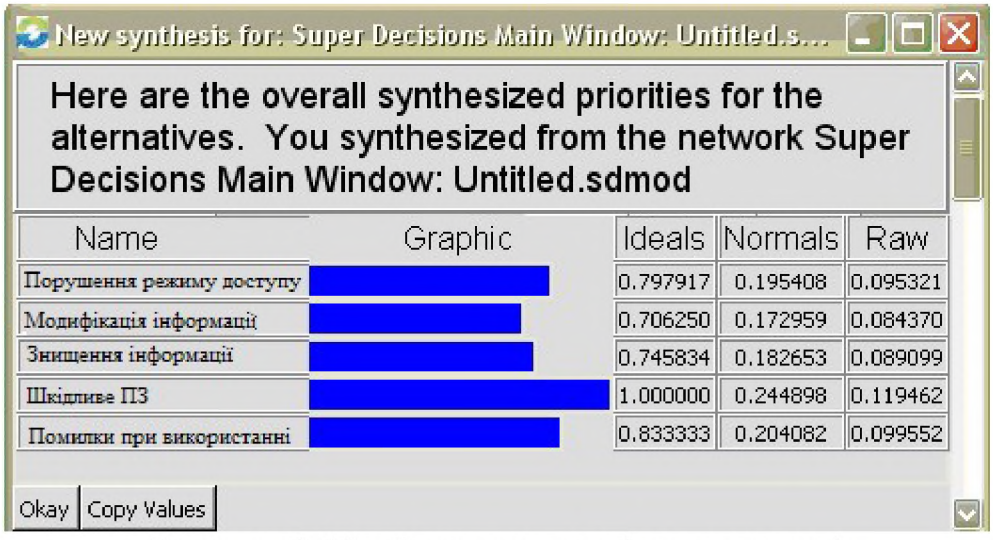

Рисунок 2.18 - Результат розв'язання задачі

Виходячи з отриманих результатів, альтернативи можна ранжувати наступним чином:

1 Шкідливе програмне забезпечення;

2 Порушення встановленого режиму доступу;

3 Помилки при використанні програмного забезпечення;

4 Знищення (руйнування) інформації;

5 Модифікація інформації.

Найбільш небезпечною є загроза шкідливого програмного забезпечення. На другому місці розташовується загроза порушення встановленого режиму доступу.

2.4.2 Рішення задачі за допомогою експертної системи підтримки прийняття рішень

Розгорнувши ПЗ «Експертна система підтримки прийняття рішень» у своїй «хмарі», ми можемо приступати до вирішення завдань. Розглянемо алгоритм рішення у даній системі на прикладі вихідною для даного дослідження завдання - це дозволить порівняти системи з точки зору витрат трудомісткості і часу.

Після створення завдання система пропонує вибрати метод її рішення. Здійснюється вибір або безпосередньо зі списку доступних методів, або за допомогою «майстра вибору, відповівши на кілька запитань якого, вам буде запропоновано конкретний метод рішення для вашої задачі (рисунок 2.19).

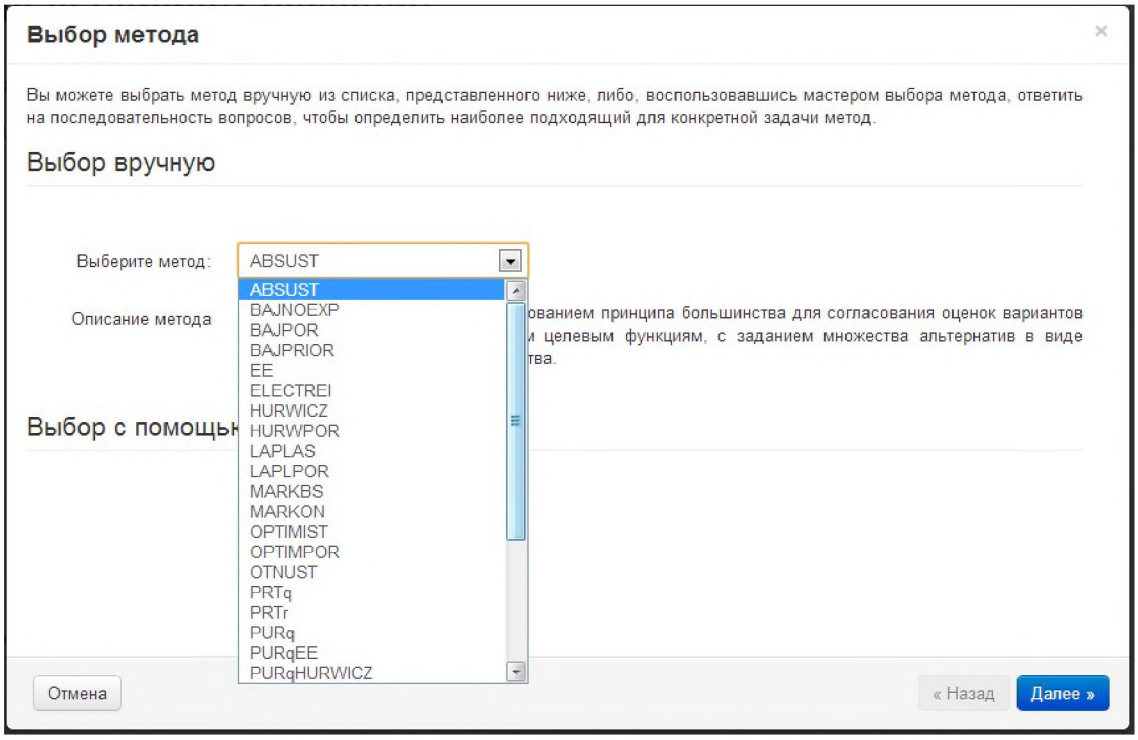

Рисунок 2.19 - Список методів ЕСППР

Розглянемо рішення задачі методом PURr - метод з використанням принципу більшості для узгодження оцінок варіантів рішення, формуються окремими експертами з позицій різних ознак (критеріїв) в різних проблемних ситуаціях, із завданням переваг в кількісній шкалі.

Створивши у відповідних вкладках альтернативи, ситуації, ознаки та експертів, можна приступати до введення значень вихідних даних завдання (рисунок 2.20 - рисунок 2.23).

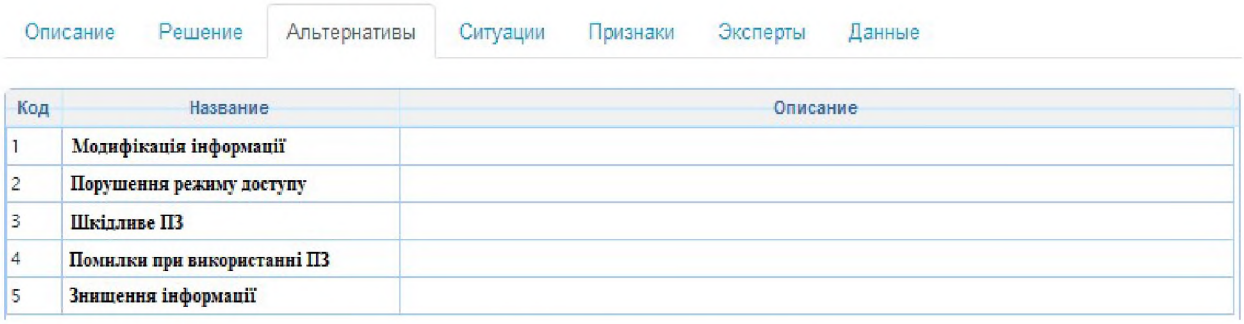

Рисунок 2.20 – Альтернативи

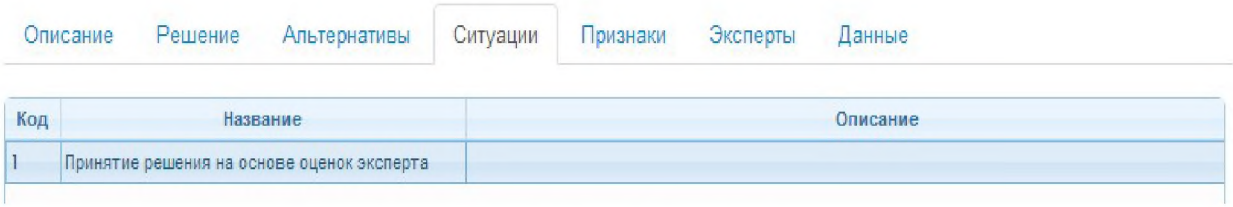

Рисунок 2.21 - Ситуації

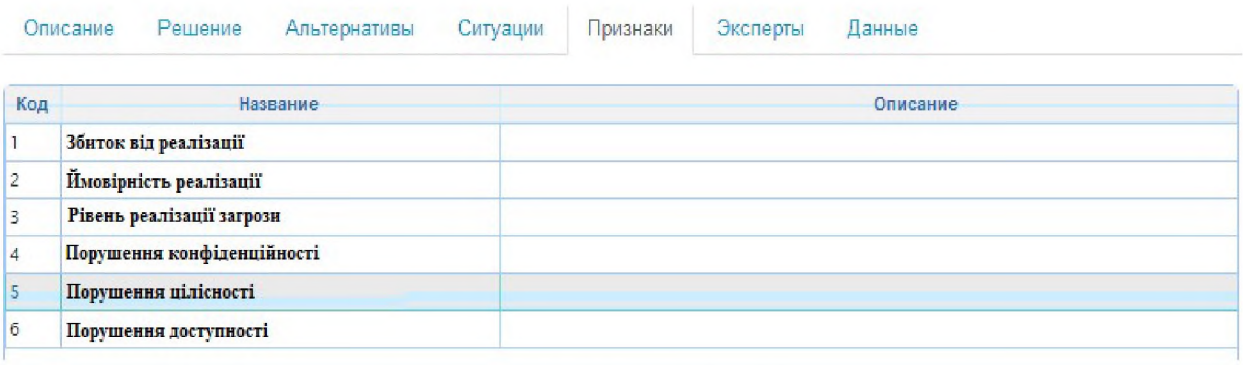

Рисунок 2.22 - Ознаки

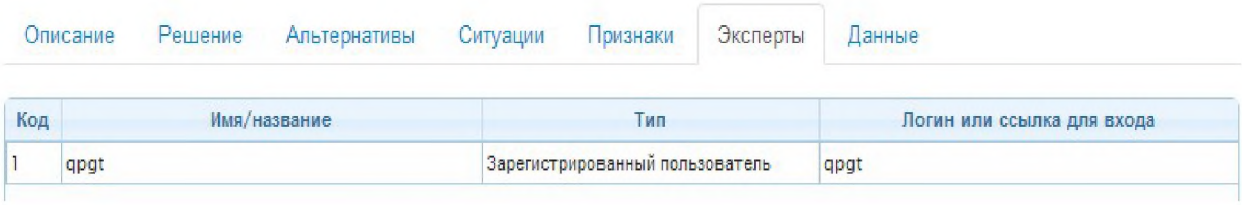

Рисунок 2.23 - Експерти

На вкладці «Дані» вводимо початкові значення коефіцієнтів відносної значущості ознак, а також експертні оцінки для кожної з альтернатив по кожній ознаці (рисунок 2.24).

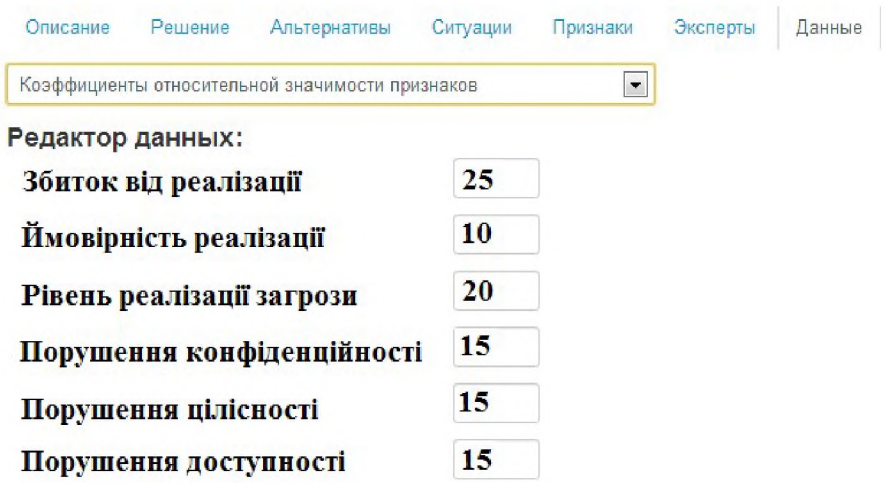

Рисунок 2.24 - Введення коефіцієнтів значимості

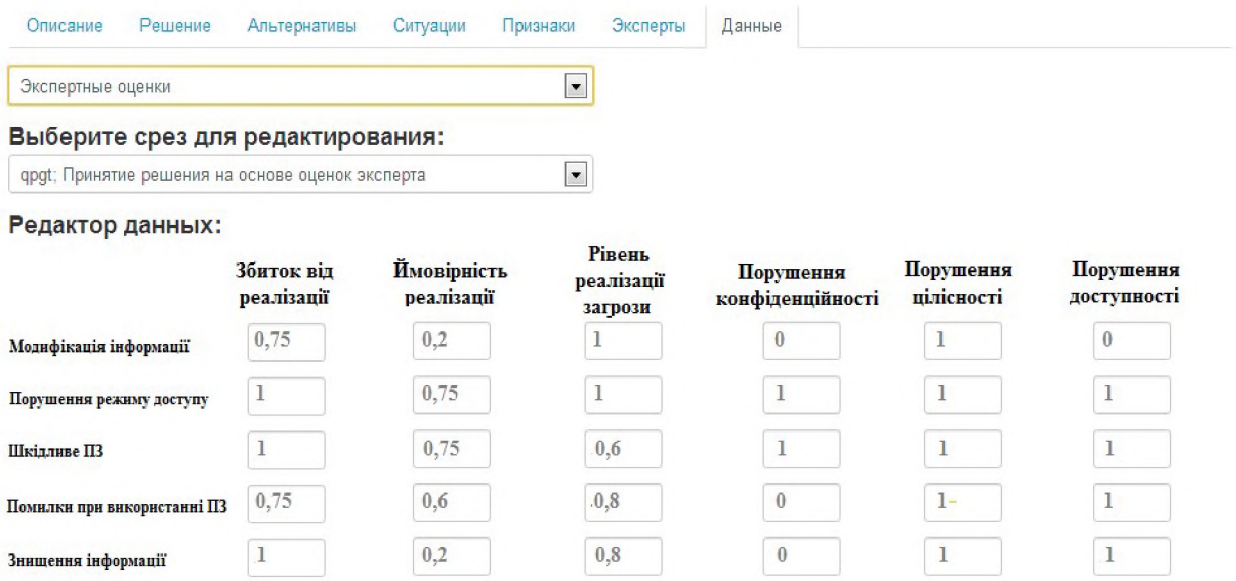

Рисунок 2.25 - Експертні оцінки

Переконавшись у правильності введення даних потрібно перейти на вкладку «Рішення» і натиснути кнопку «Вирішити».

Результат рішення представлений в компактному вигляді; ранжований за бажанням список альтернатив представлений на рисунок 2.26

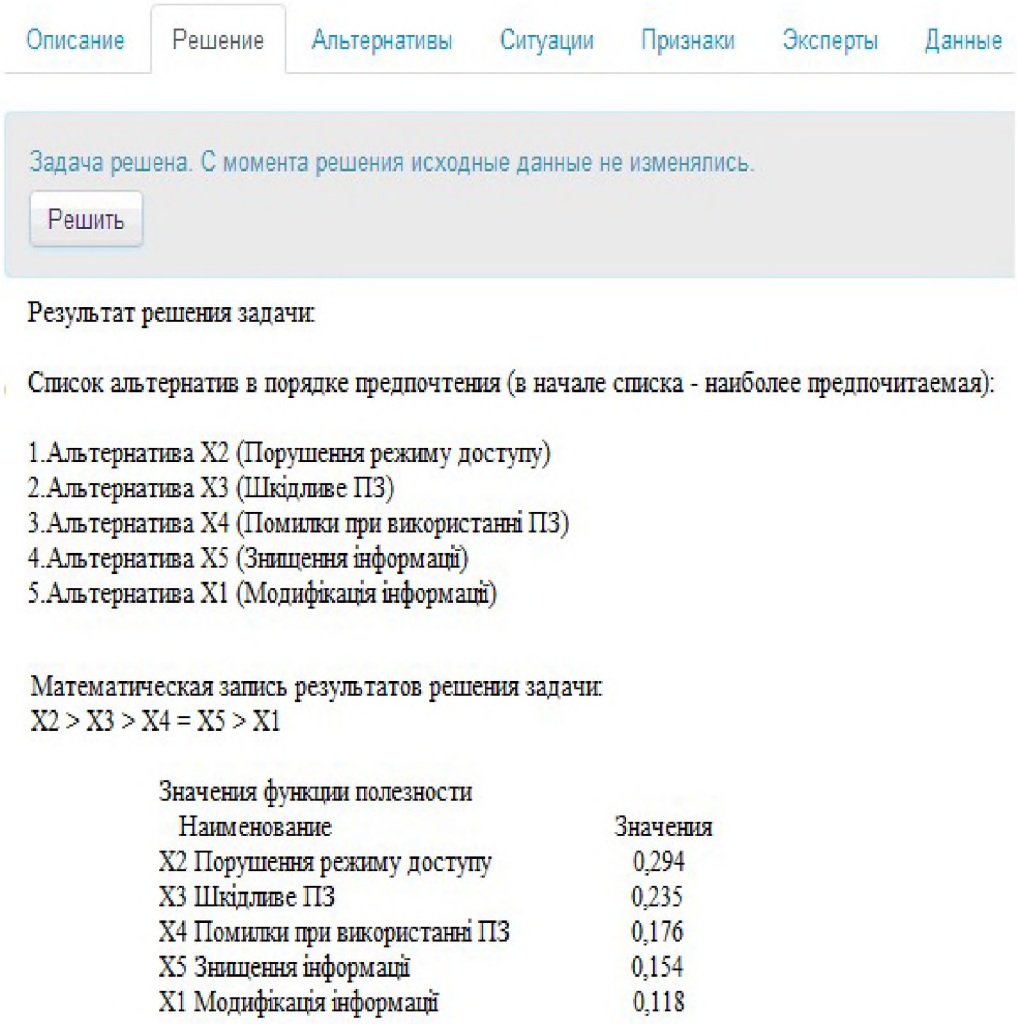

Рисунок 2.26 - Рішення завдання

Найбільш небезпечною є загроза порушення встановленого режиму доступу. На другому місці розташовується загроза шкідливе програмне забезпечення.

2.4.3 Порівняння результатів дослідження

В результаті оцінки альтернатив методам PURr, складемо зведену таблицю, що містить альтернативи і відповідні їм пріоритети, які були отримані в результаті вирішення задачі:

Таблиця 2.4 - Порівняння результатів дослідження

Альтернативи	Пріоритети	
	Метод аналітичних мереж	Метод Експертної системи
Модифікація інформації	0.172	0.118
Порушення встановленого режиму доступу	0.195	0.294
Шкідливе ПЗ	0.244	0.235
Знищення (руйнування) інформації	0.182	0.154
Помилки при використанні ПЗ	0.204	0.176

Метод показав схожі результати, однак ранжування відрізняється.

Метод Експертної СППР дозволяє враховувати не тільки взаємозв'язки ознак між собою і альтернатив, але ще і вплив різних ситуацій на прийняття рішення, враховуючи в той же час оцінки декількох експертів.

Фактично, вирішувати завдання вибору маючи вихідні дані з оцінками експертів не передбачає використання методу аналітичних мереж. Метод Експертної СППР повністю відповідає вимогам вирішення даної задачі. Тому, можна зробити висновок, що метод Експертної СППР , здійснює більш швидкий і простий спосіб вироблення безпосередньо рекомендацій ОПР для прийняття рішення, оскільки він лише здійснює розрахунки згідно з введеними даними і не вимагає перетворення їх у форму моделі вибору.

Після розгляду запровадження системи підтримки прийняття рішення в веб-інтерфейс і вирішення практичних завдань з використанням СППР, заснованих на методі аналітичних мереж і методі Експертної СППР, можна прийти до висновку, що «Експертна система підтримки прийняття рішень» є більш потужним інструментом у вирішенні задач вибору альтернатив. А враховуючи той факт, що за впровадженням такої системи у віддалене сховище слід неминуче скорочення витрат, робить її потенційно привабливим інструментів в питанні використання промислових масштабів.

2.5 Висновок

Важливо зазначити, що подальший розвиток систем підтримки прийняття рішень відбувається за принципом ускладнення інтелектуальних інформаційних технологій, здатних більш глибоко описувати проблемні ситуації з різних точок зору. Опис проблемної ситуації будується не тільки на самій виділеної ситуації, але й на індивідуальному сприйнятті її людиною. Іншими словами, проблемна ситуація описується в першу чергу зовнішніми і внутрішніми факторами, співвідношення між якими змінюється в залежності від зміни ситуації.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Завданням даної кваліфікаційної роботи є підвищення безпеки підприємства за рахунок впровадження розробленої системи підтримки прийняття рішень. У даному розділі були виконані наступні розрахунки:

1) розрахунок капітальних витрат;
2) розрахунок поточних витрат;
3) визначена величина можливого збитку;
4) визначені та проаналізовані показники економічної ефективності системи інформаційної безпеки.

На підставі отриманих результатів було зроблено висновок щодо економічної ефективності створення цього алгоритму.

3.1 Визначення трудомісткості розробки системи підтримки прийняття рішень

Трудомісткість створення системи підтримки прийняття рішень визначається тривалістю кожної робочої операції, починаючи зі складання технічного завдання і закінчуючи оформленням документації.

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ год.}$$

Де $t_{тз}$ = 10 год. – тривалість складання технічного завдання на розробку системи;

$t_{в}$ = 6 год. – тривалість вивчення технічного завдання, літературних джерел за темою тощо;

$t_{а}$ = 10 год. – тривалість розробки системи;

$t_{пр}$ = 6 год. – тривалість програмування за готовою системою;

$t_{опр}$ = 8 год. – тривалість опрацювання системи підтримки;

$t_{д}$ = 4 год. – тривалість підготовки технічної документації.

$$t = 10 \text{ год.} + 6 \text{ год.} + 10 \text{ год.} + 6 \text{ год.} + 8 \text{ год.} + 4 \text{ год.} = 44 \text{ год.}$$

3.2 Розрахунок витрат на створення системи підтримки

Витрати на створення системи підтримки прийняття рішень Крп складаються з витрат на заробітну плату виконавця розробки Ззп і вартості витрат машинного часу, що необхідний для опрацювання алгоритму на ПК Змч:

$$Крп = Ззп + Змч,$$

де Крп – витрати на створення системи підтримки;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для створення системи підтримки.

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) і визначається за формулою:

$$Ззп = t * Зіб = 44 * 125 = 5500 \text{ грн.}$$

де t – загальна тривалість розробки системи підтримки, год.;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 125 грн/год.

Вартість машинного часу для розробки алгоритму на ПК визначається за формулою:

$$Змч = t * Смч, \text{ грн.},$$

де t – трудомісткість розробки алгоритму на ПК, год.;

Смч – вартість 1 години машинного часу ПК, грн/год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р * tнал * Се + \frac{Фзал * На}{Fр} + \frac{Клпз * Напз}{Fр} =$$

$$= 0,4 * 2 * 2,64 + (7000 * 0,5)/1920 + (10000 * 0,5)/1920 =$$

$$= 2,11 + 1,82 + 2,6 = 6,53$$

де Р- встановлена потужність апаратури інформаційної безпеки, 0,4 кВт - середня потужність одного комп'ютера;

tнал – кількість машин на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 2,64 грн/кВт·год;

Фзал – залишкова вартість ПК на поточний рік, 7000 грн.;

На – річна норма амортизації на ПК, 0.5 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,5 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 10000 грн.;

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920 год.)

$$Змч = t * Смч = 44 * 6,53 = 287,32 \text{ грн.}$$

Визначена таким чином вартість створення системи підтримки Крп є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

$$Крп = Ззп + Змч = 5500 + 287,32 = 5787,32 \text{ грн.}$$

3.3 Розрахунок (фіксованих) капітальних витрат

Капітальні (фіксовані) витрати на проєктування та впровадження проєктного варіанта системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Каз + Кнавч. + Кн,$$

де Кпр – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, 15000 грн.;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 40000 грн.;

Крп – вартість розробки політики безпеки інформації, 5787,32 грн.;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів, 12000 грн.;

Кнавч - витрати на навчання технічних фахівців і обслуговуючого персоналу, 15000 грн.;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 27000 грн.

Відповідно до заданих даних розраховуємо капітальні витрати

$$К = Кпр + Кзпз + Крп + Каз + Кнавч. + Кн =$$
$$= 15000 + 40000 + 5787,32 + 12000 + 15000 + 27000 = 114787,32 \text{ грн.}$$

3.4 Розрахунок поточних (експлуатаційних) витрат

Поточні витрати включають:

- навчання персоналу в питаннях інформаційної безпеки;
- витрати на керування системою інформаційної безпеки.

1. Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки інформації та відповідно до неї розробляють інструкції для персоналу, що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 15000 грн. – витрати на навчання персоналу.

2. Обов'язки з керування системою інформаційної безпеки виконує керівник та адміністратор безпеки (за відсутності керівника), тому річний фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зк + Заб = 1500 + 1000 = 2500 \text{ грн. (в міс.)}$$
$$Сз = 2500 * 12 = 30000 \text{ грн. (рік),}$$

де Зк – додаткова заробітна плата керівника, 18000 грн. на рік.

Заб – додаткова заробітна плата адміністратора безпеки, 12000 грн. на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$Се = Р * Fp * Це,$$

де Р – встановлена потужність апаратури інформаційної безпеки (0,4 кВт*10 комп'ютерів = 4 кВт)

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 10 комп'ютерів = 19200 год. – річний фонд робочого часу системи інформаційної безпеки;

Це = 2,64 грн за 1 кВт/год. – тариф на електроенергію на 01.01.2023 року.

$$Се = 4 * 19200 * 2,64 = 202752 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$Стос = К * 0,02 = 114787,32 * 0,02 = 2295,75 \text{ грн.}$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = Со + Сз + Се + Стос =$$

$$= 15000 + 30000 + 202752 + 2295,75 = 250047,75 \text{ грн.}$$

3.5 Розрахунок оцінки величини збитку

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки (Пп).

Таблиця 3.1 Заробітні плати працівників за місяць

Посада	Розмір зар. плати	Кількість співробітників	Витрати на зар. плату на міс., грн
Директор	28000	1	28000
Заступник директора	24000	1	24000
Менеджер по роботі з клієнтам	20000	5	100000
Головний бухгалтер	25000	1	25000
Юрист	24000	1	24000
Системний адміністратор	25000	1	25000
		Сума	226000

Місячний фонд робочого часу складає 176 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 4 год.

$$Пп = (Зс/Fр) * tп = (226000/176) * 4 = 5136,36 \text{ грн.}$$

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн.;

Ппв – витрати на відновлення системи, грн.;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви = 6 год.:

$$Пви = (226000/176) * 6 = 7704,55 \text{ грн.}$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год. і розміром середньогодинної заробітної плати адміністратора безпеки:

$$Ппв = (25000/125) * 4 = 800 \text{ грн.}$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч = 7704,55 + 800 + 5000 = 13504,55 \text{ грн.},$$

Пзч = 5000 грн. - вартість для витрат на заміну частин;

О = 6500000 грн. - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = О/Fр * (tп + tв + tви) = 6500000/1920 * (4 + 4 + 6) = 3385,42 * 14 = 47395,88 \text{ грн.}$$

Fр – це річний фонд часу роботи офісу, 1920 годин;

tп – 4 годин простою після атаки;

tв – 4 годин відновлення після атаки;

tви – 6 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки на інформаційну систему при реалізації загрози складе:

$$U = Пп + Пв + V = 5136,36 + 13504,55 + 47395,88 = 66036,79 \text{ грн.}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum i \sum n * U = 10 * 4 * 66036,79 = 2641471,6 \text{ грн.},$$

де: і- число атакованих вузлів, 10 комп'ютерів;

n – середнє число атак на рік, 4 рази.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням В – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; С – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R – C = 2641471,6 * 0.25 - 250047,75 = 410320,15 \text{ грн.}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу наступних показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій То.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

$$ROSI = E/K = 410320,15 /114787,32 = 3,57$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$To = K/E = 1/ROSI = 1/3,57 = 0,28 \text{ року} = 3,6 \text{ місяця}.$$

3.6 Висновок

У даному розділі були проведені розрахунки витрат на проєкт системи захисту інформації. Також була визначена економічна ефективність розробки і впровадження системи підтримки прийняття рішень.

В результаті отримано наступні дані:

- капітальні витрати на впровадження інформаційної політики безпеки становлять 114787,32 грн.;
- експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 250047,75 грн.;
- загальний збиток від атаки на вузол складає 2641471,6 грн.;
- ефект від впровадження системи інформаційної безпеки становить 410320,15 грн.

Відповідно до розрахунків, виконаних в даному розділі, проєкт системи інформаційної безпеки є доцільним і економічно вигідним. Термін окупності капітальних інвестицій складає приблизно 3,5 місяці. Тому можна зробити висновок, що запропонована система є економічно ефективною та показує необхідність застосування на практиці.

ВИСНОВКИ

Важливо зазначити, що подальший розвиток систем підтримки прийняття рішень відбувається за принципом ускладнення інтелектуальних інформаційних технологій, здатних більш глибоко описувати проблемні ситуації з різних точок зору. Опис проблемної ситуації будується не тільки на самій виділеної ситуації, але й на індивідуальному сприйнятті її людиною.

Різноманітність програмних продуктів, спрямованих, в першу чергу, допомогти особі, що приймає рішення дозволяє максимально точно визначити необхідні технології і зробити вибір у відповідності з вимогами та потребами організації. Кілька десятків всіляких програмних продуктів реалізують різні методи та підходи до розв'язання задач вибору та підвищення ефективності процесу прийняття рішення, а постійне прагнення організацій до спрощення внутрішніх процесів рухає, в свою чергу, процесом освоєння систем все нових горизонтів інформаційних технологій. Говорячи про нові технології, у першу чергу, мова йде саме про хмарні обчислення. Майбутнє за хмарними обчисленнями. Вони - наступна гілка розвитку багатьох галузей діяльності інформаційних технологій, і рішення проблемних ситуацій за рахунок систем підтримки прийняття рішень є далеко не останнім завданням у цьому списку.

В кваліфікаційній роботі проведено аналіз специфіки комерційних підприємств, виконано аналіз нормативно-правової бази у сфері захисту інформації, виконана характеристика підприємства, категоріювання об’єктів, розроблена модель порушника та виконано постановку задачі.

У спеціальній частині визначено необхідність розробки системи підтримки прийняття рішень, надані методи і технології систем підтримки прийняття рішень, розглянуто практичне застосування різних технологій при вирішенні задачі вибору, виконано синтез методів підтримки прийняття рішень для вибору найбільш актуальної загрози інформації з моделі загроз для АСЗ на прикладі мережі будівельних гіпермаркетів.

Здійснено економічний розрахунок ефективності застосування система підтримки прийняття рішень Проведені розрахунки засвідчили позитивний економічний ефект.

ПЕРЕЛІК ПОСИЛАНЬ

1. Указ Президента України N 1431/2003 "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" від 31.10.2001;
2. Закон України № 2938-VI «Про інформацію», редакція від 03.07.2012;
3. Методи забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://pidruchniki.ws/15950210/politologiya/metodi_zabezpechennya_informatsiynoyi_bezpeki (Назва з екрана);
4. Закон України «Про власність» // Баланс. – 1995. – № 12. – С. 13;
5. Смолин Г.В. // Господарське право України. Особлива частина: Навчальний посібник. - Л. 2010 р.;
6. Закон України № 245-VII «Про захист персональних даних» від 16.05.2013;
7. ДСТУ ISO/IEC 27001:2010 «Інформаційні технології. Методи і засоби досягнення інформаційної безпеки. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2010, IDT)»;
8. В.Ф. Авраменко, Г.О. Брудний, С.І. Жлобін та ін. Правові основи охорони інформації; за ред. В.О. Хорошка. – К.: ТОВ «ПоліграфКонсалтінг», 2003. – 176;
9. Лазарєв Г.П., Кльоцкін С.М., Хорошко В.О. Шляхи вирішення проблем інформаційної безпеки в Україні // Захист інформації;
10. Дудикевич В.Б., Зачепило В.С., Хома В.В. Правові основи захисту інформації; Конспект лекцій. – Львів: Видавництво Національного університету «Львівська політехніка», 2002. – 168 с.;
11. «Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України» 03.03.2011 N 24-112/365;

12. ДСТУ ISO/IEC TR 13335-4:2005 «Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту (ISO/IEC TR 13335-4:2001, IDT)»;
13. ISM3 «Модель зрілості управління інформаційною безпекою»;
14. Комерційна діяльність торгового підприємства по продажу товарів І обслуговуванню покупців [Електронний ресурс]. – Режим доступу: http://uadocs.exdat.com/docs/index-33327.html?page=3 (Назва з екрана);
15. Комерційна діяльність : підручник / за ред. проф. В.В. Апопія. – К. : Вид-во "Знання", 2008. – 558 с.;
16. Характеристика доктрини інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://ms.znate.ru/docs/1651/index-18756.html?page=37#264119 - Назва з екрана;
17. Система збалансованих показників (BSC) [Електронний ресурс]. – Режим доступу: http://www.qm-s.com/it_consulting/balanced_scorecard_bsc/index.php - Назва з екрана;
18. НД ТЗІ 1.6-005-2013 № 215 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»;
19. НД ТЗІ 3.7-003-2005 № 125 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;
20. НД ТЗІ 1.4-001-2000 №53 «Типове положення про службу захисту інформації в автоматизованій системі»;
21. НД ТЗІ 1.1-003-99 №22 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»;
22. Закон України N 32-33 «Про захист інформації в інформаційно-телекомунікаційних системах» від 19.03.2009;

23. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»;
24. ДСТУ 3396.1-96 «Захист інформації Технічний захист інформації. Порядок проведення робіт»;
25. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»;
26. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»;
27. Основи економічної теорії / С.В. Мочерний, С.А Єрохін, Л.О. Канищенко та ін. – К.: – 463 с.;
28. Закон України № 221-VII «Про господарські товариства» від 18.04.2013;
29. Закон України № 1294-IV «Про підприємства в Україні» від 20.11.2003;
30. Податковий кодекс України № 5519-VI від 06.12.2012.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1	21	
6	А4	Розділ 2	43	
7	А4	Розділ 3	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	12	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	2	

ДОДАТОК Б. Акт обстеження ТОВ «Епіцентр К»

До складу штату співробітників входять:

- директор (1 чол.);
- заступник директора департаменту інформаційних технологій (1 чол.);
- секретар директора департаменту інформаційних технологій (1 чол.);
- секретар підприємства (1 чол.);
- фахівець суспільної приймальні (1 чол.);
- фахівець соціально-економічного відділу (3 чол.);
- фахівець рекламного відділу (4 чол.);
- фахівець відділу аналітики (3 чол.);
- фахівець організаційного відділу (3 чол.);
- фахівець торгового відділу (10 чол.);
- фахівець загального відділу (5 чол.);
- охоронець (4 чол.);
- прибиральниця (2 чол.).

Загальна кількість працівників: 39 чоловік.

У використанні організації знаходиться 22 комп'ютера:

- кабінет директора - 1 ПК;
- кабінет секретаря директора - 1 ПК;
- кабінет заступника директора департаменту інформаційних технологій - 1 ПК (сервер);
- організаційний відділ - 2 ПК;
- відділ аналітики - 3 ПК;
- відділ торгівлі - 4 ПК;
- соціально-економічний відділ - 3 ПК;
- загальний відділ - 3 ПК;

– суспільна приймальня - 1 ПК;

– рекламний відділ - 3 ПК.

В організації п'ятиденний режим роботи:

– робочий день з 8:00 - 17:00;

– перерва з 12:00 - 12:45;

– вихідний: субота, неділя.

Прибирання здійснюється щодня з понеділка по п'ятницю з 5:00 - 8:00.

Охорона об'єкта ведеться цілодобово. Два охоронці працюють з 08:00 - 17:00, ще двоє охоронців з 17:00 - 08:00.

ТОВ " Епіцентр К " займає двоповерхову будівлю.

На першому поверсі розташований хол, приймальня директора департаменту ІТ, його кабінет, кабінет заступника директора департаменту ІТ і секретаря, зал засідань, суспільна приймальня, кімната охорони і санвузол (рис.Д.1).

На другому поверсі розміщені такі відділи: торговий, аналітики, соціально-економічний, загальний, рекламний, організаційний відділ і санвузол (рис.Д.2).

Будівля розташована з півночі на 70 м від господарчого магазину, з півдня на 20 м від житлового будинку, зі сходу на 50 м від мінімаркету і з заходу на 100 м від середньоосвітньої школи.

В організації спроєктовані централізоване опалення і водопостачання, міська каналізація, автономне кондиціонування приміщень (у виді кондиціонерів) у кожній з кімнат. Встановлено стаціонарні телефони, що обслуговуються АТС №7, "УКРТЕЛЕКОМ".

Інтернет підключений до провайдера "Fregat".

Загальна площа кімнат регіонального офісу ТОВ "Епіцентр К ":

– хол - 39 м^2;

- кімната охорони - 26 м^2;
- приймальня директора департаменту ІТ - 19,5 м^2;
- кабінет директора департаменту ІТ - 32,5 м^2;
- кабінет секретаря підприємства -18 м^2;
- зал засідань - 27 м^2;
- суспільна приймальня - 36 м^2;
- соціально-економічний відділ - 32,5 м^2;
- рекламний відділ - 52 м^2;
- відділ аналітики - 32,5 м^2;
- організаційний відділ - 39 м^2;
- відділ торгівлі - 27 м^2;
- загальний відділ - 36 м^2.

Генеральний план

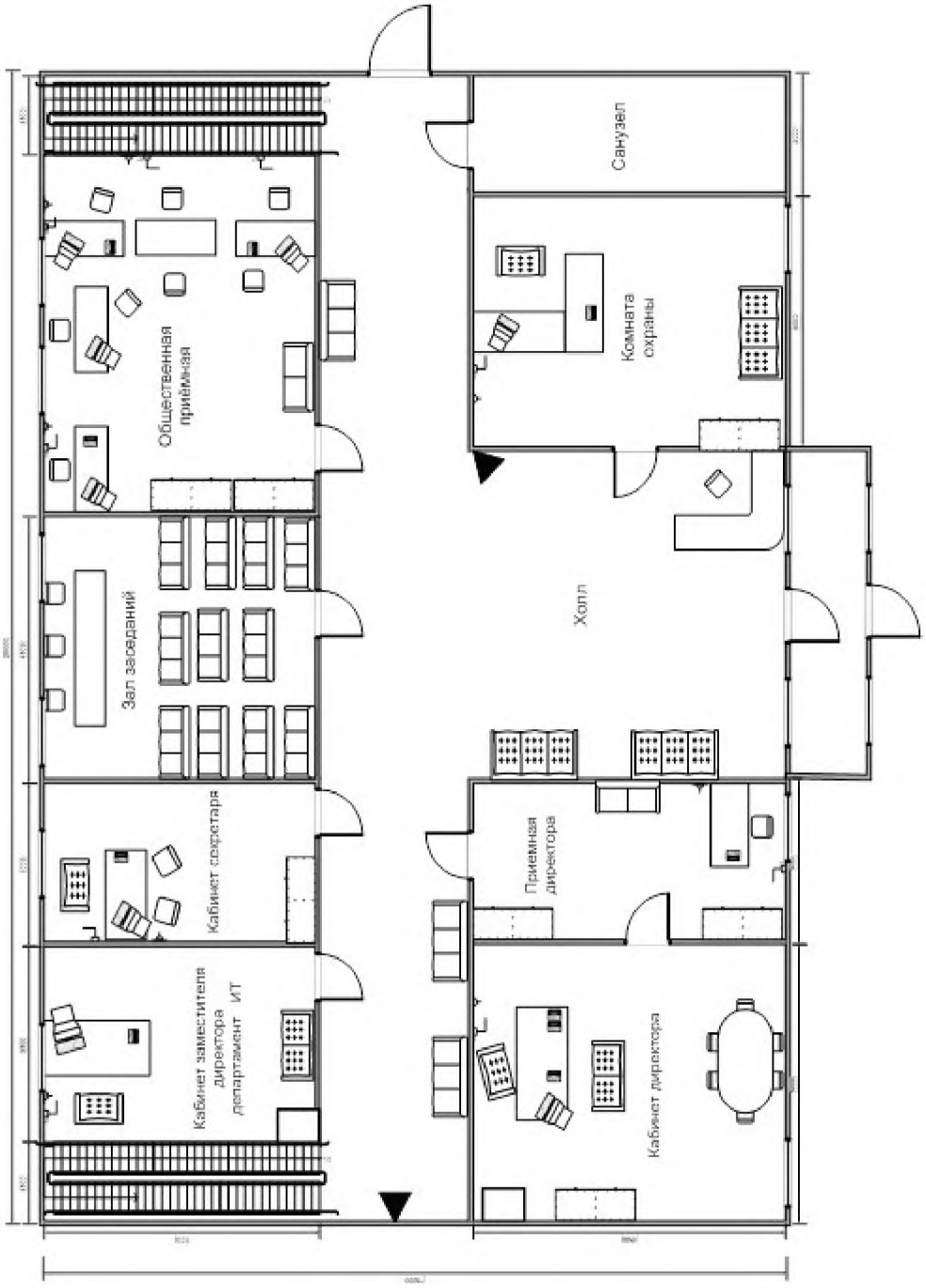

Рисунок Д.1 – Розташування кімнат на першому поверсі

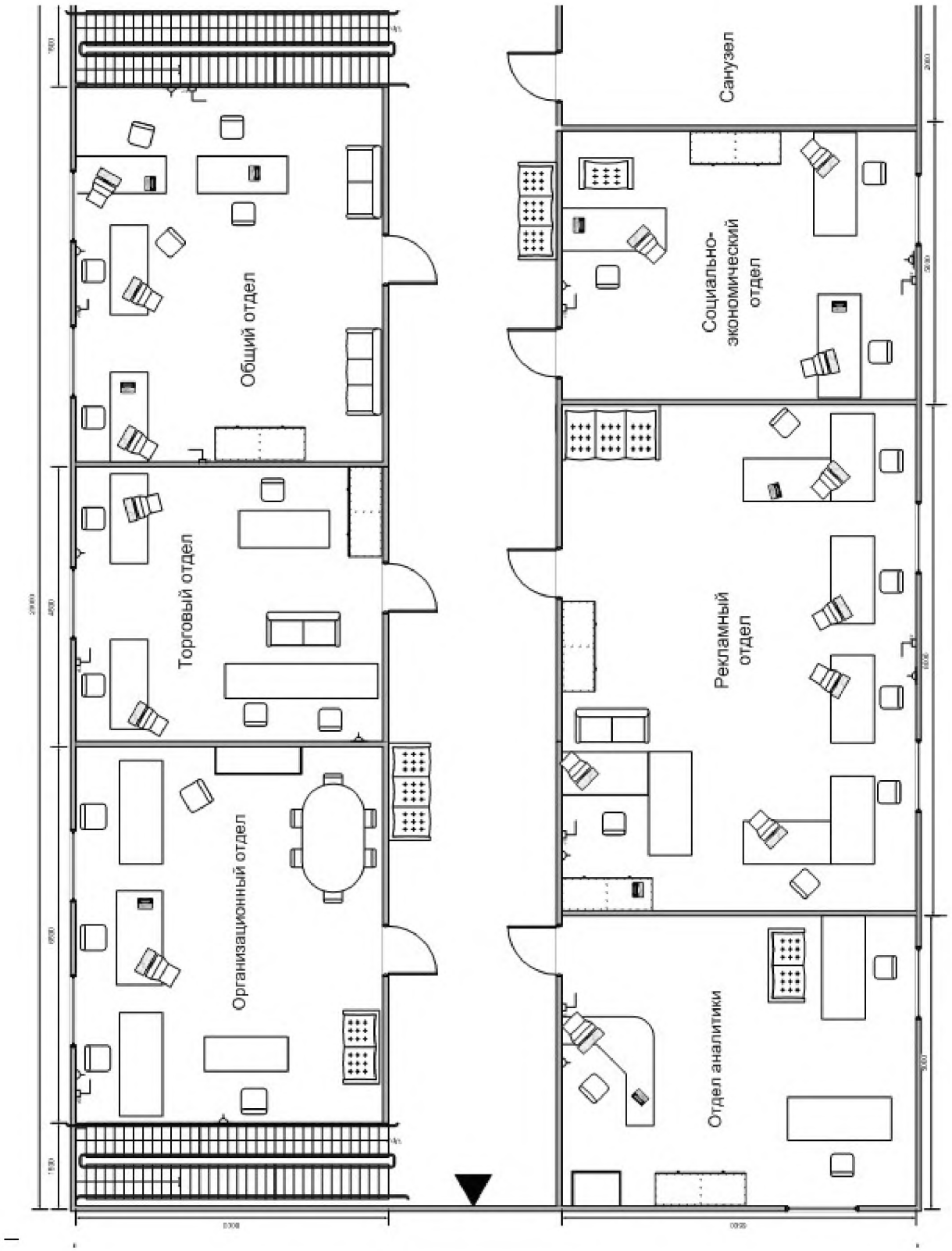

Рисунок Д.2 – Розташування кімнат на другому поверсі

Представимо загальну характеристику організації у виді таблиці Д.1.

Таблиця Д.1 - Загальна характеристика організації

№	Назва	Характеристика
1	Назва підприємства	ТОВ " Епіцентр К "
2	Форма власності	приватна
3	Наявність структурних підрозділів	без структурних підрозділів
4	Рід діяльності підприємства	продаж господарчих товарів в роздрібній мережі магазинів
5	Розміщення підприємства	2 поверхи, 13 кімнат, 3 коридори, 2 санвузли, 2 вхідні двері
6	Контрольована зона	обмежена стінами приміщень
7	Наявність розгалуженої ІС	немає
8	Персонал підприємства	директор (1 чол.), співробітники (32 чол.), охоронець (4 чол.), прибиральниця (2 чол.)
9	Персонал, відповідальний за роботу ІС	адміністратор ІБ
11	Тип циркулюючої інформації	конфіденційна інформація, відкрита
12	Види циркулюючої інформації	на паперовому та електронному носіях
15	Склад апаратних засобів ІС	1 ПК директора, 21 ПК співробітників, 1 концентратор.
16	Тип ОС	Microsoft Windows 11, на сервері - Windows Server 2019
17	Системне ПЗ	«Діловод», спеціалізоване бухгалтерське ПЗ, Pen Drive Data Recovery
18	Прикладне ПЗ	MS Office 2021, ESET NOD32 Smart Security

Класифікація інформаційних потоків підприємства

До загальнодоступної інформації підприємства відноситься:

– інформація про діяльність фірми: мета і характер діяльності; форма власності, правовий статус і форма господарювання, національна приналежність;

– інформація про товари: переліки наявних товарів на складах; переліки наявних товарів в магазині; перелік очікуваних товарів; технічні характеристики; інформація про виробника; тип оплати за товар; гарантійний термін;

– інформація про послуги: перелік послуг, що надаються; перелік вартості послуг; тип оплати за надані послуги; гарантія на послуги; терміни виконання послуги;

– інформація, що міститься в бухгалтерській звітності, яка надається в податкові служби та органи державної статистики.

До конфіденційної інформації підприємства відносяться всі види інформації з обмеженим доступом, що захищається законом:

– комерційна:

1) управління: відомості про перспективні методи управління виробництвом;

2) виробництво: організаційна структура підприємства; характер виробництва; організація роботи на підприємстві; відомості про виробничі можливості підприємства; характеристика виробництва;

3) плани розвитку підприємства; відомості про плани підприємства з розширення виробництва; інвестиційні програми, плани інвестицій; планово-аналітичні матеріали за поточний період; обсяг майбутніх закупівель за строками, асортиментом, цінами, країнами, фірмами; зведені

відомості про ефективність експорту або імпорту товарів в цілому по зовнішньо економічній діяльності;

4) фінанси: відомості, які розкривають планові і фактичні показники фінансового плану; майновий стан; вартість основних засобів та товарних запасів; бюджет; обороти; банківські операції; відомості про фінансові операції; банківські зв'язки; стан банківських рахунків підприємства; рівень виручки; рівень доходів; боргові зобов'язання; стан кредиту (активи і пасиви); розміри і умови банківських та інших кредитів; розміри, джерела кредитів та умови надання кредитів;

5) партнери: характеристика клієнтів; дані представників, посередників, дилерів і партнерів; дані про покупців і споживачів (оптових і роздрібних); дані про постачальників; негласні компаньйони товариств; комерційні зв'язки; місця закупівлі товарів; відомості щодо іноземних комерційних партнерів; характеристика підприємств - торгових партнерів (основні виробничі фонди, кредити, товарообіг); дані про клієнтів у торгівлі та рекламі;

6) контракти: умови за контрактами, угодами - як укладеними, так і плановаными (терміни, обсяги, номенклатура, умови поставки); особливі умови контрактів (знижки, доплати, розстрочка платежів, опціони); умови платежів за контрактами (ціни, знижки, доплати, розстрочка платежів, опціони); особливі угоди і умови компенсаційних угод; відомості про виконання контрактів; відомості про номенклатуру і кількість товарів за взаємними зобов'язаннями, передбаченими угодами, протоколами, а також про товарообіг; відомості про авторські договори;

7) ціни: відомості про методики розрахунків цін і принципи ціноутворення; структура цін; калькуляція витрат виробництва; дані для калькуляції ціни;

8) оплата праці: умови укладання контрактів між адміністрацією підприємства і працівниками; відомості про оплату праці, преміальні, доплати і компенсації.

– Службова (відомості організаційного і технічного характеру, які стосуються стратегії продажу, організації праці): реквізити постачальників; перелік несправностей; довідники по ремонту та налагодженню обладнання.

– Особиста (персональні дані - відомості про факти, події і обставини життя працівника, що дозволяють ідентифікувати його особу): особистий телефонний номер, місце проживання, місце прописки; серія та номер паспорта, ідентифікаційний номер; відомості про зарплату і премії; персональні дані автобіографії, що дозволяють ідентифікувати його особу.

Класифікація інформаційної системи і її елементів

1 По доступності чи наявності:

Д5 - критична інформація (робота суб'єкта буде зупинена);

Д4 - дуже важлива інформація (суб'єкт буде працювати, але короткий час);

Д3 - важлива інформація (суб'єкт може працювати без цієї інформації якийсь час, але вона незабаром знадобиться);

Д2 - корисна інформація (без інформації можна працювати, але її використання заощаджує час);

Д1 - несуттєва інформація (застаріла чи невикористовувана, що не впливає на роботу суб'єктів інформація);

Д0 - шкідлива інформація (наявність такої інформації вимагає обробки, а обробка веде до перевитрат ресурсів).

2 По несанкціонованій модифікації чи цілісності:

Ц4 - критична інформація (несанкціонована зміна приведе до неправильної роботи всього підприємства чи значної його частини; наслідки такої модифікації необоротні);

ЦЗ - дуже важлива інформація (несанкціонована зміна приводить до невірної роботи підприємства чи його частини через якийсь час, якщо не будуть початі деякі дії; наслідки такої модифікації необоротні);

Ц2 - важлива інформація (несанкціонована зміна приводить до неправильної роботи підприємства через якийсь час, якщо не будуть початі деякі дії; наслідки такої модифікації оборотні);

Ц1 - значима інформація (несанкціонована зміна позначиться через якийсь час, але не приведе до збою в системі; наслідки такої модифікації оборотні);

Ц0 - незначуща інформація (несанкціонована зміна не позначиться на роботі системи).

3 По розголошенню чи конфіденційності:

ДО5 - критична інформація (розголошення інформації приведе до краху підприємства чи дуже значним матеріальним втратам);

ДО4 - дуже важлива інформація (розголошення приведе до значних матеріальних втрат, якщо не будуть прийняті які-небудь міри);

ДО3 - важлива інформація (розголошення приведе до деяких матеріальних чи моральних втрат, якщо не будуть початі деякі дії);

ДО2 - значима інформація (приносить моральний збиток, може бути використана у визначений момент);

ДО1 - малозначима інформація (може принести моральний збиток у дуже рідких випадках);

ДО0 - незначуща інформація (не впливає на роботу суб'єкта).

Згідно приведеним позначенням, розглянемо класифікацію інформаційних об'єктів у таблиці Д.2.

Таблиця Д.2 - Класифікація інформаційних об'єктів

№	Найменування	За доступністю	За цілісністю	За конфіденційністю
1	Бухгалтерська інформація (податкові накладні, бухгалтерські звіти, інформація про платежі)	Д4	Ц3	К4
2	Інформація про клієнтів	Д2	Ц1	К3
3	Інформація про співробітників	Д1	Ц1	К2
4	Інформація, отримана з клієнтських ПК	Д2	Ц1	К3
5	Договори й листи замовлень	Д3	Ц2	К3
6	Інформація про плани підприємства	Д3	Ц1	К3

Інформаційна система представлена на рис. Д.3:

РС1 - директора;

РС2 - секретаря директора;

РС3-РС4 - організаційний відділ;

РС5-РС7 - відділ аналітики;

S1 (Сервер) - заступника директора, департамент інформаційних технологій;

PC8-PC11 - відділ торгівлі;

PC12-PC14 - соціально-економічний відділ;

PC15-PC17 - загальний відділ;

PC18 - суспільна приймальня;

PC19-PC21 - рекламний відділ.

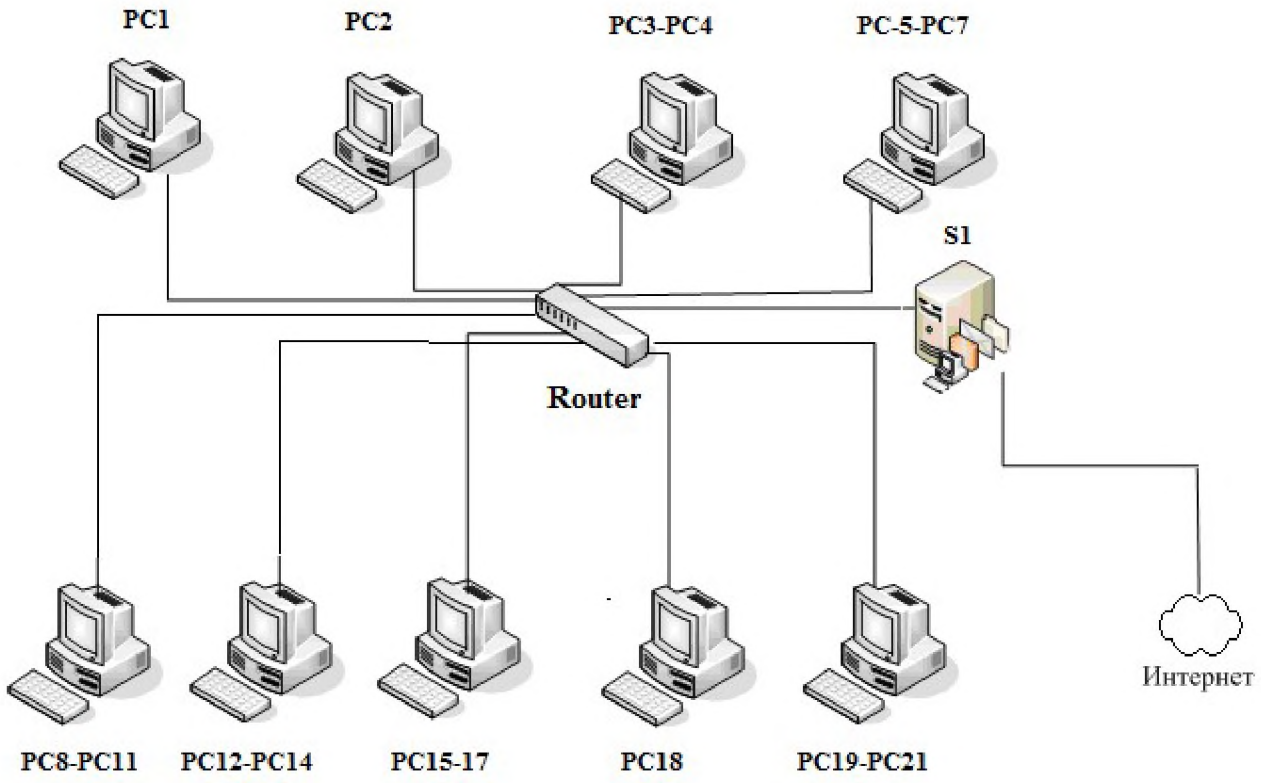

Рисунок Д.3 – Інформаційна система

ДОДАТОК В. Перелік документів на оптичному носії

1 Презентація_Ковальчук.ppt

2 Кваліфікаційна робота_Ковальчук.doc

ДОДАТОК Г. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Ґ. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-2 Ковальчука Д.В. на тему: «Синтез системи підтримки прийняття рішень для оцінки інформаційних загроз в ІКС гіпермаркету»

Пояснювальна записка містить 104 сторінки, 27 рис., 7 табл., 5 додатків, 30 джерел.

Метою даної кваліфікаційної роботи є підвищення ефективності роботи систем підтримки прийняття рішень шляхом впровадження сучасних інформаційних технологій на комерційних підприємствах.

У спеціальній частині визначено необхідність розробки системи підтримки прийняття рішень, подано методи і технології систем підтримки прийняття рішень, розглянуто практичне застосування різних технологій при вирішенні задачі вибору, виконано синтез методів підтримки прийняття рішень для вибору найбільш актуальної загрози інформації з моделі загроз для АС3 на прикладі мережі будівельних гіпермаркетів.

В економічному розділі виконано розрахунок економічного ефекту від впровадження системи в регіональний офіс комерційного підприємства.

Наукова новизна очікуваних результатів полягає у використанні інформаційних технологій, методів прийняття рішень і можливого застосування системи підтримки прийняття рішень на практиці у комерційних підприємствах.

Передбачувана практична цінність полягає в розробці рекомендацій для синтез-системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 3.

Запропонована в роботі рекомендації синтезу систем підтримки прийняття рішень для підвищення рівню захищеності об’єкту інформаційної

діяльності впроваджені у робочий процес підприємства.

До недоліків проєкту слід віднести помилки у виборі методів оцінки ефективності, частковий аналіз загроз інформації для автоматизованої системи класу 3 та окремі невідповідності вимогам при оформленні, а також нечіткість деяких формулювань та визначень.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Ковальчук Д.В. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.ф.-м.н., проф. **Гусєв О.Ю.**