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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студента *Дунаєва Яна Олексійовича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Система підтримки прийняття рішень для моделювання загроз інформаційній безпеці в автоматизованій системі класу 2*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Ковальова Ю.В.			
розділів:				
спеціальний	к.т.н., доц. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Дунаєву Яну Олексійовичу* **академічної групи** *125м-21-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Система підтримки прийняття рішень для моделювання загроз інформаційній безпеці в автоматизованій системі класу 2***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.22р. № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Синтез системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2, що дозволяє підвищити ефективність інформаційної безпеки автоматизованої системи класу 2.	20.10.2022
Розділ 2	Розглянути основні принципи і технології функціонування системи підтримки прийняття рішень, розглянути моделі систем підтримки прийняття рішень, уразливість основних елементів АС та класифікація загроз безпеки.	16.11.2022
Розділ 3	Виконати розрахунок вартості заходів щодо впровадження системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2.	05.12.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 05.09.2022 р.

Дата подання до екзаменаційної комісії: 12.12.2022 р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 95 с., 8 рис., 4 табл., 4 додатка, 26 джерел.

Мета роботи: синтез системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2, що дозволяє підвищити ефективність інформаційної безпеки автоматизованої системи класу 2.

Об'єкт дослідження: автоматизована система класу 2.

Предмет дослідження: синтез системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2.

У спеціальній частині розглянуто основні принципи і технології функціонування системи підтримки прийняття рішень, розглянуті моделі систем підтримки прийняття рішень, уразливість основних елементів АС та класифікація загроз безпеки.

В економічному розділі виконано розрахунок вартості заходів щодо впровадження системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2.

Новизна роботи полягає в розробці системи підтримки прийняття рішень, яка дозволить зробити початкову оцінку систем захисту автоматизованої системи класу 2 і побудує модель загроз для даної автоматизованої системи.

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, АВТОМАТИЗОВАНА СИСТЕМА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛІ СППР, ФОРМУВАННЯ МОДЕЛІ ЗАГРОЗ, УРАЗЛИВІСТЬ ЕЛЕМЕНТІВ АС.

ABSTRACT

Explanatory note: 95 p., 8 pic., 4 tabl., 4 app., 26 sources.

Purpose: synthesis of decision support system for modeling information threats for automated system of class 2, which allows to increase the efficiency of information security of automated system of class 2.

Object of research: automated system of class 2.

Subject of research: synthesis of decision support system for modeling information threats for automated system of class 2.

The special part considers the basic principles and technologies of the decision support system, models of decision support systems, the vulnerability of the main elements of the AS and the classification of security threats.

In the economic section, the cost of measures to implement a decision support system for modeling information threats for an automated system of class 2 is calculated.

The novelty of the work is the development of a decision support system that will allow to make an initial assessment of the protection systems of the automated system of class 2 and build a threat model for this automated system.

DECISION SUPPORT SYSTEM, AUTOMATED SYSTEM, THREAT MODEL, DSS MODEL, THREAT MODEL FORMATION, VULNERABILITY of AS ELEMENTS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АСППР – автоматизована система підтримки прийняття рішень;

АС – автоматизована система;

ЕОМ – електронна обчислювальна машина;

ІСПДн – інформаційна система персональних даних;

КЗСІ – комплексна система захисту інформації;

ОПР – особа, що приймає рішення;

ПЗ – програмне забезпечення;

ПДн – персональні дані;

ПЕВМ – персональна електронна обчислювальна машина;

СУБД – системи управління базою даних;

СУІБ – системи управління інформаційною безпекою.

СППР – система підтримки прийняття рішень;

СКБД – система керування базами даних;

ТЗ – технічне завдання;

DSS – (decision support system) комп'ютерна автоматизована система;

OLAP – online analytical processing аналітична обробка в реальному часі;

ІСК – інформаційна система керівництва;

ISO – (international organization for standardization) міжнародна організація стандартизації.

ЗМІСТ

ВСТУП

Забезпечення інформаційної безпеки є важливим завданням для будь якої організації, оскільки від збереження конфіденційності, цілісності та доступності інформаційних ресурсів багато в чому залежать якість і оперативність прийняття технічних рішень, ефективність їх реалізації.

Держава, регламентуючи відносини в інформаційній сфері не здатне впоратися у повному обсязі з завданням забезпечення безпеки всіх суб'єктів інформаційних відносин, однозначно відповідаючи лише за захист відомостей, що становлять державну таємницю. Тому в умовах різних форм власності задача забезпечення інформаційної безпеки повністю лягає на плечі підприємців, керівників організацій, різних комерційних структур. За підрахунками американських фахівців, втрата 20% інформації веде до розорення організації протягом місяця в 60 випадках зі 100. Інформація є основою для прийняття рішень людиною і від її достовірності, повноти, системної організованості залежить ризик прийняття неефективних і небезпечних рішень. Ненавмисне або навмисне спотворення інформації, несанкціонований доступ до інформації, що захищається може становити значну загрозу.

Проте інформаційна безпека – це виключно комплексний процес, що вимагає участі всіх співробітників підприємства, тимчасових і постійних, а також третіх осіб, постачальників, контрагентів, партнерів задля надійного використання інформаційних технологій, обслуговування обладнання і каналів зв'язку, створення документації бізнес-процесів - тобто організації ефективної системи управління інформаційної безпеки.

Різноманітність і постійна зміна загроз ускладнює управління ними, при цьому вірогідність їх реалізації не зменшується. Процес управління ризиками забезпечує постійний аналіз, оцінку та обробку ризиків, який є необхідним інструментом на кожному підприємстві. Проте досягнення високої ефективності процесу управління ризиками вимагає наявності

висококваліфікованих спеціалістів в даній галузі та можливості аналізувати великої кількості несистематизованої інформації.

Розв'язанням проблеми ефективного управління ризиками інформаційної безпеки є використання систем підтримки прийняття рішень, котрі сьогодні дозволяють застосовувати передові технології обробки та збереження інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Поняття та аналіз систем підтримки прийняття рішень

Останнім часом проблеми прийняття рішень заслуговують все більшої уваги, так як динаміка навколишнього середовища стрімко зростає разом з науково-технічним прогресом. Керівники, приймаючи рішення, стикаються зі складним вибором, з необхідністю розгляду множини альтернативних варіантів. Для оцінювання варіантів використовують знання фахівців, складні аналітичні розрахунки, наукові дослідження, засоби сучасних інформаційних технологій.

Питання підтримки рішень на всіх стадіях цього процесу стають все актуальнішими. Проблема полягає в автоматизації творчої частини праці відповідальної групи працівників організаційного управління - керівників усіх рангів і осіб, які приймають рішення, за реальних умов їхньої діяльності.

Проблеми прийняття рішень в організаційному управлінні переважно унікальні й нестандартні, але вони у своїй ситуаційній основі мають такі загальні риси:

- складний для оцінювання характер альтернатив, що розглядаються;
- наявність сукупності різнорідних факторів, які необхідно враховувати під час прийняття рішень;
- неповторність ситуації вибору;
- недостатня визначеність наслідків дій (невизначеність після дій);
- наявність особи або групи осіб, які несуть відповідальність за прийняття рішень.

Системи підтримки прийняття рішень (далі - СППР) виникли завдяки розвитку управлінських інформаційних систем і являють собою системи, розроблені для підтримки процесів прийняття рішень менеджерами за складних слабо структурованих умов. На розвиток СППР істотний вплив справили вражаючі досягнення в галузі інформаційних технологій, зокрема,

поява телекомунікаційних мереж, персональних комп'ютерів, динамічних електронних таблиць, експертних систем, Інтернету тощо.

Термін СППР (DSS-Decision Support System) виник у 70-х роках і належить Горрі та Мортону [1]. Досі немає єдиного визначення СППР. Наприклад, деякі автори під СППР розуміють «інтерактивну прикладну систему, яка забезпечує кінцевим користувачам, котрі приймають рішення, легкий і зручний доступ до даних і моделей з метою прийняття рішень у напівструктурованих і неструктурованих ситуаціях з різних галузей людської діяльності».

Відомі й інші означення, зокрема: «СППР – комп'ютерна інформаційна система, яка використовувався для підтримки різних видів діяльності під час прийняття рішень у ситуаціях, де неможливо або небажано мати автоматичну систему, яка повністю виконує весь процес створення рішень».

Також існує твердження, згідно з яким СППР – специфічний і добре описуваний тип систем на базі персональних комп'ютерів. Таке розмаїття означень систем підтримки прийняття рішень спричинене існуючим широким діапазоном різних форм, розмірів і типів СППР.

Системи підтримки прийняття рішень націлені на неструктуровані і напівструктуровані проблеми. Розробляючи специфічні, нетипові рішення за допомогою СППР, менеджери самостійно, індивідуально, автономно та незалежно формують інформацію в інтерактивному режимі. Для планування і контролювання на тактичному і стратегічному рівнях менеджерам потрібна додаткова, унікальна, і, найчастіше, разова, тобто отримана для окремого випадку інформація.

Порівняння технологій формування інформації в традиційній звітній ІС і в СППР розкриває головну особливість СППР. Регламентовані звіти, які менеджери отримують від інформаційної системи готовими, сформовані на основі чітко визначеної технології, описаної в проєктній документації інформаційної системи і контрольованої її інженерно-технічним персоналом. Формування інформації засобами СППР також передбачає певну технологію

використання наявних ресурсів (програмного забезпечення, бази моделей даних, телекомунікацій).

Однак цю технологію повинен визначити й організувати сам менеджер. Іншими словами, у СППР із першим питанням менеджера «Яка інформація необхідна?» нерозривно зв'язане друге: «Як, яким чином її одержати?», оскільки саме він за своїм задумом повинен сформувати додаткову унікальну інформацію.

Менеджер, наприклад, може добре знати теоретичну сутність математико-статистичного моделювання зв'язків чи математичну сутність оптимізації, однак для швидкого практичного застосування цих знань йому необхідно правильно задіяти конкретні програмні засоби. Тому найважливішою метою СППР є в першу чергу забезпечення технологією формування інформації а також технологічна підтримка прийняття рішення в цілому.

Технологія підтримки рішення, на відміну від технології формування традиційного звіту, не виконується цілком автоматично, оскільки вона здійснюється під управлінням менеджера.

СППР орієнтовані не на процес, а на набір альтернатив та варіантів, що інтерактивно обираються менеджером. Таким чином, СППР повинна надавати кінцевому користувачу не підтримку однозначно описаного процесу обробки даних, а набір можливостей, що не залежать від процесу. Така творча робота із СППР потребує від менеджера глибоких знань своєї ділової сфери, високого інтелекту, професійного оволодіння набором технологічних можливостей комп'ютерної підтримки рішень, адже завдання,

які потребують прийняття рішень, що підтримуються СППР, є дуже складними з двох причин: або мета, або засоби її досягнення незрозумілі. СППР не продукує рішення, а скоріше забезпечує інформацією, яка використовується користувачем разом з іншими відомостями, щоб прийняти рішення.

У теорії СППР на сьогодні виділяють три покоління розвитку систем [3]:

- перше покоління – з 1970 до 1980 р.,
- друге – з 1980 р. до середини 90-х років,
- третє – з середини 90-х років XX ст. і донині (розроблення нових типів триває).

СППР першого покоління мають такі основні характеристики:

- управління даними – велика кількість інформації, банки даних;
- управління обчисленнями – моделі розроблялися фахівцями в галузі інформатики для спеціальних проблем;
- користувацький інтерфейс – мови програмування для великих ЕОМ, що використовуються тільки програмістами.

СППР другого покоління мають нові властивості:

- управління даними – необхідна і достатня кількість інформації відповідно до сприйняття ОПР;
- управління обчисленнями – гнучкі моделі, що відповідають способові мислення ОПР;
- інтерфейс користувача – дружній користувачеві, безпосередня робота кінцевого користувача.

СППР третього покоління мають ті самі ознаки, що й другого покоління, але з'явилися додаткові можливості за рахунок упровадження таких нових засобів інформаційних технологій і методів штучного інтелекту:

а) сховищ і вітрин даних, що дає змогу творцям рішень аналізувати величезні обсяги даних про поточні ділові транзакції з метою вибору раціонального рішення;

б) OLAP-систем, які уможливлюють швидке та зручне маніпулювання великими базами даних для дослідження багатьох показників бізнесової діяльності в різних ракурсах.

1.1.1 Класифікація існуючих систем підтримки прийняття рішень

На сьогодні не існує єдиної загальної класифікації СППР. На рівні користувача виділяють такі види СППР [4]:

- активна – може зробити пропозицію, яке рішення варто вибрати;
- пасивна – допомагає у процесі ухвалення рішення, але не може внести пропозицію, яке рішення прийняти;
- кооперативна – дозволяє особам, що приймають рішення змінювати, поповнювати або поліпшувати рішення, пропоновані системою, посилаючи потім ці зміни в систему для перевірки.

На технічному рівні розрізняють такі СППР:

- СППР рівня підприємства – підключена до великих сховищ даних і обслуговує багатьох менеджерів підприємства;
- персональна настільна СППР – мала система, що обслуговує лише один комп'ютер користувача.

На концептуальному рівні відрізняють такі типи СППР:

- керована повідомленнями (Communication-Driven DSS) – підтримує групу користувачів, що працюють над виконанням загальної задачі;
- керована даними (Data-Driven DSS, Data-oriented DSS) – в основному орієнтується на доступ і маніпуляції з даними;
- керована документами (Document-Driven DSS) – здійснює пошук і маніпулювання неструктурованою інформацією, заданої в різних форматах;
- керована знаннями (Knowledge-Driven DSS) – забезпечує рішення задач у виді фактів, правил, процедур;
- керована моделями (Model-Driven DSS) – забезпечує доступ і маніпуляції з математичними моделями (статистичними, фінансовими, оптимізаційними, імітаційними).

Залежно від рівня вирішуваних задач, від масштабу наочної області виділяють три класи СППР.

СППР першого класу мають найбільші функціональні можливості і призначені для застосування в органах державного управління вищого рівня (наприклад, міністерства) і органах управління великих компаній при плануванні масштабних комплексних цільових програм для обґрунтовування рішень щодо включення в програму різних політичних, соціальних або

економічних заходів і розподілу між ними ресурсів на основі оцінки їх впливу на досягнення основної мети програми. СППР цього класу є системами колективного користування, бази знань яких формуються багатьма експертами – фахівцями в різних областях знань.

СППР другого класу є системами індивідуального користування, бази знань яких формуються самим користувачем. Вони призначені для використання державними службовцями середнього рангу, а також керівниками малих і середніх фірм для вирішення оперативних задач управління.

СППР третього класу є системами індивідуального користування, що адаптуються до досвіду користувача. Вони призначені для вирішення прикладних задач системного аналізу та управління, що часто зустрічаються (наприклад, вибір суб'єкта кредитування, вибір виконавця роботи, призначення на посаду та ін.). Такі системи забезпечують отримання рішення поточної задачі на основі інформації про результати практичного використання рішень цієї ж задачі, прийнятих у минулому.

Кінцеві користувачі СППР за характером діяльності можуть бути об'єднані в три основні категорії:

1) аналітики, які повинні володіти не тільки методами дослідження предметної області, але й мати уявлення про сховище даних, а також володіти інструментами розробки спеціалізованих додатків;

2) середня ланка керівних працівників, які використовують дані для підготовки рішень на рівні свого підрозділу. Ця категорія рідко використовує деталізовані дані, зосереджуючись на слабко та дуже агрегованих даних. Інструментами їх роботи є стандартні звіти, налаштовані на інтерактивний режим роботи зі спеціалізованими додатками;

3) вищий ешелон керівництва, котрий використовує агреговані дані з основних показників, спеціалізовані додатки у вигляді інтерактивних звітів, які відображають діяльність організації загалом для прийняття стратегічних рішень.

В залежності від типів даних, з якими ці системи працюють, СППР умовно можна розділити на:

- оперативні;
- стратегічні.

Оперативні СППР призначені для негайного реагування на зміни поточної ситуації в керуванні фінансово-господарськими процесами компанії, об'єднання, галузі чи держави. Такі СППР називають «Виконавчі Інформаційні Системи» (Executive Information Systems). За суттю, вони представляють собою кінцеві множини звітів, побудовані на підставі даних із транзакційної інформаційної системи оперативного обліку підприємства. Вони забезпечують адекватне відображення в режимі реального часу основних аспектів виробничої і фінансової діяльності підприємства. Для таких СППР характерні такі риси:

- звіти ґрунтуються на стандартних для організації запитах, кількість яких відносно невелика;
- СППР представляє звіти в максимально зручному виді, що включає поряд з таблицями ділову графіку, мультимедійні можливості і т. п.;
- СППР зазвичай орієнтовані на конкретну сферу, наприклад, фінанси, маркетинг, керування ресурсами.

Стратегічні СППР орієнтовані на аналіз значних обсягів різнорідної інформації, що збираються з різних джерел. Найважливішою метою цих СППР є пошук найбільш раціональних варіантів розвитку бізнесу компанії із урахуванням впливу різних факторів, таких як кон'юнктура цільових для компанії ринків, зміни фінансових ринків і ринків капіталів, зміни у законодавстві і т. ін.

Такі СППР припускають достатньо глибоке перетворення даних, спеціально перетворених таким чином, щоб їх було зручно використовувати у процесі прийняття рішень. Невід'ємним компонентом СППР цього виду є правила прийняття рішень, які на основі агрегованих даних дають можливість менеджерам компанії обґрунтовувати свої рішення, використовувати фактори

стійкого росту бізнесу компанії і комп'ютерні системи підтримки прийняття рішень знижувати ризики. Стратегічні СППР будуються на принципах багатовимірного представлення та аналізу даних (OLAP).

Для сучасних СППР характерна наявність характеристик, наведених нижче [5].

1 СППР допомагає керівнику у процесі прийняття рішень і забезпечує підтримку у всьому діапазоні контекстів задач. Думка людини та інформація, що генерується ЕОМ, являють єдине ціле для прийняття рішень.

2 СППР підтримує і посилює (але не змінює і не відміняє) міркування та оцінку керівника. Контроль залишається за людиною, при цьому користувачу комфортно працювати в системі.

3 СППР підвищує ефективність прийняття рішень. На відміну від адміністративних систем, де робиться акцент на аналітичному процесі, у СППР пріорітетом є ефективність процесу прийняття рішень.

4 СППР виконує інтеграцію моделей і аналітичних методів із стандартним доступом до даних і вибіркою з них. Для надання помочі при прийнятті рішень активується одна або декілька моделей. Вміст БД охоплює історію поточних і попередніх операцій, а також інформацію зовнішнього характеру та інформацію про середовище.

5 СППР проста в роботі для осіб, що мають досвід роботи з ЕОМ, при цьому не потребують глибоких знань про обчислювальну техніку і забезпечують просте керування системою.

6 СППР побудовані за принципом інтерактивного рішення задач. Користувач має можливість підтримувати діалог із СППР у безперервному режимі.

7 СППР орієнтована на гнучкість і адаптивність для пристосування до змін середовища або підходів до рішення задач, що обирає користувач. Керівник повинен пристосуватися до змінюваних умов сам і відповідно підготувати систему.

8 СППР не нав'язує користувачу визначеного процесу прийняття рішень.

1.1.2 Базові компоненти СППР

Незважаючи на те, що сьогодні існує велика кількість різних видів СППР, всі вони характеризуються однотипною структурою, яка включає основні базові підсистеми як вказано на рисунку 1.1 [3]:

1) інтерфейс користувача, основною функцією якого є забезпечення можливості ОПР проводити діалог із системою, використовуючи різні способи введення інформації і формати її виведення;

2) підсистему роботи з даними, головна функція якої – збереження, управління, вибірка, відображення, аналіз даних;

3) підсистему роботи з моделями, призначенням якої є збереження, управління та вибір моделей для забезпечення користувача відповідями на безліч його запитів;

4) базу знань.

Поняття “інтерфейс користувача” означає комплекс програмних засобів, які реалізують діалог користувача з системою на стадії введення інформації та при одержанні результатів.

Користувач сприймає систему (в тому числі СППР) через її інтерфейс. Фактично він ототожнює систему з її інтерфейсом. Незалежно від того, наскільки добре реалізовані інші компоненти СППР, без відповідного інтерфейсу користувача система не зможе повною мірою забезпечувати підтримку прийняття рішення.

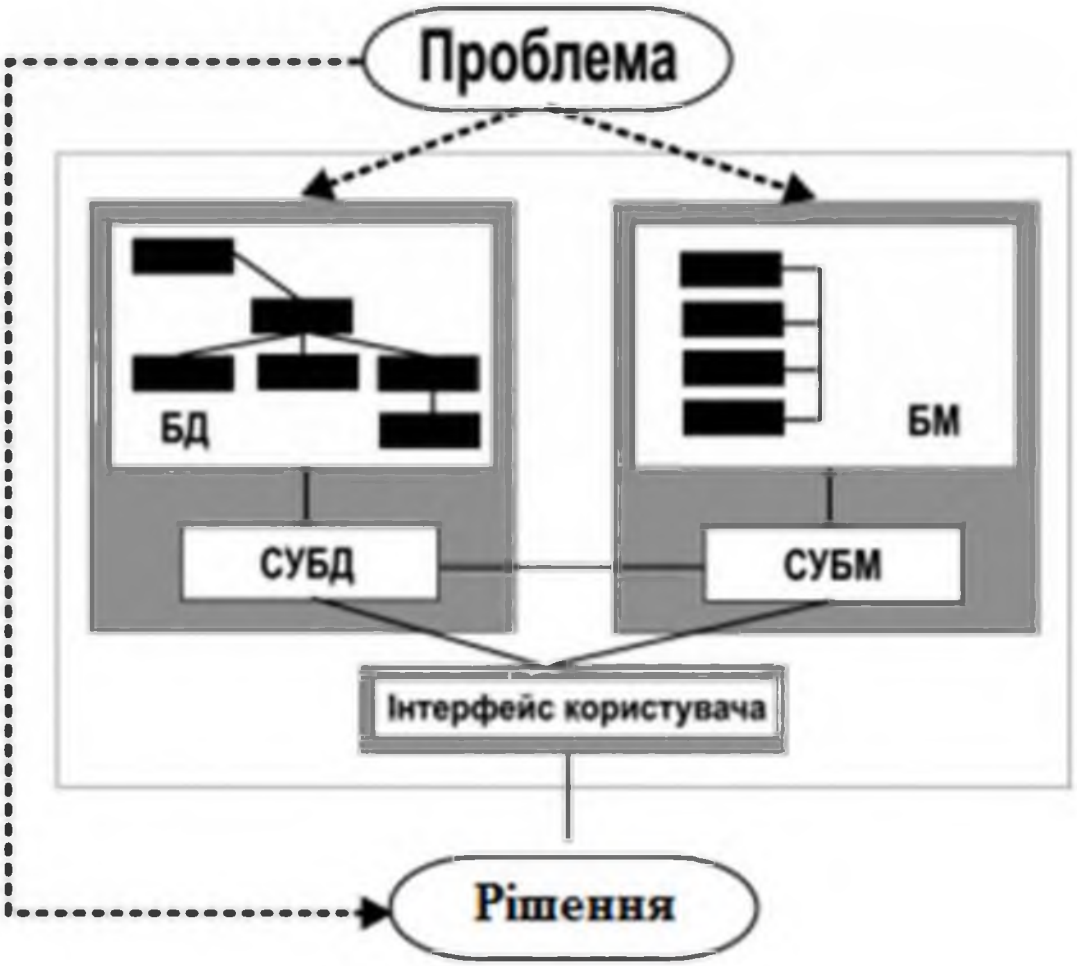


Рисунок 1.1 – Загальна структура СППР

До основних принципів, що обумовлюють визначений стандарт проєктування інтерфейсу “користувач – система”, належать:

1) засоби відображення управління;

2) компоненти діалогу між користувачем і системою;

3) підтримка сумісності відображуваної інформації та діалогу по всій СППР;

4) наявність засобів збереження виконаної роботи (з метою повторного входу в систему) та забезпечення “дружнього” режиму повторного входу;

5) наявність спеціалізованих і вмонтованих засобів протоколювання;

6) ключовим засобом інтерфейсу є графічне відображення і перетворення табличних даних у графіку;

7) наявність у СППР засобів прийому даних із зовнішніх джерел.

На даний момент у практиці створення СППР широко використовуються чотири альтернативні варіанти інтерфейсу:

1) інтерфейс, заснований на меню;

2) адаптивний інтерфейс;

3) інтерфейс на основі природної мови;

4) графічні засоби для побудови діалогу «користувач – система».

Інтерфейс, заснований на меню, забезпечує координацію дій користувача в складних ситуаціях, створюючи їм умови для прийняття послідовності більш простих рішень. Меню являє собою список варіантів (режимів, команд), що виводяться на екран і пропонуються користувачеві для вибору за допомогою однозначних кодових позначок кожного з варіантів.

В основі адаптивного інтерфейсу лежить концепція створення адаптивних програмних засобів, що здатні пристосовуватися до умов функціонування, непередбачених на етапі розробки системи. Такий інтерфейс дає можливість ОПР вносити в систему зміни, обумовлені особистісними особливостями сприйняття інформаційного середовища.

Головна перевага інтерфейсу на основі природної мови полягає в тому, що користувачі, що не мають значної кваліфікації в області інформатики або працюючі за межами своєї сфери знань, можуть спілкуватися із системою так, ніби вони спілкувалися з професіоналом у тій або іншій сфері. Графічні засоби для побудови діалогу є одним із найбільш розповсюджених способів забезпечення діалогу в інтерактивних інформаційних системах, якою, безумовно, є і система підтримки прийняття рішень.

Мова повідомлень - це те, що користувач бачить на екрані дисплея (символи, графіка, колір), дані, отримані на принтері, звукові вихідні сигнали і т.п. Важливим показником ефективності інтерфейсу є обрана форма діалогу між користувачем і системою. В даний час найбільш поширені наступні форми діалогу: запитання-відповідь, командний режим, режим меню, режим заповнення пропусків у виразах, запропонованих комп'ютером.

Підсистема даних СППР складається з бази даних і системи управління базою даних (далі - СУБД).

Особливості підсистеми даних у СППР:

- необхідність виконання великого обсягу операцій з переструктурування даних;
- необхідність передбачати можливість завантаження наступної обробки даних із зовнішніх джерел (потреба в зовнішніх даних тим вища, чим більш високий рівень керівництва);
- функціонування СУБД у середовищі СППР вимагає більш широкого набору функцій;
- швидке збільшення або виключення того чи іншого джерела даних з системи;
- побудова логічної структури даних в термінах користувача;
- використання і маніпулювання неофіційними даними для експериментальної перевірки робочих альтернатив користувача;
- забезпечення повної логічної незалежності цієї бази даних від інших операційних баз даних, що функціонують в рамках фірми.

Підсистема моделей СППР складається з бази моделей і системи управління базою моделей (далі - СУБМ). Під базою моделей мається на увазі сукупність формалізованих моделей, спрямованих на дослідження та перевірку безлічі альтернатив. Метою створення моделей є опис та оптимізація деякого об'єкта або процесу. Використання моделей забезпечує проведення аналізу в системах підтримки прийняття рішень.

База моделей може включати:

1) оптимізаційні моделі (моделі математичного програмування, розподіл ресурсів, оптимальне планування, аналіз сіткових графіків, моделі нелінійного і динамічного програмування та ін.);

2) неоптимізаційні моделі (статистичні моделі на основі аналізу регресії, моделі машинної імітації тощо);

3) моделі на основі понять і методів представлення знань (формальна

логіка, моделі продукцій, семантичні мережі, фрейми та гібриди перерахованих способів представлення знань).

Взаємодію користувача з моделями забезпечує система управління базою моделей, що є однією з компонентів архітектури СППР.

До основних функцій системи управління базою моделей належать:

1) створення нових і редагування існуючих моделей;

2) каталогізація широкого діапазону моделей;

3) поєднання компонентів моделей у бази моделей;

4) інтеграція складових елементів моделей;

5) виконання набору загальних функцій керування базу моделей;

6) забезпечення засобів зв'язку з базою даних.

Ще одним важливим і все частіше використовуваним компонентом СППР є база знань. Знання – це виявлені людиною закони й закономірності предметної галузі, які дозволяють ставити та вирішувати задачі. Знання, хоча й засновані на емпіричних даних, але являють собою результат розумової діяльності людини, спрямованої на узагальнення її практичного досвіду. У базі знань зберігаються знання про раніше вирішені проблеми та способи їхнього вирішення, а також різні рекомендації, які узагальнюють досвід експертів щодо процесу прийняття рішень. До них відносяться не тільки план дій, що знаходиться в голові у користувача, але і підручники, інструкції, довідкові дані, які видає комп'ютер.

1.1.3 Процес проєктування та реалізації СППР

Процес проєктування систем підтримки прийняття рішень розпочинається з того, що обирається задача, для вирішення якої необхідно створити СППР. Для виконання конкретних етапів необхідно мати спеціальний інструментарій, а також опис результату кожного етапу. Графічно процес проєктування цілком представлений на рисунку 1.2 [6].

При реалізації СППР використовуються останні досягнення в галузі інформаційних технологій, такі як:

а) OLAP-технології;

б) сховища даних;

в) вітрини даних;

г) добування знань (Data Mining);

д) генетичні алгоритми;

е) нейромережі;

є) імітаційне моделювання та інші.

OLAP-технології представляють собою набори даних (багатовимірні куби, гіперкуби, метакуби, OLAP-куби), які дозволяють підвищити ефективність роботи з даними, а також дають можливість у реальному часі генерувати складні запити, створювати звіти, виділяти підмножини даних, створювати описові і порівняльні зведення даних. OLAP-куби являють собою проєкцію вихідного куба даних на куб даних меншої розмірності. Значення осередків таких кубів, як правило, являють собою агреговані дані (сума, середнє, кількість, мінімум, максимум).

Вирішення проблеми неефективної підготовки інтегрованої інформації на основі запитів і звітів знайдено у вигляді концепції сховища даних (Data Ware House – DWH) – бази даних, що містить попередньо оброблені вихідні дані. Сховище даних може містити дані якогось одного або декількох типів. Однією з основних властивостей таких інформаційних структур є багатовимірна модель представлення даних.

СППР з незалежними вітринами даних поширені на великих підприємствах, котрим властива велика кількість підрозділів і департаментів, до складу яких входять власні відділи інформатизації.

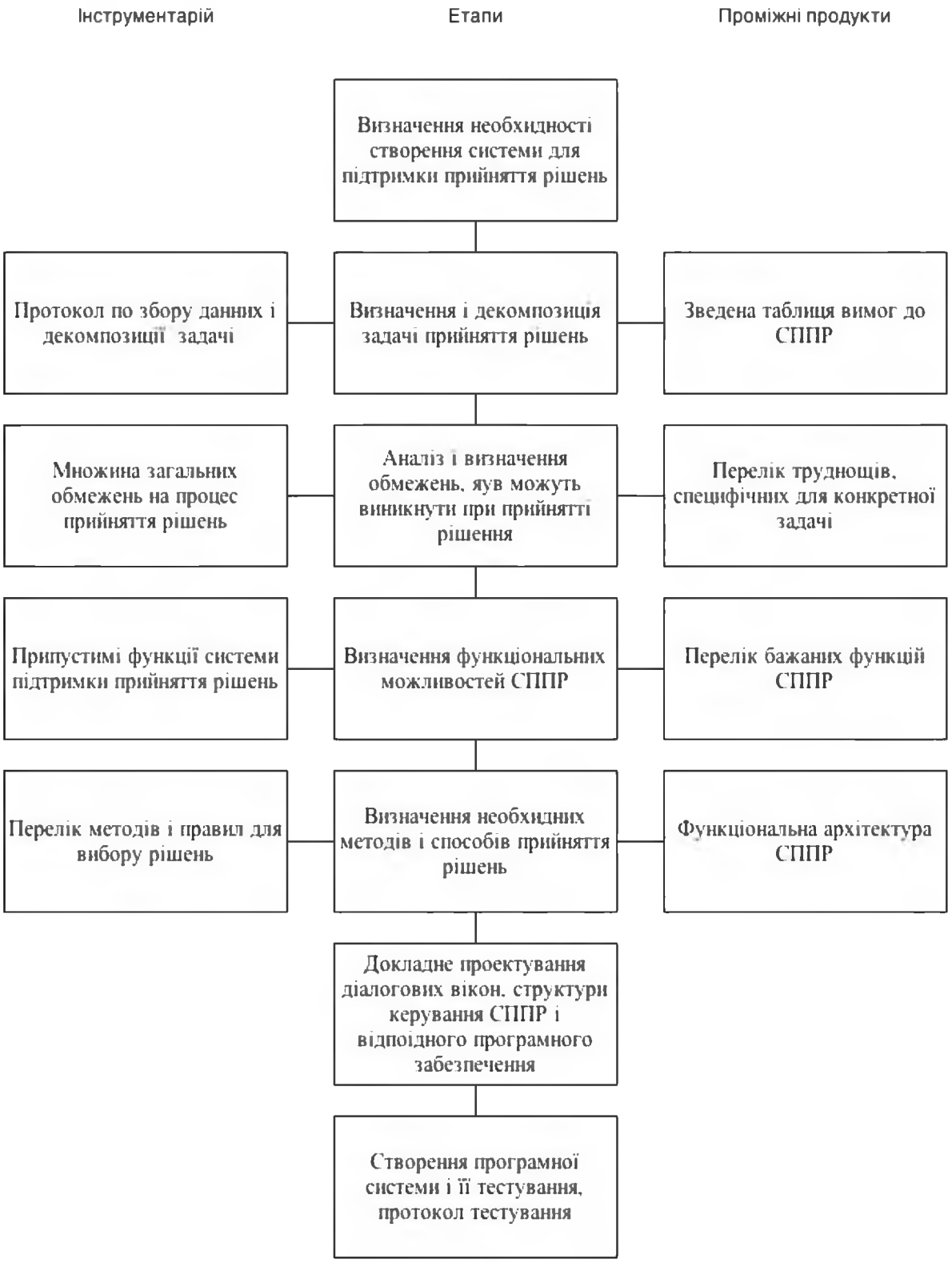


Рисунок 1.2 - Процес проєктування СППР

Тому незалежні вітрини даних часто з'являються в процесі функціонування і розвитку систем.

Технологія добування знань (Data Mining) дозволяє вирішувати питання аналізу даних, проводить найбільш глибокий і всебічний аналіз даних в

пошуку в них нетривіальних знань, які будуть надалі використовуватися для прийняття рішення. Технології Data Mining мають ряд переваг порівняно з аналізом на основі математичної статистики, так як призначені для пошуку шаблонів, що відбивають закономірності.

Головна відмінність методів, що використовують генетичні алгоритми та нейромережі полягає в тому, що нейромережі не мають потреби в заздалегідь відомій моделі, а будують її самостійно самі на основі запропонованої інформації. Саме тоді подібні алгоритми використовуються всюди, де є задачі, що погано алгоритмізуються. Основний недолік – необхідно мати великий обсяг початкової вибірки.

Суть методу імітаційного моделювання полягає в математичному описі динамічних процесів, відтворюючого функціонування системи, що вивчається. Даний метод дозволяє аналізувати складні динамічні системи (підприємства, банки, галузі економіки, регіони тощо) і складається з двох етапів: побудова комплексу динамічних імітаційних моделей та виконання аналітичних і прогнозних розрахунків. У більшості випадків імітаційне моделювання використовується у СППР під час проєктування структури складної системи або для пошуку оптимальних значень її параметрів (моделювання ситуацій за сценарієм “що буде, якщо...”, тощо).

1.1.4 Сфери застосування та проблеми використання СППР

СППР набуло широкого застосування в сфері економіки передових країн світу, при цьому їхня кількість постійно збільшується. На рівні стратегічного керування використовується ряд СППР, окремо для довго-, середнє- і короткострокового, а також для фінансового планування,
включаючи систему для розподілу капіталовкладень. Орієнтовані на операційне керування СППР застосовуються в галузях маркетингу (прогнозування й аналіз збуту, дослідження ринку і цін), науково-дослідних і конструкторських робіт, у керуванні кадрами, в медицині, в освіті, в

управлінні соціальними процесами, і в урядовій діяльності. Операційно-інформаційне застосування пов'язане з виробництвом, придбанням і обліком товарно-матеріальних запасів, їхнім фізичним розподілом і бухгалтерським обліком.

Комп'ютерна підтримка різних функцій за допомогою СППР має такий розподіл:

- операційне керівництво - 30%;
- довгострокове керівництво - 40%;
- розподіл ресурсів - 15%;
- розрахунок річного бюджету - 12 %.

Проте найчастіше СППР використовують для підтримки прийняття рішень в економічній сфері, найвідоміші реалізації СППР:

- SIMPLAN - для підтримки корпоративного планування;
- PIMS - для підтримки прийняття рішень в маркетингу;
- IFPS - для інтерактивного фінансового планування;
- PMS - для підтримки рішень при управлінні цінними паперами;
- Precision Tree Prime Decision - для підтримки прийняття рішень в економіці на основі дерев рішень;
- Decision Grid - для підтримки прийняття багатокрітеріальних рішень в економіці;
- Marketing Expert - для підтримки прийняття стратегічних рішень в маркетингу.

Успішне використання систем підтримки прийняття рішень вимагає долання ряду труднощів [7].

1 Верифікація рекомендацій СППР. Користувачі систем підтримки прийняття рішень мусять знати певні застереження щодо таких систем. Те, що ми можемо отримати від системи, не завжди є тим, що необхідно, а те, що необхідно, не завжди буде отримане або досягнуте. Досить часто перебільшуючи можливості СППР за її впровадження, менеджери чекають багато чого від нової СППР. Необхідно враховувати, що навіть найкраща

СППР не зможе виявити "погані" рішення. Деякі менеджери будуть продовжувати ставити неправильні запитання і формулювати неправильні висновки на підставі отриманої ними інформації. Отже, слід пам'ятати, що корпоративні СППР можуть ускладнити проблему і посилити шкоду, що завдається помилками у прийнятті рішень.

2 Психологічні проблеми застосування СППР. Для багатьох керівників старшого віку думка про те, що рекомендації надаватиме «якась машина» є неприпустимою. Подібна реакція пов'язана не тільки з суцільною недовірою до техніки, а й з відсутністю звички приймати рішення на основі формалізованих оцінок.

3 Необхідність збереження конфіденційності мотивів дій керівництва – іноді ця проблема є серйозною завадою для впровадження СППР. Адже не всі керівники мають бажання долучати співробітників до стратегічного планування, наприклад. Проте дана проблема вирішується засобами кодування справжніх побажань керівництва, що унеможливлюють ознайомлення співробітників з ними.

4 Протиріччя, що виникають при поєднанні відповідальності математиком-програмістом та керівником. Математик-програміст несе відповідальність лише за якість рішення поставленої задачі. Відповідальність же за прийняте рішення несе керівник, для якого процедура отриманого рішення математичними методами не є прозорою та зрозумілою. Саме таке протиріччя, коли рішення приймає одна людина, а формує інша є однією з причин відмови від користування таким корисним інструментом, як система підтримки прийняття рішень.

1.2 Загальні поняття та визначення в галузі проєктування захищених автоматизованих систем

Існуюча в Україні нормативна база ще не досягла необхідного розвитку в даній області. Так, наприклад, з величезного списку стандартів і нормативних документів України можна виділити лише деякі, які можуть бути використані при проєктуванні захищених АС.

Тому, при проведенні даного роду робіт, фахівці використовують також міжнародні (ISO) і міждержавні (ГОСТи, затверджені до 1992 року, включно) стандарти.

Згідно з одним із таких стандартів АС являє собою систему, що складається з персоналу та комплексу засобів автоматизації його діяльності, реалізовує інформаційну технологію виконання установлених функцій.

Залежно від виду діяльності виділяють наступні види АС: автоматизовані системи управління (АСУ), системи автоматизованого проєктування (САПР), автоматизовані системи наукових досліджень (АСНИ) і ін.

Залежно від виду керованого об'єкта (процесу) АСУ ділять на АСУ технологічними процесами (АСУТП), АСУ підприємствами (АСУП) і т.д.

У нашому випадку АС являє собою середовище обробки інформації, і також інформаційних ресурсів в інформаційно-телекомунікаційній системі. Тому надалі будемо використовувати поняття автоматизована інформаційна система.

Закон України «Про інформацію» [1] трактує поняття «інформація» в наступному вигляді: «під інформацією розуміється документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому середовищі».

У свою чергу, захист інформації в АС - діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації і АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків у результаті реалізації загроз.

Таким чином, автоматизована інформаційна система (АІС) являє собою складну систему, яку доцільно розділяти на окремі блоки (модулі) для полегшення її подальшого проєктування. У результаті цього, кожен модуль буде незалежний від інших, а в комплексі вони будуть складати цілісну систему захисту.

Виділення окремих модулів АІС дозволяє службі захисту інформації:

- своєчасно і адекватно реагувати на певні види загроз інформації, які властиві певному модулю;
- в короткі терміни впроваджувати систему захисту інформації в модулях, які щойно з'явилися;
- спростити процедуру контролю системи захисту інформації в цілому (під системою захисту інформаційної інфраструктури підприємства в цілому слід розуміти сукупність модулів систем захисту інформації).

Поступово нарощуючи кількість модулів, а також ускладнюючи структуру захисту, АІС набуває певної комплексність, яка має на увазі використання не одного типу захисних функцій у всіх модулях, а їх добуток.

Таким чином, побудова КСЗІ стає невід'ємним фактором у розробці ефективної системи захисту від несанкціонованого доступу.

Згідно з КСЗІ - сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Звідси видно, що, наприклад, простим екрануванням приміщення при проєктуванні КСЗІ не обійтися, тому що цей метод передбачає лише захист інформації від витоку по радіоканалу.

У загальному випадку поняття «комплексність» представляє собою рішення в рамках єдиної концепції двох або більше різнопланових завдань (цільова комплексність), або використання для вирішення однієї і тієї ж задачі різнопланових інструментальних засобів (інструментальна комплексність), або те й інше (загальна комплексність).

Цільова комплексність означає, що система інформаційної безпеки повинна будуватися таким чином:

- захист інформації, інформаційних ресурсів та систем особистості, суспільства і держави від зовнішніх і внутрішніх загроз;
- захист особи, суспільства і держави від негативного інформаційного впливу.

Інструментальна комплексність передбачає інтеграцію всіх видів і напрямків ІБ для досягнення поставлених цілей.

Сучасна система захисту інформації повинна включати структурну, функціональну і тимчасову комплексність.

Структурна комплексність передбачає забезпечення необхідного рівня захисту в усіх елементах системи обробки інформації.

Функціональна комплексність означає, що методи захисту повинні бути спрямовані на всі виконувані функції системи обробки інформації.

Тимчасова комплексність передбачає безперервність здійснення заходів щодо захисту інформації, як в процесі безпосередньої її обробки, так і на всіх етапах життєвого циклу об'єкта обробки інформації.

1.3 Класифікація автоматизованих систем

Нормативним документом (НД ТЗИ 2.5-005-99) передбачається розподіл АС на 3 класи:

- Клас 1 - одномашінний однокористувацький комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності. Приклад - автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.
- Клас 2 - локалізований багатомашинний багатокористувацький комплекс, що обробляє інформацію різних категорій конфіденційності. Приклад - локальна обчислювальна мережа.
- Клас 3 - розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності. Приклад - глобальна обчислювальна мережа.

1.3.1 Особливості АС класу 1

Інформація з обмеженим доступом, а саме: конфіденційна інформація, що належить державі, та інформація, що містить державну таємницю, створюється, обробляється і зберігається в режимно-секретному (РСО) органі. Така інформація, в більшості випадків, обробляється з використанням АС класу 1, які мають такі особливості:

- в кожен момент часу з комплексом може працювати тільки один користувач, хоча в загальному випадку осіб, які мають доступ до комплексу, може бути кілька, але всі повинні мати однакові повноваження (права) щодо доступу до оброблюваної інформації;

- технічні засоби (носії інформації та засоби введення / виводу), з точки зору, захищеності відносяться до однієї категорії і всі вони можуть використовуватися для зберігання та / або введення / виведення всієї інформації.

Для проведення робіт, пов'язаних з побудовою КСЗІ РСО, фахівцям організації виконавця повинен бути оформлений допуск до державної таємниці.

При створенні КСЗІ РСО використовуються тільки ті технічні засоби захисту інформації, які мають експертний висновок або сертифікат відповідності державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ) Україна, застосування інших технічних засобів захисту інформації заборонено.

Методика проведення робіт з побудови КСЗІ АС класу 1 базується на наступних вихідних даних:

- Об'єкт захисту - робоча станція.

- Захист інформації від витоку по технічних каналах здійснюється за рахунок використання робочої станції в захищеному виконанні або спеціальних засобів.

- Захист від несанкціонованого доступу до інформації здійснюється спеціальними програмними або апаратно-програмними засобами захисту від несанкціонованого доступу.

- Захист комп'ютера від вірусів, троянських і шпигунських програм - антивірусне програмне забезпечення.

1.3.2 Особливості АС класу 2 і 3

В основному в АС класу 2 і класу 3 обробляється конфіденційна або відкрита інформація, яка належить державі і до якої висуваються вимоги щодо забезпечення цілісності та доступності.

Особливості АС класу 2: наявність користувачів з різними повноваженнями по доступу та / або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності.

Особливості АС класу 3: необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, які реалізують різну політику безпеки.

АС класу 3 відрізняється від АС класу 2 наявністю каналу доступу в Інтернет.

Так само, як і для створення КСЗІ РСО, для створення КСЗІ АС класу 2 і класу 3 організація-виконавець повинна мати ліцензію на проведення робіт у сфері технічного захисту інформації, а також використовувати сертифіковані технічні засоби захисту інформації.

Методика проведення робіт з побудови КСЗІ АС класу 2 (3) базується на таких вихідних даних:

- Об'єктами захисту є робочі станції, канали передачі даних, веб-сервери, периметр інформаційної системи і т. д.
- Захист від несанкціонованого доступу здійснюється за допомогою базових засобів операційної системи або з використанням спеціальних програмних, апаратно-програмних засобів.
- Захист каналів передачі даних через незахищену середу - апаратні, програмні, апаратно-програмні засоби шифрування інформації.
- Захист периметру - програмні, апаратні міжмережеві екрани, системи виявлення атак.
- Захист комп'ютера (мережі) від вірусів, троянських і шпигунських програм - антивірусне програмне забезпечення.

- Захист електронного документообігу та електронної пошти - використання засобів електронного цифрового підпису.

Споживачами КСЗІ АС класу 2 і класу 3 є органи державної влади, а також підприємства, діяльність яких пов'язана з обробкою конфіденційної інформації, що належить державі.

1.3.3 Системи інформаційної безпеки

Виділяють ще один тип АС - системи інформаційної безпеки (СІБ).

СІБ представляють собою рішення, спрямоване на забезпечення захисту критичної інформації організації від розголошення, витоку і несанкціонованого доступу. Як і КСЗІ, СІБ об'єднує в собі комплекс організаційних заходів і технічних засобів захисту інформації.

СІБ в основному призначені для захисту інформації в АС класу 2 і класу 3. Однак між КСЗІ та СІБ є принципові відмінності.

Перша відмінність полягає в тому, що при побудові СІБ немає необхідності виконувати вимоги нормативних документів у сфері технічного захисту інформації, так як основними споживачами СІБ є комерційні організації, які не обробляють інформацію, що належить державі. Другим принциповою відмінністю є відсутність контролюючого органу, і, як наслідок, спроєктована СІБ не вимагає проведення державної експертизи. Ще одна відмінність від КСЗІ - вільний вибір технічних засобів, можливе застосування будь-яких апаратних і програмних засобів захисту інформації.

СІБ можна рекомендувати комерційним організаціям, які піклуються про збереження своєї комерційної (критичною) інформації або збираються вживати заходів щодо забезпечення безпеки своїх інформаційних активів.

Для визначення необхідності побудови СІБ та напрями робіт із захисту інформації, а також для оцінки реального стану інформаційної безпеки організації необхідно проводити аудит інформаційної безпеки.

Стосовно до КСЗІ РСО та КСЗІ АС класу 2 і класу 3 проведення такого аудиту теж є першим етапом робіт. Такі роботи називаються обстеженням інформаційної інфраструктури організації.

Важливим моментом, який стосується експлуатації як КСЗІ АС класу 2 і класу 3, так і СІБ, є той факт, що недостатньо просто побудувати і експлуатувати ці системи захисту, необхідно постійно їх удосконалювати так само, як удосконалюються способи несанкціонованого доступу, методи злому і хакерські атаки.

Порівняльний аналіз всіх перерахованих систем захисту інформації (Табл.1.1).

Як бачимо, більш жорсткі вимоги висунуті до процесу побудови КСЗІ та виконавцю цих робіт у порівнянні з вимогами до побудови СІБ.

Надалі, при проєктуванні системи захисту будемо брати за основу АС класу 1 і 2, тому що саме ці системи обробки інформації представляють найбільш великий інтерес у зловмисника з точки зору її розкрадання.

Таблиця 1.1 - Порівняльний аналіз систем захисту інформації

Особливості КСЗІ	РСО КСЗІ	АС класу 2 (3)	СІБ
Споживачі послуг	Органи державної влади, комерційні організації	Органи державної влади, комерційні організації	Комерційні організації
Оброблювана інформація	Конфіденційна інформація, яка належить державі, або інформація, яка містить	Конфіденційна інформація, яка належить державі (фізичній особі), або відкрита інформація, яка належить державі	Критична інформація організації (персональна, фінансова,

	державну таємницю		договірна інформація)
Суб'єкти	Замовник, виконавець, контролюючий орган	Замовник, виконавець, контролюючий орган	Замовник, виконавець
Наявність ліцензії на проведення робіт з побудови	Ліцензія на проведення робіт з технічного захисту інформації	Ліцензія на проведення робіт з технічного захисту інформації	Не вимагається
Проведення державної експертизи	Обов'язково	Обов'язково	Не вимагається
Технічні засоби захисту інформації	Тільки сертифіковані засоби захисту інформації	Тільки сертифіковані засоби захисту інформації	Будь-які засоби захисту інформації
Виконання вимог нормативів	Обов'язково	Обов'язково	Не вимагається

1.3.4 Порядок створення комплексної системи захисту інформації

Створення КСЗІ в ІТС здійснюється відповідно до нормативного документа системи технічного захисту інформації на підставі технічного завдання (далі - ТЗ), розробленого згідно з вимогами нормативного документа системи технічного захисту інформації. Крім того, при проєктуванні КСЗІ можна керуватися стандартом.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричних та інших каналів;
- несанкціонованих дій та несанкціонованого доступу до інформації, які можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів і т.п. ;
- спеціального впливу на інформацію, що може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом АС та умовами її експлуатації.

1.3.5 Аналіз структури автоматизованої інформаційної системи

Дана стадія розробки включає в себе наступні роботи:

- проведення передпроєктного обстеження;
- розробка аналітичного обгрунтування щодо створення КСЗІ;
- розробка технічного завдання на створення КСЗІ.

У ході даного етапу проводиться аналіз ризиків. Для перевірки здатності інформаційної системи протистояти спробам несанкціонованого доступу і впливу на інформацію іноді доцільно виконувати тести на проникнення.

Існує кілька видів обстеження:

- передпроєктне діагностичне обстеження, яке виконується при модернізації чи побудові ЗЗІ;

- аудит ЗЗІ на відповідність вимогам внутрішньокорпоративним стандартам або міжнародним / національним стандартам. Прикладом може служити сертифікаційний аудит системи управління ІБ по ISO 27001;
- спеціальні види обстеження, наприклад, при розслідуванні комп'ютерних інцидентів.

Світовий досвід створення систем захисту для різного роду об'єктів дозволяє виділити три основні елементи, присутніх практично на будь-якому об'єкті і вимагають забезпечення їх безпеки:

- люди - персонал і відвідувачі об'єкта;
- матеріальні цінності, майно та обладнання;
- критична інформація - інформація з різними грифами таємності.

Кожен з виділених елементів має свої особливості, які необхідно врахувати при визначенні можливих загроз. За результатами аналізу можливих загроз безпеки АС формуються вимоги до захисту. Повний захист АС формується з приватних вимог захисту елементів шляхом об'єднання функціонально однорідних вимог по забезпеченню захисту.

За результатами даного етапу визначаються і формуються вимоги до захисту. Повний захист АС формується з приватних вимог захисту елементів шляхом об'єднання функціонально однорідних даних щодо забезпечення захисту. До таких даних відноситься захищена інформація на основі документально оформлених переліків відомостей, загрози безпеці інформації та модель ймовірного порушника, склад використовуваних технічних засобів і зв'язки між ними, складу розробленої організаційно-розпорядчої документації, клас захищеності АС в захищеному виконанні. Приймаються рішення, що стосуються складу технічних засобів і систем, передбачуваних до використання в системі, що розробляється, та заходів щодо забезпечення конфіденційності інформації на етапі проєктування системи.

1.4 Методологія формування моделі загроз

Для створення моделі загроз необхідно скласти перелік суттєвих загроз,

описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та 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 з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

- збої і відмови у роботі обладнання та технічних засобів АС;

- наслідки помилок під час проєктування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

- помилки персоналу (користувачів) АС під час експлуатації;

- навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей

вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості АС.

1.5 Висновок. Постановка задачі

В даній частині роботи була розглянута класифікація СППР, базові компоненти СППР, порядок створення комплексної системи захисту інформації, класифікація АС, системи інформаційної безпеки.

Таким чином актуальними задачами роботи будуть:

1. Розгляд основних уразливих структурно-функціональних елементів АС.
2. Розробка етапів роботи системи підтримки прийняття рішень для моделювання загроз інформації для АС класу 2.
3. Розробка алгоритму роботи системи підтримки прийняття рішень для моделювання загроз інформації для АС класу 2.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальна модель процесу прийняття рішення

Модель послідовного процесу прийняття рішення може допомогти аналізувати те, як рішення розробляється і як це слід робити. Г.А. Саймон 1960 року виділив такі три стадії в послідовному процесі прийняття рішень:

- інтелектуальна (intelligence) – виявлення обставин (можливостей) для розроблення рішення, збирання та упорядкування інформації і знань, передбачення можливих варіантів рішень;
- проєктувальна (desing) – виявлення, винайдення, розроблення й аналізування альтернативних напрямів дій, оцінювання очікуваних наслідків;
- вибору (choice), тобто відбір альтернатив – застосування повноважень для того, щоб вибрати кращий варіант з урахуванням факторів зовнішнього і внутрішнього впливу.

Інколи запроваджують четверту стадію реалізації. Перед реалізацією головне рішення має бути прийнятим, а сама реалізація потім включає багато дій. Управління цими стадіями і визначення того, як вони взаємопов'язані, може бути головним питанням всього комплексу стрімко змінюваних, неоднозначних або сумнівних проблемних ситуацій. Кожна із вищезазначених стадій може бути підтримана окремими блоками систем підтримки прийняття рішень. З погляду конкретнішого узгодження всіх операцій створення рішення можна так зобразити узагальнену модель процесу прийняття рішення (рис. 2.1), щоб вона відбивала процес генерування узгодженого рішення.

Прийняття рішення – це більше, ніж просто сам вибір. Кожний крок у процесі прийняття рішення є важливим; на кожному з них можна допуститися помилки і кожний може потенційно бути підтриманий деяким видом комп'ютеризованої допомоги. Розглянемо докладніше сімку кроків у загальній моделі процесу прийняття рішення:

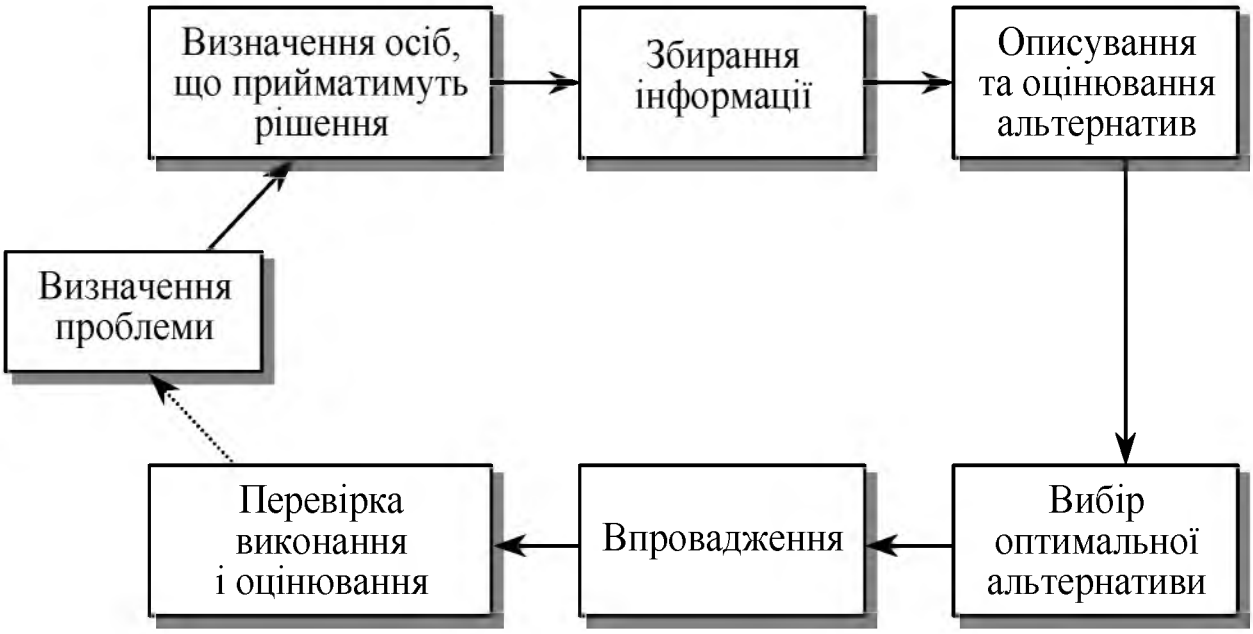


Рисунок 2.1 – Процес генерування узгодженого рішення

- визначення проблеми. Що чіткіше сформульована проблема набагато легша для розв'язування, а скорочений опис проблеми зменшує шанси отримати добру відповідь, або призводить до помилкової (несправжньої) проблеми. Коли неправильно визначена проблема, то це унеможливлює створення ефективного рішення. Від того, у який спосіб проблема «окреслена» і як визначені її чинники, залежить її розв'язок і вибір типу підтримки рішення, якщо вона використовується;

- збирання інформації. Як тільки проблема визначена, можна приступати до виявлення чинників, що визначають ефективність розв'язання проблеми, та інформації, потрібної для розроблення реальних альтернатив. Без інформації прийняття рішення є таким, що ґрунтується на передчуттях і інтуїції. З другого боку, дуже багато часу для збирання інформації може бути виснажливим. Формальний пошук і накопичення даних потребує як грошей, так і часу. Додаткові витрати слід зіставляти з вигодами від додаткових даних. СППР можуть надавати інформацію для створення рішень, але вартість цього визначається за розроблення і використання системи;

- описування та оцінювання альтернатив. Найбільш творчою складовою частиною прийняття рішень є описання альтернатив і визначення

того, що саме потрібно отримати в процесі серйозного дослідження й аналізу. Для генерування ідей корисною в багатьох ситуаціях є мозкова атака. Велика кількість ідей імовірніше веде до деяких ідей найвищої якості, ніж зосередження на одній або кількох дуже поверхових ідеях. Застосування групової мозкової атаки й інструментальних засобів оцінювання ідей реалізоване в деяких групових системах підтримки прийняття рішень: безмовне генерування ідей, колективне використання ідей, оцінювання або ранжування альтернатив, використання критеріїв, що можуть допомогти оцінити альтернативи;

- вибір оптимальної альтернативи. Прийняти рішення – це означає вибрати напрям дій або бездіяльність. У деяких ситуаціях рішення мають бути розроблені – це або є обов'язковим, або вимагається обставинами, клієнтами чи акціонерами. Рішення, крім того, інколи розробляються на підставі меншого обсягу інформації, ніж це має бути, або вибираються з деякої сукупності можливих альтернатив, які не оцінюються чи, навіть, не розглядаються. СППР, звичайно, не є такою ж корисною в цих «кризових» проблемних ситуаціях. За інших обставин є більше часу для збирання інформації і оцінювання альтернатив, зокрема, засобами СППР;

- реалізація (впровадження). Прийняття рішення є кульмінацією єдиного процесу. Специфічний процес розроблення рішення може бути затяжним і складним або стрімким і простим. Але для будь-якої проблеми і будь-якої множини альтернатив, розроблених з комп'ютерною допомогою або без неї, якщо тільки рішення розроблене, що-небудь, звичайно, має відбутися. Рішення часто ініціюють дії і інформаційні технології можуть концентрувати й направляти ті дії на розширення змін. СППР може допомогти в налагодженні зв'язків, потрібних для прийняття рішень, моніторингу планів і дій та відслідковуванні ефективності;

- перевірка виконання і оцінювання. Вимірювання і оцінювання наслідків рішення, яке було реалізоване, потрібні творцям рішень, оскільки вони відповідальні за нього. За відслідковування процесу реалізації рішення

можуть з'являтися нові проблеми. У деяких випадках потрібні незначні регулювання чи виправлення дій. Через те, що ситуації не залишаються довго такими самими, менеджери часто мають справу з проблемами, які виникли в результаті прийнятого рішення, або які пов'язані з попередніми проблемами. СППР може допомогти в моніторингу, перевірці виконання і оцінюванні рішень.

2.2 Моделі системи підтримки прийняття рішень

2.2.1 Моделі в аспекті інформаційного підходу

В аспекті інформаційного підходу СППР належать до класу інформаційних систем, основне призначення яких полягає в поліпшенні характеру діяльності управлінського персоналу організацій за рахунок застосування засобів інформаційних технологій. У рамках цього підходу було запропоновано дві моделі СППР: концептуальна модель Спрага та модель еволюціонуючої СППР.

Концептуальна модель Спрага зображена на рис. 2.2 Основними її компонентами є: інтерфейс «користувач – система», база даних і база моделей. Інтерфейс «користувач – система» забезпечує зв'язок з кожною із баз. Він включає програмні засоби для керування базою даних та базою моделей), керування генеруванням діалогу і має забезпечувати виконання таких функцій: керувати різноманітними стилями ведення діалогу; змінювати стиль діалогу за бажанням користувача; подавати дані в різних формах і виглядах; надавати гнучку підтримку користувачу.

Бази даних СППР містять як кількісну, так і якісну інформацію, що надходить із різних джерел. Засоби створення і ведення бази даних мають надавати такі можливості: об'єднувати різні джерела інформації, використовуючи процедури її «добування»; легко і швидко добавляти й виключати джерела даних; подавати логічну структуру даних у термінах

користувача; керувати персональними і неофіційними даними за вимогою користувача; мати цілий ряд функцій керування даними.

Рисунок 2.2- Концептуальна модель СППР Спрага

База моделей має забезпечувати гнучкість моделювання, зокрема, за рахунок використання готових блоків і підпрограм. Керування моделями дає змогу: каталогізувати та обслуговувати широкий спектр моделей, які підтримують всі рівні управління; легко і швидко створювати нові моделі; зв'язувати моделі з відповідними базами даних.

Модель еволюціонуючої СППР (рис.2.3) є подальшим розвитком моделі Спрага. Крім користувацького інтерфейсу, бази даних і бази моделей ця система містить базу текстів і базу правил, завдяки чому розширюються її функціональні можливості. Інформаційна база СППР дає змогу використовувати як менш структуровані (тексти звичайною мовою), так і більш структуровані види інформації.

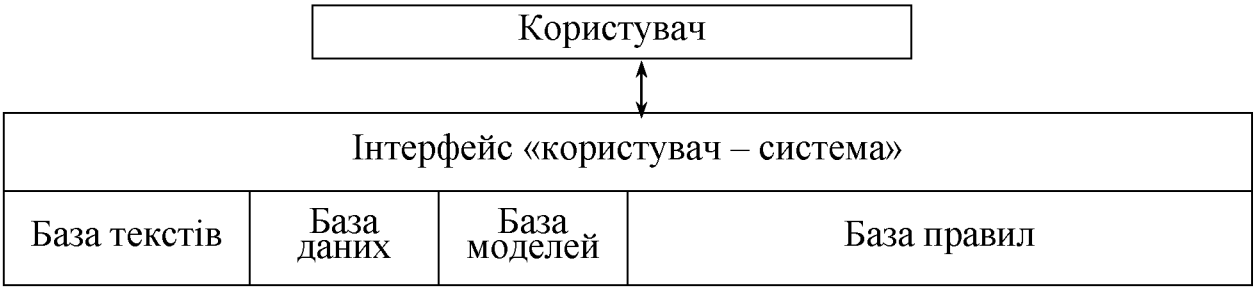


Рисунок 2.3 - Модель еволюціонуючої СППР

2.2.2 Модель, основана на знаннях

Елементи штучного інтелекту, зокрема, використання звичайної мови для спілкування з системою, методологія експертних систем, інженерія знань і комп'ютерних мов штучного інтелекту знайшли своє застосування в усіх трьох базових компонентах СППР: у базі даних і СКБД, у базі моделей і СКБМ, у користувацькому інтерфейсі. Але є концепції створення СППР, в яких система знань у СППР є одним із визначальних факторів. Характерною особливістю СППР, основаних на знаннях, є явне виділення нового аспекту підтримки рішень – спроможність «розуміти» проблеми, тобто здатність прийняти запит користувача, зібрати відповідну інформацію і підготувати звіт.

Модель СППР, яка базується на знаннях, зображена на рис. 2.4 Вона складається з трьох взаємодіючих частин: мовної системи, системи знань і системи оброблення проблем (проблемного процесора).

Мовна система забезпечує комунікацію між користувачем і усіма компонентами комп'ютерної системи. З її допомогою користувач формулює проблему і керує процесом її розв'язання, використовуючи пропоновані мовною системою синтаксичні й семантичні засоби.

Система знань містить інформацію стосовно проблемної галузі. Типи цих систем відрізняються за характером подання в них даних і використовуваними моделями формалізації знань (ієрархічні структури, графи, семантичні мережі, фрейми, системи продукції, обчислення предикатів тощо).

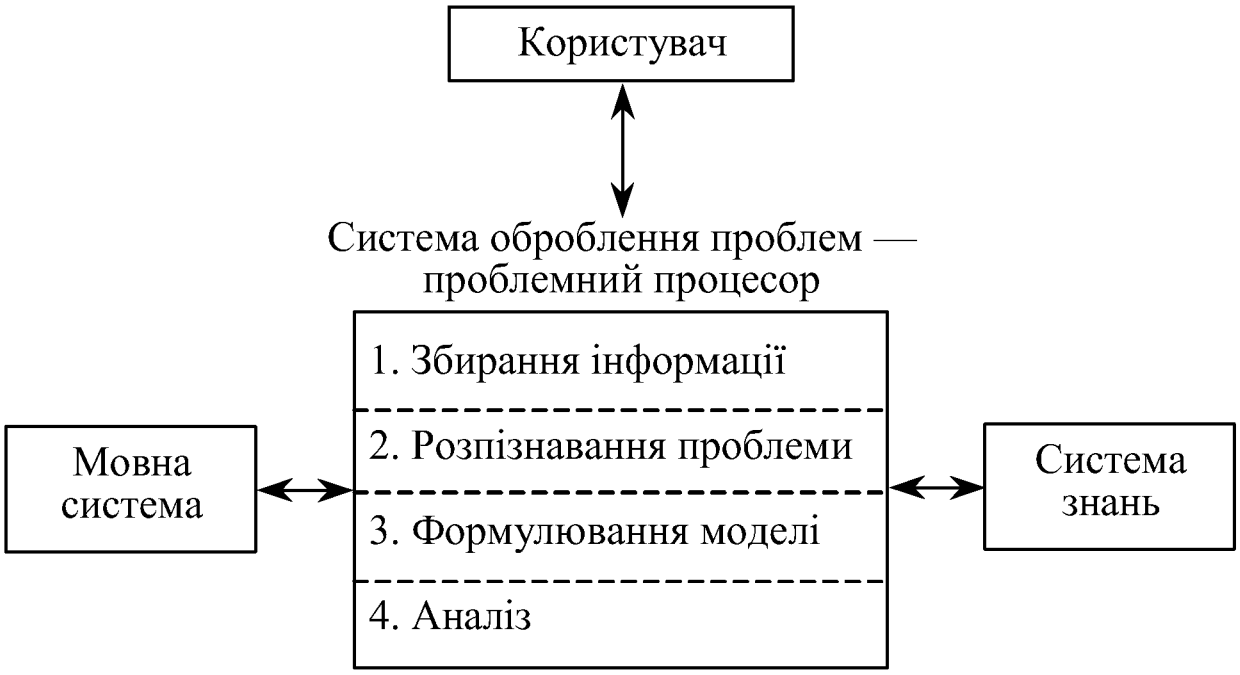


Рисунок 2.4 - Модель СППР, основаної на знаннях

Система оброблення проблем є механізмом, який зв'язує мовну систему і систему знань. Цей проблемний процесор забезпечує збирання інформації, формулювання моделі, її аналіз тощо. Він сприймає описання проблеми, виконане у відповідності з синтаксисом мовної системи, і використовує знання, організовані згідно з прийнятими в системі знань правилами, з метою створення інформації, необхідної для підтримки рішень. Проблемний процесор є динамічним компонентом СППР, який відображає поведінку людини, яка розв'язує проблему. Тому він, як мінімум, має бути спроможним інтегрувати інформацію, що надходить від користувача через мовну систему і систему знань, і, використовуючи моделі, перетворювати формулювання проблеми в детальні процедури, виконання яких урешті-решт приводить до відповіді. У складніших випадках проблемний процесор має вміти формувати моделі, необхідні для розв'язання поставленої проблеми.

2.2.3 Модель ієрархії управління

У сфері організаційного управління прийнято виділяти вищий, середній і нижчий рівні ієрархічної структури. Модель СППР, орієнтована на ієрархію

управління, забезпечує підтримку ОПР на всіх рівнях управління, а також супроводжує координування цих рівнів там, де це можливо.

До недавнього часу найпоширенішою була думка, що СППР призначені для керівників вищих і середніх ланок адміністративної ієрархії, причому вважалося, що керівники вищого рівня рідко виявлялися серед кінцевих користувачів систем і що такі системи впливають на вищий рівень прийняття рішень переважно непрямим (опосередкованим) способом за рахунок використання СППР керівниками нижчого рівня і співробітниками, котрі обслуговують керівників високого рангу. Але з часом було доведено, що СППР для керівників вищої ланки може бути цілком успішно реалізована за умови, що вона буде правильно спроєктована, буде задовольняти вимоги і містити основні для цієї особливої групи користувачів методи розв'язання задач.

Адміністративна СППР розробляється для безпосереднього використання керівниками вищого рівня управління. Тому вона має надавати вільний доступ до поточної інформації стосовно статусу організації і враховувати головні фактори успіху керівника. АСППР має використовувати сучасну графіку, засоби комунікації і методи зберігання та вибирання даних. Засоби моделювання мають бути подані в мінімальному обсязі. Вищим керівникам не потрібні хитромудрі моделі й методи, оскільки ці засоби можуть продуктивно використовуватися на рівні їх безпосередньо підлеглих і на нижчих рівнях керівництва, звідки кінцеві результати моделювання можуть потрапляти до керівників вищого рівня шляхом брифінгів, звітів і рекомендацій.

Наріжним каменем ефективно й успішно функціонуючої АСППР є користувацький інтерфейс. Головне меню та індекс ключових слів розраховані на надання користувачеві допомоги стосовно швидкого пошуку всієї необхідної інформації. Інформація організована за принципом «зверху вниз», тобто спочатку подається зміст інформації, а потім керівник за

бажанням чи необхідністю може рухатися «вниз» для деталізації повідомлень. Для окремих екранних зображень дотримуються стандартів відповідно до застосовуваних термінів, кольорових кодів і графічних структур.

Перевагами цієї системи є краща інформативність, досконаліші комунікації, розвиваюче розуміння інформаційних вимог і відчутне зниження затрат. За вигідністю, частотою користування і задоволення користувачів відчутно проявляється успіх системи, але головним визначальним фактором є те, що керівники регулярно її використовують. Цей приклад підтверджує те, що адміністративні системи підтримки рішень реальні й потенційно життєздатні, а це відкрило, як уже зазначалося, новий напрям для застосувань і досліджень СППР – виконавчі інформаційні системи.

2.2.4 Моделі, орієнтовані на особистість ОПР

Моделі СППР, орієнтовані на особистість користувача, що приймає рішення, реалізують ідею універсальної підтримки різнобічних процесів прийняття рішень. Для повнішого розуміння контексту проблем підтримки рішень потрібно зіставити деякі аспекти оброблення інформації людиною і комп'ютером. Оброблення інформації людиною тісно пов'язане з біологічною спеціалізацією частин її мозку: ліва півкуля мозку виконує раціональні, упорядковані й динамічні функції, а права – інтуїтивні, паралельні дії. Комп'ютер виконує лише логічні й упорядковані дії, тобто його архітектура моделює роботу лівої півкулі мозку.

Визнаючи, що електронний і біологічний «комп'ютери» виконують різні дії, потрібно розв'язати дилему: у який спосіб розділити роботу між ними. Інформаційні системи для оперативного рівня менше залежать від біокомп'ютера і тому спроможні значною мірою автоматизувати дії, виконувані людиною. Це має місце також і стосовно структурованих завдань управління. Але за зміни акцентів у бік неструктурованих завдань і проблем стратегічного управління роль біокомп'ютера зростає, тобто за створення

засобів підтримки рішень складних проблем значення біокомп'ютера стає вирішальним.

2.2.5 Моделі для планування та прогнозування

Планування і прогнозування є одними з найширших сфер застосування систем підтримки прийняття рішень. Нараховуються десятки реалізацій СППР, головне завдання яких полягає в забезпеченні керівників різних рангів технологічними засобами, що створюють одночасно з наданням нової інформації умови для пробудження зацікавленості та інтуїції, ділової активності господарських керівників. У цих засобах акумульовані власний досвід керівників і досвід ОПР інших організацій, застосований широкий спектр методів і моделей, зокрема, математичне програмування, статистичний аналіз, теорія статистичних рішень, методи прийняття рішень за умов невизначеності, евристичні методи, методи теорії ігор тощо. Вартість СППР, орієнтованих на корпоративне планування, досить висока і може змінюватись від кількох тисяч до кількох сотень тисяч доларів. Тому лише великі корпорації в змозі експлуатувати ці системи в повному обсязі можливостей, які надаються (СППР реалізуються на великих ЕОМ). Середні й дрібні фірми, як правило, використовують подібні СППР шляхом оренди ліній зв'язку і роботи з ними з віддалених терміналів у режимі розподілу часу.

СППР у сфері планування надають користувачам такі можливості:

- мову моделювання, за допомогою якої описується структура досліджуваної проблеми у вигляді співвідношень, що пов'язують вхідні, вихідні й керуючі змінні;
- генерування повідомлень різного типу, в тому числі стандартні повідомлення фіксованого формату; повідомлення, форматовані на основі параметрів моделі; мова повідомлень, яка уможливлює вибір змінних і форм їх подання; графічні повідомлення, що включають графіки, діаграми, гістограми й інші види зображення інформації;

- аналітичні засоби, що містять моделі і пакети програм. Здебільшого керівники й працівники апарату управління не можуть точно описати програмістам і конструкторам моделей, які ситуації їм належить розглядати в майбутньому, тому аналітичні засоби СППР реалізуються у вигляді різних пакетів оброблення, організованих у такий спосіб, що користувачі мають можливість формулювати завдання у термінах звичної для них професійної мови плановиків.

2.2.6 Модель для конторської діяльності

У сучасному офісі інтелектуальна діяльність працівників направлена на збирання та аналіз необхідної інформації, генерування, обговорення і поширення нових ідей, на прийняття відповідних рішень. Використання СППР у сфері автоматизації функціонування офісу підвищує ефективність діяльності управлінського персоналу за рахунок поліпшення якості створюваної інформації і комунікаційних зв'язків. Цьому призначенню відповідають функції СППР:

- підтримка процесів генерування інформації відповідно до індивідуальних здібностей кожного працівника;
- підтримка процесів точного і швидкого передавання та поширення інформації, що виникла в результаті інтелектуальної діяльності;
- підтримка процесів зберігання, пошуку і видачі потрібної інформації.

СППР офісу можуть містити різні підсистеми, зокрема, за функціональною ознакою можна виділити три групи:

- Процесорні системи, починаючи від персональних ЕОМ і закінчуючи високопродуктивними обчислювальними машинами, забезпечують оброблення і зберігання інформації на різних рівнях ієрархії;
- локальні мережі зв'язку підтримують обмін діловою інформацією, яка знаходиться у різних користувачів, забезпечують організацію телеконференцій, прийняття колективних рішень;

- робочі станції складаються із цілого ряду зв'язаних із процесорами термінальних пристроїв, пристроїв для введення і виведення інформації, засобів телекомунікації;

2.3 Уразливість основних структурно-функціональних елементів автоматизованої системи

У загальному випадку АС складаються з наступних основних структурно-функціональних елементів:

- робочих станцій - окремих ЕОМ або віддалених терміналів мережі, на яких реалізуються автоматизовані робочі місця користувачів (абонентів, операторів);
- серверів або host машин (служб файлів, друку, баз даних тощо) не виділених (Або виділених, тобто не суміщених з робочими станціями) високопродуктивних ЕОМ, призначених для реалізації функцій зберігання, друку даних, обслуговування робочих станцій мережі і т.п. дій;
- міжмережевих мостів (шлюзів, центрів комутації пакетів, комунікаційних ЕОМ) - елементів, що забезпечують з'єднання декількох мереж передачі даних, або декількох сегментів однієї і тієї ж мережі, що мають різні протоколи взаємодії;
- каналів зв'язку (локальних, телефонних, з вузлами комутації і т.д.).

Робочі станції є найбільш доступними компонентами мереж і саме з них можуть бути зроблені найбільш численні спроби здійснення несанкціонованих дій. З робочих станцій здійснюється управління процесами обробки інформації, запуск програм, введення і коректування даних, на дисках робочих станцій можуть розміщуватися важливі дані і програми обробки. На відеомонітори та друкуючі пристрої робочих станцій виводиться інформація при роботі користувачів (операторів), що виконують різні функції і мають різні повноваження по доступу до даних і інших ресурсів системи. Імен але тому робочі станції повинні бути надійно захищені від доступу сторонніх осіб і затримати кошти розмежування доступу до ресурсів з боку законних

користувачів, мають різні повноваження. Крім того, засоби захисту повинні запобігати порушенням нормального налаштування робочих станцій і режимів їх функціонування, викликані ненавмисним втручанням недосвідчених (неуважних) користувачів.

Особового захисту потребують такі привабливі для зловмисників елементи мереж як сервери (host - машини) і мости. Перші - як концентратори великих обсягів інформації, другі - як елементи, в яких здійснюється перетворення (можливо через відкриту, нешифрований форму подання) даних при узгодженні протоколів обміну в різних ділянках мережі.

Сприятливою для підвищення безпеки серверів і мостів обставиною є, як правило, наявність можливостей по їх надійного захисту фізичними засобами і організаційними заходами в силу їх виділення, що дозволяє скоротити до мінімуму число осіб з персоналу мережі, що мають безпосередній доступ до них. Іншими словами, безпосередні випадкові впливи персоналу і навмисні дії зловмисників на виділенні сервери і мости можна вважати малоймовірними. У той же час, треба очікувати масованої атаки на сервери і мости з використанням засобів віддаленого доступу. Тут зловмисники насамперед можуть шукати можливості вплинути на роботу різних підсистем серверів і мостів, використовуючи недоліки протоколів обміну і засобів розмежування віддаленого доступу до ресурсів і системних таблиць. Використовуватися можуть всі можливості і засоби, від стандартних (без модифікації компонентів) до підключення спеціальних апаратних засобів (канали, як правило, слабо захищені від підключення) та застосування висококласних програм для подолання системи захисту.

Звичайно, сказане вище не означає, що не буде спроб впровадження апаратних і програмних закладок в самі мости і сервери, які відкривають додаткові широкі можливості з несанкціонованого віддаленого доступу. Закладки можуть бути впроваджені як з видалених станцій (за допомогою вірусів чи іншим способом), так і безпосередньо в апаратуру і програми серверів при їх ремонті, обслуговуванні, модернізації, перехід на нові версії

програмного забезпечення, зміні обладнання.

Канали і засоби зв'язку також потребують захисту. У силу великої просторової протяжності ліній зв'язку (через неконтрольовану або слабо контрольовану територію) практично завжди існує можливість підключення до них, або втручання в процес передачі даних. Можливі при цьому загрози детально викладені нижче.

2.4 Основні види загроз безпеки суб'єктів інформаційних відносин

Основними видами загроз безпеці АС та інформації (загроз інтересам суб'єктів інформаційних відносин) є:

- стихійні лиха і аварії (повінь, ураган, землетрус, пожежа тощо);
- збої і відмови устаткування (технічних засобів) АС;
- наслідки помилок проєктування та розробки компонентів АС (апаратних засобів, технології обробки інформації, програм, структур даних тощо);
- помилки експлуатації (користувачів, операторів та іншого персоналу);
- навмисні дії порушників і зловмисників (скривджених осіб з числа персоналу, злочинців, шпигунів, диверсантів і т.п.).

2.5 Класифікація загроз безпеки

Всі потенційні загрози за природою їх виникнення поділяється на два класи: природні (об'єктивні) і штучні (суб'єктивні) (рис.2.5).

Природні загрози - це загрози, викликані впливами на АС і її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози - це загрози АС, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

- ненавмисні (ненавмисні, випадкові) загрози, викликані помилками в проєктуванні АС та її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і т.п .;
- навмисні (навмисні) загрози, пов'язані з корисливими діями людей (зловмисників).

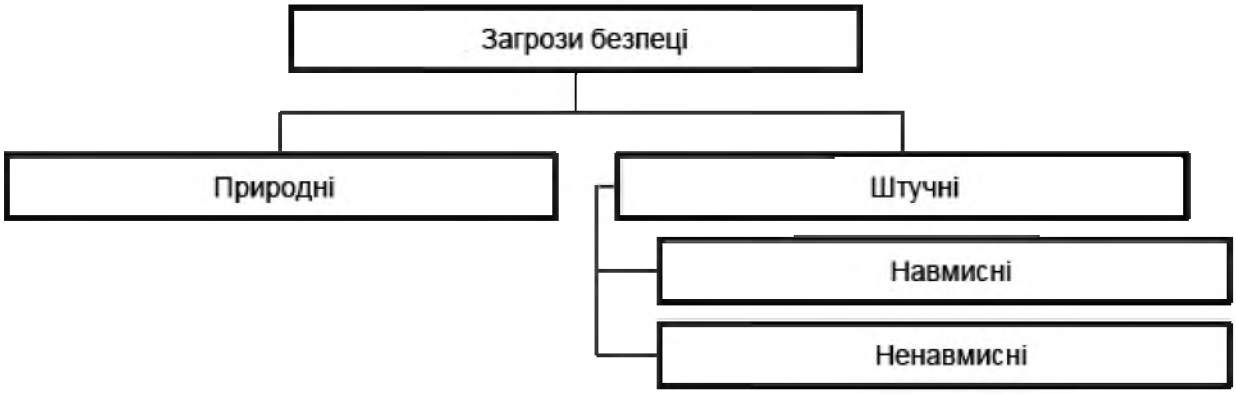


Рисунок 2.5 - Класифікація загроз безпеки

Джерела загроз по відношенню до АС можуть бути зовнішніми або внутрішніми (компоненти самої АС - її апаратура, програми, персонал).

Основні ненавмисні штучні загрози АС (дії, що здійснюються людьми випадково, через незнання, неуважність або недбалість, з цікавості, але без злого умислу):

1) ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисна псування устаткування, видалення, спотворення файлів з важливою інформацією або програм, у тому числі системних тощо);

2) неправомірне відключення устаткування або зміна режимів роботи пристроїв та програм;

3) ненавмисна псування носіїв інформації;

4) запуск технологічних програм, здатних при некомпетентне використанні викликати втрату працездатності системи (зависання або

зациклення) або здійснюють незворотні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних тощо);

5) нелегальне впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та ін., Які не є необхідними для виконання порушником своїх службових обов'язків) з наступним необґрунтованим витрачанням ресурсів (завантаження процесора, захоплення оперативної пам'яті і пам'яті на зовнішніх носіях);

6) зараження комп'ютера вірусами;

7) необережні дії, що призводять до розголошення конфіденційної інформації, або роблять її загальнодоступною;

8) розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, пропусків тощо);

9) проєктування архітектури системи, технології обробки даних, розробка прикладних програм, з можливостями, що представляють небезпеку для працездатності системи та безпеки інформації;

10) ігнорування організаційних обмежень (встановлених правил) при роботі в системі;

11) вхід в систему в обхід засобів захисту (завантаження сторонньої операційної системи зі змінних магнітних носіїв тощо);

12) некомпетентне використання, налаштування або неправомірне відключення засобів захисту персоналом служби безпеки;

13) пересилання даних за помилковою адресою абонента (пристрої);

14) введення помилкових даних;

15) ненавмисне пошкодження каналів зв'язку.

Основні можливі шляхи навмисної дезорганізації роботи, виведення системи з ладу, проникнення в систему і несанкціонованого доступу до інформації:

1) фізичне руйнування системи (шляхом вибуху, підпалу тощо) або виведення з ладу всіх або окремих найбільш важливих компонентів

комп'ютерної системи (пристроїв, носіїв важливої системної інформації, осіб з числа персоналу тощо);

2) відключення або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо);

3) дії по дезорганізації функціонування системи (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних радіозавад на частотах роботи пристроїв системи і т.п.);

4) впровадження агентів у число персоналу системи (у тому числі, можливо, і в адміністративну групу, відповідальну за безпеку);

5) вербування (шляхом підкупу, шантажу тощо) персоналу або окремих користувачів, які мають певні повноваження;

6) застосування підслуховуючих пристроїв, дистанційна фото- та відеозйомка і т.п .;

7) перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв та ліній зв'язку, а також наведень активних випромінювань на допоміжні технічні засоби, безпосередньо не беруть участь в обробці інформації (телефонні лінії, мережі живлення, опалення тощо);

8) перехоплення даних, переданих по каналах зв'язку, та їх аналіз з метою з'ясування протоколів обміну, правил входження в зв'язок і авторизації користувача і наступних спроб їх імітації для проникнення в систему;

9) розкрадання носіїв інформації (магнітних дисків, стрічок, мікросхем пам'яті, запам'ятовуючих пристроїв і цілих ПЕОМ);

10) несанкціоноване копіювання носіїв інформації;

11) розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації тощо);

12) читання залишкової інформації з оперативної пам'яті і з зовнішніх запам'ятовуючих пристроїв;

13) читання інформації з областей оперативної пам'яті, використовуваних операційною системою (у тому числі підсистемою захисту)

або іншими користувачами, в асинхронному режимі використовуючи недоліки мультизадачних операційних систем і систем програмування;

14) незаконне одержання паролів та інших реквізитів розмежування доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбору, шляхом імітації інтерфейсу системи тощо) з наступною маскуванням під зареєстрованого користувача ("маскарад");

15) несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізичну адресу, адресу в системі зв'язку, апаратний блок кодування і т.п .;

16) розтин шифрів криптозахисту інформації;

17) впровадження апаратних спецвложеній, програмних "закладок" і "вірусів" ("троянських коней" та "жучків"), тобто таких ділянок

програм, які не потрібні для здійснення заявлених функцій, але дозволяють долати систему захисту, потай і незаконно здійснювати доступ до системних ресурсів з метою реєстрації та передачі критичної інформації або дезорганізації функціонування системи;

18) незаконне підключення до ліній зв'язку з метою роботи "між рядків", з використанням пауз в діях законного користувача від його імені з наступним введенням помилкових повідомлень або модифікацією переданих повідомлень;

19) незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його фізичного відключення після входу в систему та успішної аутентифікації з наступним введенням дезінформації та нав'язуванням помилкових повідомлень.

Слід зауважити, що найчастіше для досягнення поставленої мети зловмисник використовує не один, а деяку сукупність з перерахованих вище шляхів.

2.6 Класифікація каналів проникнення в систему і витоку інформації

Всі канали проникнення в систему і витоку інформації поділяють на прямі і непрямі. Під непрямими розуміють такі канали, використання яких не вимагає проникнення в приміщення, де розташовані компоненти системи. Для використання прямих каналів таке проникнення необхідно. Прямі канали можуть використовуватися без внесення змін до компоненти системи або зі змінами компонентів.

За типом основного засобу, який використовується для реалізації загрози всі можливі канали можна умовно розділити на три групи, де такими засобами є: людина, програма або апаратура. Класифікація видів порушень працездатності систем і несанкціонованого доступу до інформації по об'єктах впливу і способам нанесення шкоди безпеці приведена в таблиці 2.1.

За способом отримання інформації потенційні канали доступу можна розділити на:

- фізичний;
- електромагнітний (перехоплення випромінювань);
- інформаційний (програмно-математичний).

При контактному НСД (фізичному, програмно-математичному) можливі загрози інформації реалізуються шляхом доступу до елементів АС, до носіїв інформації, до самої вводиться і виводиться інформації (і результатами), до програмного забезпечення (у тому числі до операційних систем), а також шляхом підключення до ліній зв'язку.

При безконтактному доступі (наприклад, по електромагнітному каналу) можливі загрози інформації реалізуються перехопленням випромінювань апаратури АС, у тому числі наводяться в струмопровідних комунікаціях і ланцюгах харчування, перехопленням інформації в лініях зв'язку, введенням в лінії зв'язку неправдивої інформації, візуальним спостереженням (фотографуванням) пристроїв відображення інформації, прослуховуванням переговорів персоналу АС і користувачів.

Таблиця 2.1 - Класифікація видів порушень працездатності систем і несанкціонованого доступу до інформації по об'єктах впливу і способам нанесення шкоди безпеці

Способи нанесення збитку	Об'єкти впливів			
	Обладнання	Програми	Дані	Персонал
Розкриття (витік) інформації	Розкрадання носіїв інформації, підключення до лінії зв'язку, несанкціоноване використання ресурсів	Несанкціоноване копіювання перехоплення	Розкрадання, копіювання, перехоплення	Передача відомостей про захист, розголошення, недбалість
Втрата цілісності інформації	Підключення, модифікація, зміна режимів роботи, несанкціоноване використання ресурсів	Впровадження "троянських коней" та "жучків"	Спотворення, модифікація	Вербовка персоналу, "маскарад"
Порушення працездатності автоматизованої системи	Зміна режимів функціонування, виведення з ладу, розкрадання, руйнування	Спотворення, видалення, підміна	Спотворення, видалення, нав'язування помилкових даних	Догляд, фізичне усунення
Незаконне тиражування (відтворення) інформації	Виготовлення аналогів без ліцензій	Використання незаконних копій	Публікація без відома авторів	

Злочини, в тому числі і комп'ютерні, відбуваються людьми. Користувачі системи та її персонал, з одного боку, є складовою частиною, необхідним елементом АС. З іншого боку, вони ж є основною причиною і рушійною силою порушень і злочинів. У цьому сенсі питання безпеки автоматизованих систем є суть питання людських відносин і людської поведінки.

2.7 Опис деяких актуальних загроз інформації для АС класу 2

2.7.1 Загрози витоку інформації технічними каналами

Загрози витоку інформації технічними каналами:

1) загрози витоку акустичної (мовної) інформації. Виникнення загроз витоку акустичної (мовної) інформації, що міститься безпосередньо в

виголошуваної мови користувача ІСПДн, при обробці ПДн в ІСПДн, можливо при наявності функцій голосового введення ПДн в ІСПДн або функцій відтворення ПДн акустичними засобами ІСПДн;

2) загрози витоку видової інформації. Реалізація загрози витоку видової інформації можлива за рахунок перегляду інформації за допомогою оптичних (оптико-електронних) засобів з екранів дисплеїв і інших засобів відображення засобів обчислювальної техніки, інформаційно-обчислювальних комплексів, технічних засобів обробки графічної, відео та буквено-цифрової інформації, входящіх до складу ІСПДн;

3) загрози витоку інформації каналами ПЕМВН. Загрози витоку інформації по каналу ПЕМВН, можливі через наявність паразитних електромагнітних випромінювань у елементів ІСПДн. Загрози даного класу малоймовірні, тому розмір контрольованої зони великий, і елементи ІСПДн, знаходяться в на великій відстані від її кордону й екрануються декількома несучими стінами, і паразитний сигнал маскується з безліччю інших паразитних сигналів елементів, що не входять в ІСПДн.

2.7.2 Загрози несанкціонованого доступу до інформації

Реалізація загроз НСД до інформації може призводити до наступних видів порушення її безпеки:

- порушення конфіденційності (копіювання, неправомірне поширення);
- порушення цілісності (знищення, зміна);
- порушення доступності (блокування).

Загрози знищення, розкрадання апаратних засобів ІСПДн носіїв інформації шляхом фізичного доступу до елементів ІСПДн:

1) крадіжка ПЕОМ. Загроза здійснюється шляхом НСД зовнішніми і внутрішніми порушниками в приміщення, де розташовані елементи ІСПДн;

2) крадіжка носіїв інформації. Загроза здійснюється шляхом НСД зовнішніми і внутрішніми порушниками до носіїв інформації;

3) крадіжка ключів і атрибутів доступу. Загроза здійснюється шляхом НСД зовнішніми і внутрішніми порушниками в приміщення, де відбувається робота користувачів;

4) кражі, модифікації, знищення інформації. Загроза здійснюється шляхом НСД зовнішніми і внутрішніми порушниками в приміщення, де розташовані елементи ІСПДн та засоби захисту, а так само відбувається робота користувачів;

5) висновок з ладу вузлів ПЕОМ, каналів зв'язку. Загроза здійснюється шляхом НСД зовнішніми і внутрішніми порушниками в приміщення, де розташовані елементи ІСПДн і проходять канали зв'язку;

6) несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищення) вузлів ПЕОМ;

7) несанкціоноване відключення засобів захисту. Загроза здійснюється шляхом НСД зовнішніми і внутрішніми порушниками в приміщення, де розташовані засоби захисту ІСПДн.

Загрози розкрадання, несанкціонованої модифікації або блокування інформації за рахунок несанкціонованого доступу (НСД) із застосуванням програмно-апаратних і програмних засобів (в тому числі програмно-математичних впливів):

1) дії шкідливих програм (вірусів). Програмно-математичне вплив - це вплив за допомогою шкідливих програм. Програмою з потенційно небезпечними наслідками або шкідливою програмою (вірусом) називають деяку самостійну програму (набір інструкцій), що здатна виконувати будь-яке непорожнє підмножина таких функцій:

- приховувати ознаки своєї присутності в програмному середовищі комп'ютера;
- мати здатність до самодублірованію, ассоциированию себе з іншими програмами та (або) переносу своїх фрагментів в інші області оперативної або зовнішньої пам'яті;

- руйнувати (спотворювати довільним чином) код програм в оперативної пам'яті;

- виконувати без ініціювання з боку користувача (користувальницької програми в штатному режимі її виконання) деструктивні функції (копіювання, знищення, блокування тощо);

- зберігати фрагменти інформації з оперативної пам'яті в деяких областях зовнішньої пам'яті прямого доступу (локальних або віддалених);

- спотворювати довільним чином, блокувати і (або) підміняти виведений в зовнішню пам'ять або в канал зв'язку масив інформації, утворився в результаті роботи прикладних програм, або вже знаходяться в зовнішній пам'яті масиви даних.

2) декларованих можливостей системного ПЗ та ПЗ для обробки персональних даних. Декларованих можливостей - функціональні можливості засобів обчислювальної техніки, не описані або не відповідають описаним у документації, при використанні яких можливе порушення конфіденційності, доступності або цілісності оброблюваної інформації.

3) установка ПО не пов'язаного з виконанням службових обов'язків. Загроза здійснюється шляхом несанкціонованого встановлення ПО внутрішніми порушниками, що може призвести до порушення конфіденційності, цілісності та доступності всієї ІСПДн або її елементів.

2.7.3 Загрози не навмисних дій користувачів і порушень безпеки функціонування ІСПДн і СЗПДн

Нижче розглянуті загрози не навмисних дій користувачів і порушень безпеки функціонування ІСПДн і системи захисту персональних даних (далі - СЗПДн) в її складі через збої в програмному забезпеченні, а також від погроз неантропогенного (збоїв апаратури через ненадійність елементів, збоїв електроживлення) і стихійного (ударів блискавок, пожеж, повеней тощо) характеру:

1) втрата ключів і атрибутів доступу. Загроза здійснюється за рахунок дії людського фактора користувачів ІСПДн, які порушують

положення пральний політиці в частині їх створення (створюють легкі або порожні паролі, не змінюють паролі після закінчення терміну їх життю або компрометації тощо) та зберігання (записують паролі на паперові носії , передають ключі доступу третім особам тощо) або не обізнані про них;

2) ненавмисна модифікація (знищення) інформації співробітниками. Загроза здійснюється за рахунок дії людського фактора користувачів ІСПДн, які порушують положення прийнятих правил роботи з ІСПДн або не обізнані про них;

3) ненавмисне відключення засобів захисту. Загроза здійснюється за рахунок дії людського фактора користувачів ІСПДн, які порушують положення прийнятих правил роботи з ІСПДн і засобами захисту або не обізнані про них;

4) вихід з ладу апаратно-програмних засобів. Загроза здійснюється внаслідок недосконалості апаратно-програмних засобів, через які може відбуватися порушення цілісності та доступності інформації, що захищається;

5) збій системи електропостачання. Загроза здійснюється внаслідок недосконалості системи електропостачання, через що може відбуватися порушення цілісності та доступності інформації, що захищається;

6) стіхійное лихо. Загроза здійснюється внаслідок недотримання заходів пожежної безпеки.

2.7.4 Загрози навмисних дій внутрішніх порушників

Загрози навмисних дій внутрішніх порушників:

1) доступ до інформації, модифікація, знищення осіб, не допущених до її обробці. Загроза здійснюється шляхом НСД зовнішніх порушників у приміщення, де розташовані елементи ІСПДн та засоби захисту, а так само відбувається робота користувачів;

2) розголошення інформації, модифікація, знищення співробітниками допущеними до її обробці. Загроза здійснюється за рахунок

дії людського фактора користувачів ІСПДн, які порушують положення про нерозголошення оброблюваної інформації або не обізнані про них.

2.7.5 Загрози несанкціонованого доступу по каналах зв'язку

Загроза «Аналіз мережевого трафіку». Ця загроза реалізується за допомогою спеціальної програми-аналізатора пакетів (sniffer), перехоплює всі пакети, що передаються по сегменту мережі, і виділяє серед них ті, в яких передаються ідентифікатор користувача і його пароль. У ході реалізації загрози порушник:

- вивчає логіку роботи ІСПДн - тобто прагне отримати однозначну відповідність подій, що відбуваються в системі, і команд, пересланих при цьому хостами, в момент появи даних подій. Надалі це дозволяє зловмисникові на основі завдання відповідних команд отримати, наприклад, привілейовані права на дії в системі або розширити свої повноваження в ній;

- перехоплює потік переданих даних, якими обмінюються компоненти мережевої операційної системи, для вилучення конфіденційної або ідентифікаційної інформації (наприклад, статичних паролів користувачів для доступу до віддалених хостів по протоколах FTP і TELNET, які не передбачають шифрування), її підміни, модифікації та т.п.

Загроза «сканування мережі». Сутність процесу реалізації загрози полягає в передачі запитів мережних служб хостів ІСПДн та аналізі відповідей від них. Мета - виявлення використовуваних протоколів, доступних портів мережевих служб, законів формування ідентифікаторів з'єднань, визначення активних мережевих сервісів, підбір ідентифікаторів і паролів користувачів.

Загроза виявлення паролів. Мета реалізації загрози полягає в отриманні НСД шляхом подолання парольного захисту. Зловмисник може реалізовувати загрозу за допомогою цілого ряду методів, таких як простий перебір, перебір з використанням спеціальних словників, установка шкідливої програми для перехоплення пароля, підміна довіреного об'єкта мережі (IP-spoofing) і перехоплення пакетів (sniffing). В основному для реалізації загрози

використовуються спеціальні програми, які намагаються отримати доступ хосту шляхом послідовність підбору паролів. У разі успіху, зловмисник може створити для себе «прохід» для майбутнього доступу, який діятиме, навіть якщо на хості змінити пароль доступу.

Загрози нав'язування помилкового маршруту мережі. Дана загроза реалізується одним із двох способів: шляхом внутрисегментного або міжсегментного нав'язування. Можливість нав'язування хибного маршруту обумовлена недоліками, притаманними алгоритмам маршрутизації (зокрема через проблеми ідентифікації мережевих керуючих пристроїв), в результаті чого можна потрапити, наприклад, на хост або в мережу зловмисника, де можна увійти в операційну середу технічного засобу у складі ІСПДн. Реалізації загрози ґрунтується на несанкціонованому використанні протоколів маршрутизації (RIP, OSPF, LSP) та управління мережею (ICMP, SNMP) для внесення змін до маршрутно-адресні таблиці. При цьому порушникові необхідно надіслати від імені мережевого керуючого пристрою (наприклад, маршрутизатора) керуюче повідомлення.

Загрози підміни довіреного об'єкта. Така загроза ефективно реалізується в системах, в яких застосовуються нестійкі алгоритми ідентифікації і аутентифікації хостів, користувачів і т.д. Під довіреним об'єктом розуміється об'єкт мережі (комп'ютер, міжмережевий екран, маршрутизатор тощо), легально підключений до сервера.

Можуть бути виділені два різновиди процесу реалізації вказаної загрози: з встановленням і без встановлення віртуального з'єднання.

Процес реалізації з встановленням віртуального з'єднання складається у привласненні прав довіреної суб'єкта взаємодії, що дозволяє порушнику вести сеанс роботи з об'єктом мережі від імені довіреної суб'єкта. Реалізація загрози даного типу вимагає подолання системи ідентифікації аутентифікації повідомлень (наприклад, атака rsh-служби UNIX-хоста).

Процес реалізації загрози без встановлення віртуального з'єднання може мати місце в мережах, що здійснюють ідентифікацію переданих повідомлень

тільки за мережевою адресою відправника. Суть полягає в передачі службових повідомлень від імені мережевих керуючих пристроїв (наприклад, від імені маршрутизаторів) про зміну маршрутно-адресних даних.

Впровадження помилкового об'єкта мережі. Ця загроза полягає в використанні недоліків алгоритмів віддаленого пошуку. У разі якщо об'єкти мережі спочатку не мають адресної інформації один про одного, використовуються різні протоколи віддаленого пошуку (наприклад, SAP в мережах Novell NetWare; ARP, DNS, WINS в мережах зі стеком протоколів TCP / IP), які полягають у передачі по мережі спеціальних запитів та отриманні на них відповідей з шуканої інформацією. При цьому існує можливість перехоплення порушником пошукового запиту і видачі на нього помилкового відповіді, використання якого призведе до необхідного зміненню маршрутно-адресних даних. Надалі весь потік інформації, асоційований з об'єктом-жертвою, проходитиме через хибний об'єкт мережі.

Загрози типу «Відмова в обслуговуванні». Ці загрози засновані на недоліках мережевого програмного забезпечення, його вразливості, що дозволяють порушнику створювати умови, коли операційна система виявляється не в змозі обробляти вступники пакети.

Можуть бути виділені кілька різновидів таких загроз:

- прихована відмова в обслуговуванні, викликана залученням частини ресурсів ІСПДн на обробку пакетів, що передаються зловмисником зі зниженням пропускної спроможності каналів зв'язку, ефективності мережевих пристроїв, порушенням вимог до часу обробки запитів. Прикладами реалізації загроз подібного роду можуть служити: спрямований шторм луна-запитів по протоколу ICMP (Ping flooding), шторм запитів на установлене TCP-з'єднань (SYN-flooding), шторм запитів до FTP-сервера;

- явна відмова в обслуговуванні, викликаний вичерпанням ресурсів ІСПДн при обробці пакетів, що передаються зловмисником (заняття всієї смуги пропускання каналів зв'язку, переповнення черг запитів на обслуговування), при якому легальні запити не можуть бути передані через

мережу через недоступність середовища передачі, або отримують відмову в обслуговування зважаючи переповнення черг запитів, дискового простору пам'яті і т.д. Прикладами загроз даного типу можуть служити шторм широкомовних ICMP-exo-запитів (Smurf), спрямований шторм (SYN-flooding), шторм повідомлень поштового сервера (Spam);

- явна відмова в обслуговуванні, викликаний порушенням логічної зв'язності між технічними засобами ІСПДн при передачі порушником керуючих повідомлень від імені мережевих пристроїв, що призводять до зміни маршрутно-адресних даних (наприклад, ICMP Redirect Host, DNS-flooding) або ідентифікаційної та аутентифікаційної інформації;

- явна відмова в обслуговуванні, викликаний передачею зловмисником пакетів з нестандартними атрибутами (погрози типу «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») або мають довжину, що перевищує максимально допустимий розмір (погроза типу «Ping Death»), що може призвести до збою мережевих пристроїв, що беруть участь в обробці запитів, за умови наявності помилок в програмах, що реалізують протоколи мережевого обміну.

Результатом реалізації даної загрози може стати порушення працездатності відповідної служби надання віддаленого доступу до ПДН в ІСПДн, передача з однієї адреси такої кількості запитів на підключення до технічного засобу у складі ІСПДн, яке максимально може «вмістити» трафік (спрямований «шторм запитів »), що тягне за собою переповнення черги запитів і відмова однієї з мережевих служб або повна зупинка ІСПДн через неможливість системи займатися нічим іншим, крім обробки запитів.

Загрози віддаленого запуску додатків. Загроза полягає в прагненні запустити на хості ІСПДн різні попередньо впроваджені шкідливі програми: програми-закладки, віруси, «мережеві шпигуни», основна мета яких - порушення конфіденційності, цілісності, доступності інформації і повний контроль за роботою хоста. Крім того, можливий несанкціонований запуск прикладних програм користувачів для несанкціонованого отримання

необхідних порушнику даних, для запуску керованих прикладної програмою процесів та ін.

Виділяють три підкласу даних загроз:

- поширення файлів, що містять несанкціонований виконуваний код;
- віддалений запуск програми шляхом переповнення буфера додатків -серверів;
- віддалений запуск програми шляхом використання можливостей віддаленого управління системою, що надаються прихованими програмними і апаратними закладками, або використовуваними штатними засобами.

Типові загрози першого із зазначених підкласів ґрунтуються на активізації поширюваних файлів при випадковому зверненні до них. Прикладами таких файлів можуть служити: файли, що містять виконуваний код в вид документи, що містять виконуваний код у вигляді елементів ActiveX, Java-аплетів, інтерпретованих скриптів (наприклад, тексти на JavaScript); файли, що містять виконувані коди програм. Для поширення файлів можуть використовуватися служби електронної пошти, передачі файлів, мережевий файлової системи.

При погрозах другого підкласу використовуються недоліки програм, що реалізують мережеві сервіси (зокрема, відсутність контролю за переповненням буфера). Налаштуванням системних регістрів іноді вдається переключити процесор після переривання, викликаного переповненням буфера, на виконання коду, що міститься за кордоном буфера. Прикладом реалізації такої загрози може служити впровадження широко відомого «вірусу Морріса».

При погрозах третього підкласу порушник використовує можливості віддаленого управління системою, що надаються прихованими компонентами (наприклад, «троянські» програми типу Back. Orifice, Net Bus), або штатними засобами управління та адміністрування комп'ютерних мереж (Landesk Management Suite, Managewise, Back Orifice і т.п.). У результаті їх

використання вдається домогтися віддаленого контролю над станцією в мережі.

Загрози впровадження по мережі шкідливих програм. До шкідливим програмам, що впроваджуються по мережі, відносяться віруси, які для свого поширення активно використовують протоколи і можливості локальних і глобальних мереж. Основним принципом роботи мережного вірусу є можливість самостійно передати свій код на віддалений сервер або робочу станцію. «Повноцінні» мережні віруси при цьому володіють ще і можливістю запустить на виконання свій код на віддаленому комп'ютері або, принаймні, "підштовхнути" користувача до запуску зараженого файлу.

Шкідливими програмами, що забезпечують здійснення НСД, можуть бути:

- програми підбору і розтину паролів;
- програми, що реалізують загрози;
- програми, що демонструють використання декларованих можливостей програмного і програмно-апаратного забезпечення ІСПДн;
- програми-генератори комп'ютерних вірусів;
- програми, що демонструють уразливості засобів захисту інформації та ін.

2.8 Етапи роботи СППР для моделювання загроз інформації для АС класу 2

Етапи роботи системи:

1) реєстрація нового об'єкта дослідження, визначається повний список інформаційних ресурсів, які мають цінність для об'єкта;

2) введення в систему всіх видів інформації, що представляє цінність для об'єкта;

3) визначення всіх видів користувальницьких груп. Потім визначається, до яких груп інформації на ресурсах має доступ кожна з груп

користувачів. На закінчення визначаються види (локальний і / або віддалений) і права (читання, запис, видалення) доступу користувачів до всіх ресурсів, що містять цінну інформацію;

4) введення в систему всього програмно-апаратного комплексу, який використовується в АС;

5) на завершальному етапі користувач повинен відповісти на список питань з політики безпеки, реалізованої в системі, що дозволяє оцінити реальний рівень захищеності системи і деталізувати оцінки загроз;

6) по закінченню відповідей на питання сформована повна модель загроз інформації з точки зору інформаційної безпеки з урахуванням реального виконання вимог комплексної політики безпеки.

2.9 Алгоритм СППР для моделювання загроз інформації для ас класу 2

Запропонована блок-схема алгоритму роботи системи підтримки прийняття рішення для моделювання загроз інформації для АС класу 2 на рисунку 2.6, після аналізу та обробки даних має видати звіт у вигляді моделі загроз для АС.

Даний алгоритм дозволяє зробити початкову оцінку системи захисту АС класу 2 і побудує попередню модель загроз для даної АС.

2.10 Список питань з політики безпеки, реалізованої в СППР для моделювання загроз інформації для АС класу 2

Список питань з політики безпеки для користувача АС:

1) Че є функції голосового введення даних в АС або функцій відтворення даних акустичними засобами АС?

2) Чи можливий візуальний перегляд сторонніми особами інформації на моніторі?

3) Чи є контроль доступу в контрольовану зону?

4) Введений цілодобовий контроль доступу в контрольовану зону?

5) Чи можливий винос комп'ютерний техніки за межі будівлі?

6) Чи ведеться облік і зберігання носіїв інформації?

7) Чи організоване зберігання ключів і паролів в сейфі і введена політика «чистого столу»?

8) Чи проінструктовані користувачі АС про роботу з ПДн та іншими даними?

9) Че є функції голосового введення даних в АС або функцій відтворення даних акустичними засобами АС?

10) Чи можливий візуальний перегляд сторонніми особами інформації на моніторі?

11) Чи є контроль доступу в контрольовану зону?

12) Введений цілодобовий контроль доступу в контрольовану зону?

13) Чи можливий винос комп'ютерний техніки за межі будівлі?

14) Чи ведеться облік і зберігання носіїв інформації?

15) Чи організоване зберігання ключів і паролів в сейфі і введена політика «чистого столу»?

16) Чи проінструктовані користувачі АС про роботу з ПДн та іншими даними?

17) Технічне обслуговування АС здійснюється співробітниками, які підписали угоду про нерозголошення?

18) На всіх елементах АС встановлений антивірусний захист?

19) Користувачі проінструктовані про заходи запобігання вірусного зараження?

20) Розробку та супровід програмного забезпечення АС здійснює довірена організація?

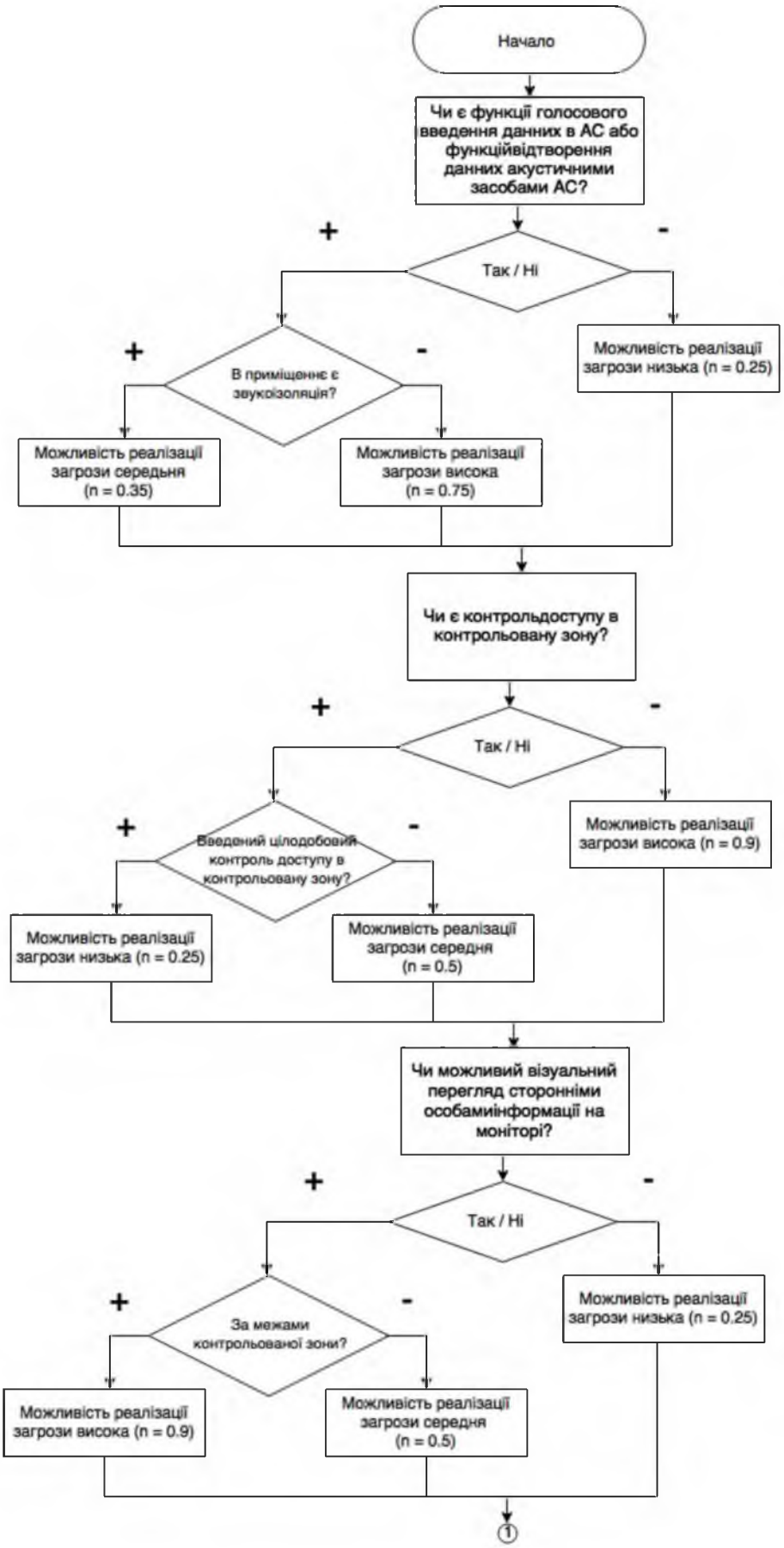
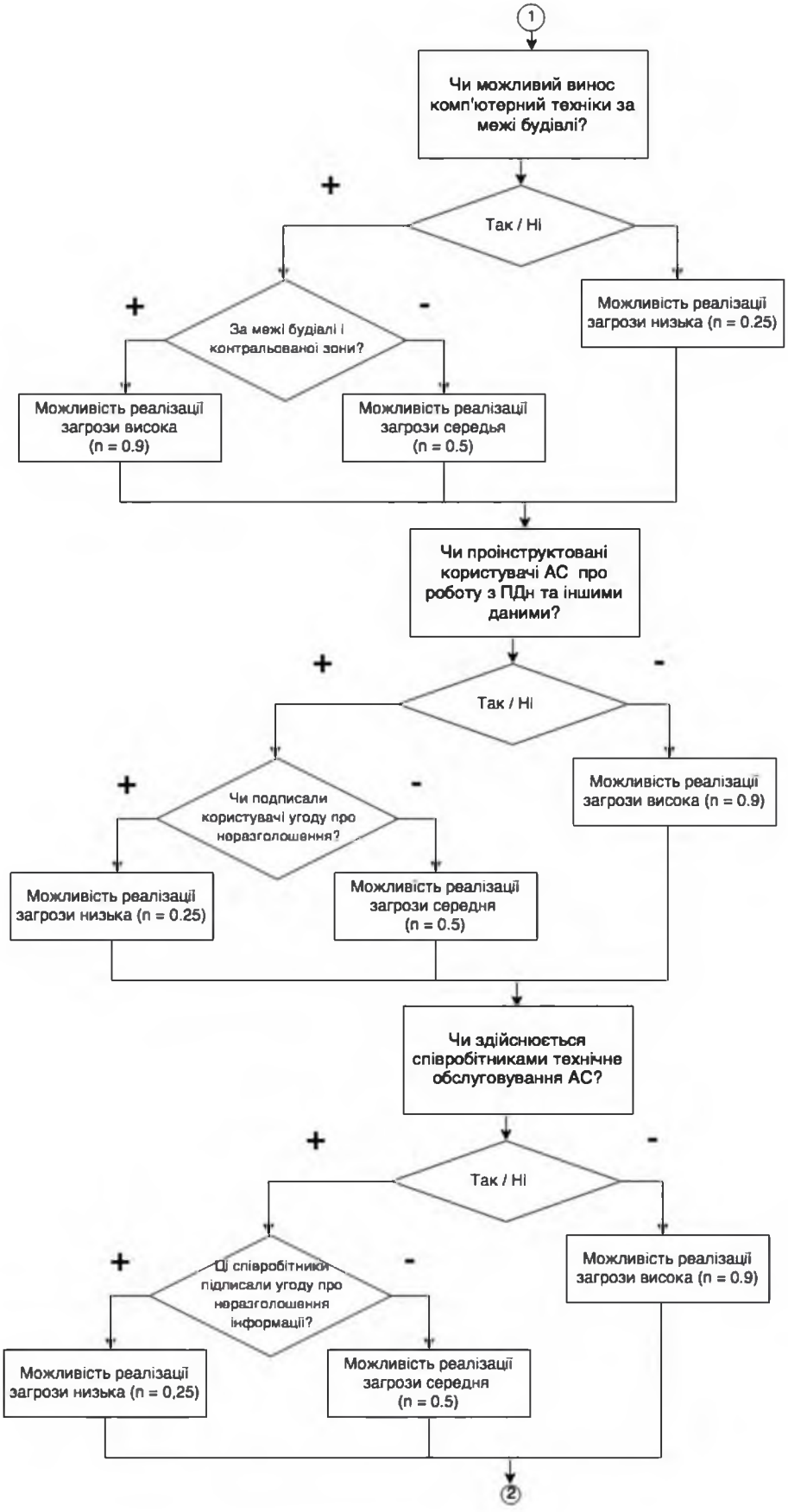
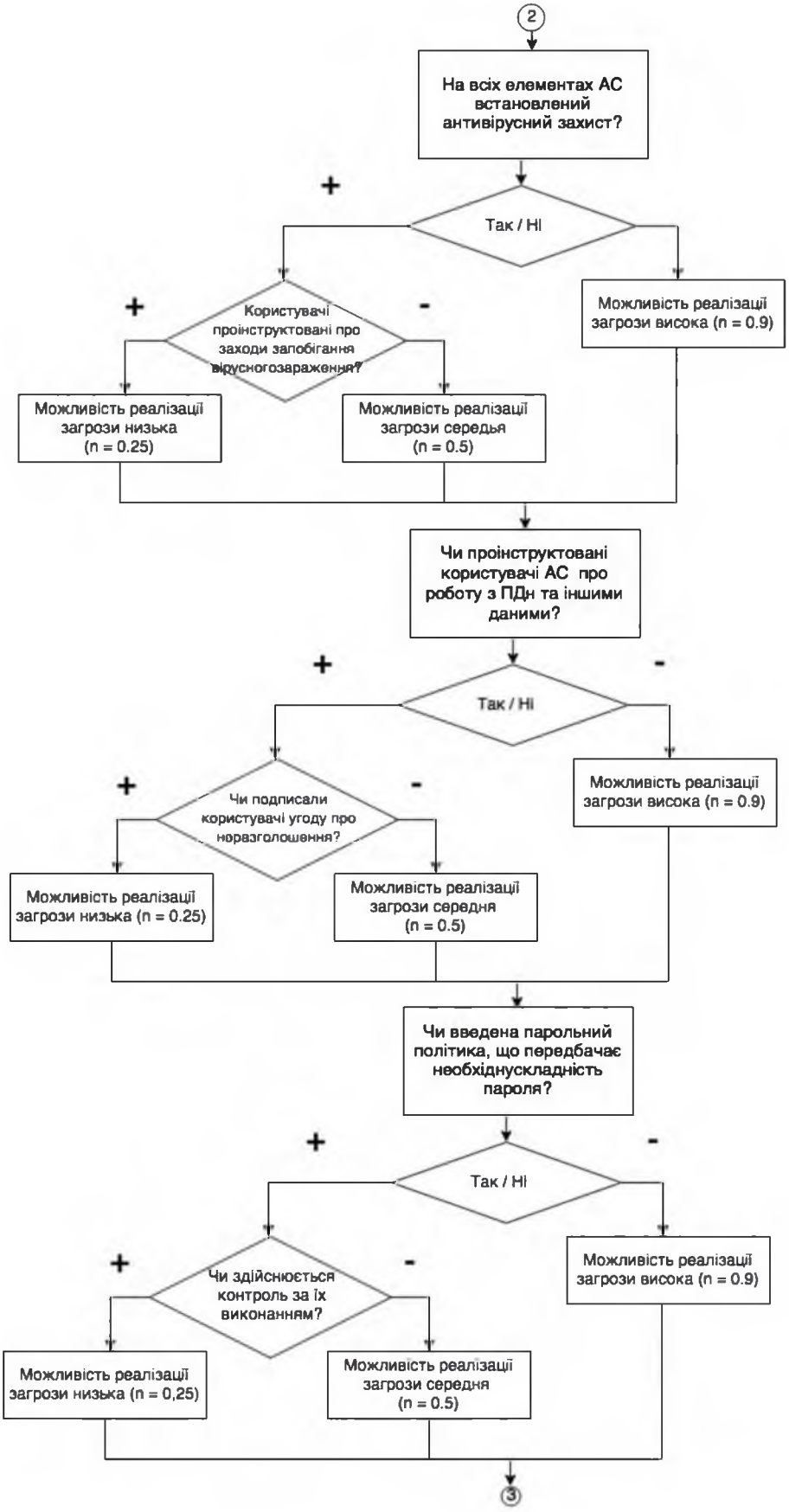


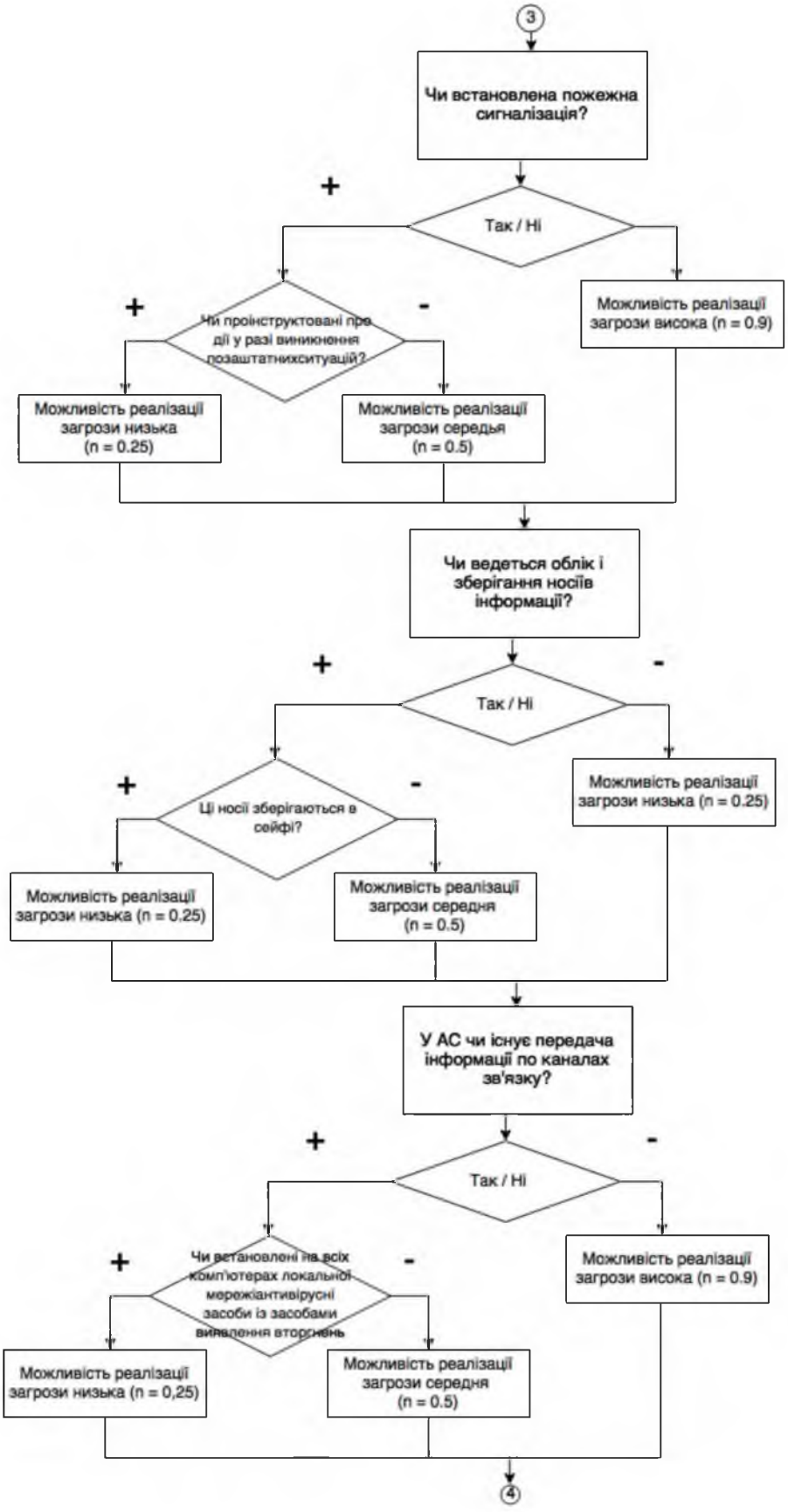
Рисунок 2.6-Алгоритм СППР для моделювання загроз інформації



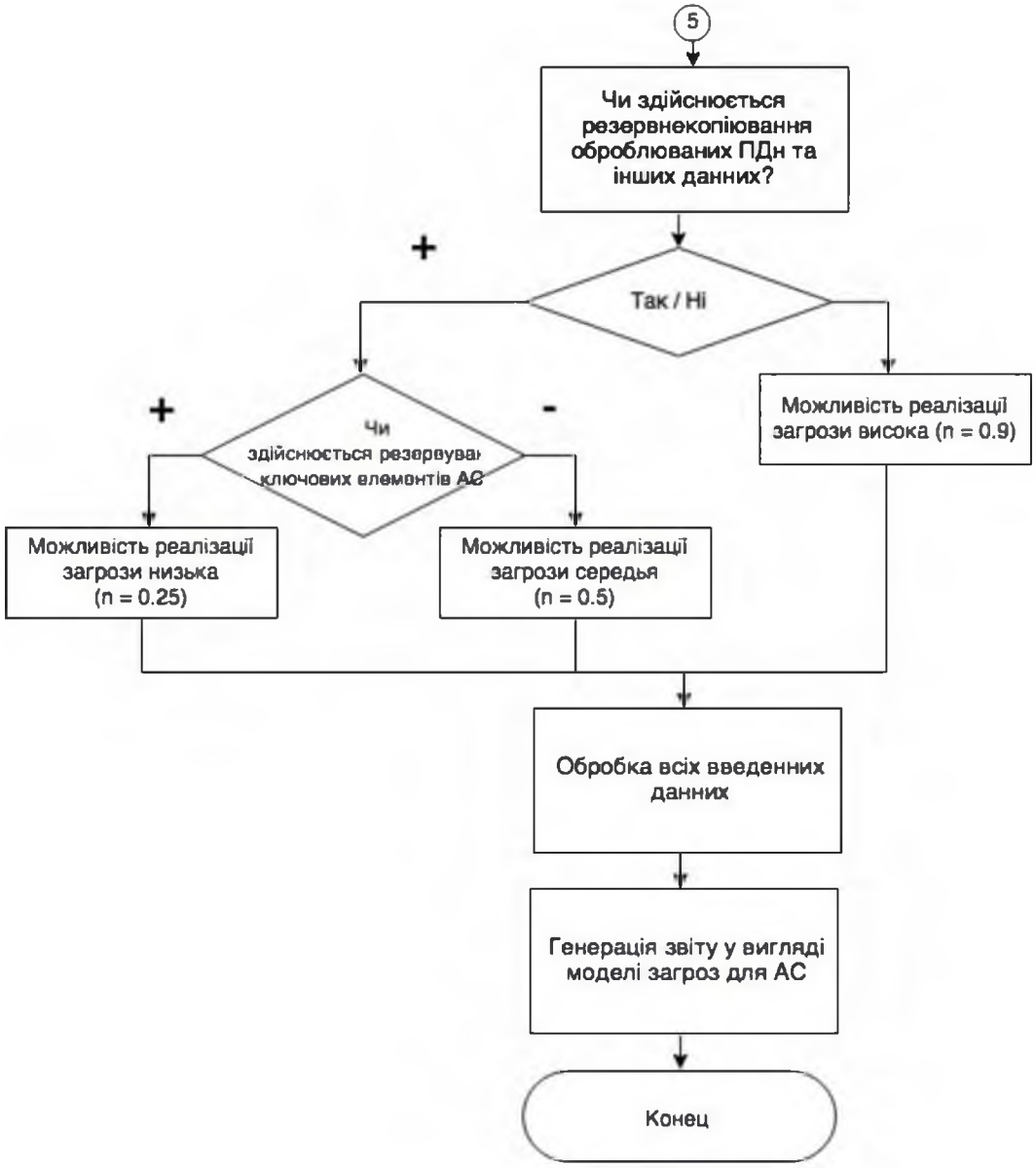
Продовження рисунку 2.6-Алгоритм СППР для моделювання загроз інформації



Продовження рисунку 2.6-Алгоритм СППР для моделювання загроз інформації



Продовження рисунку 2.6-Алгоритм СППР для моделювання загроз інформації



Продовження рисунку 2.6-Алгоритм СППР для моделювання загроз інформації

21) Чи введена парольний політика, що передбачає необхідну складність пароля, здійснюється контроль за їх виконанням?

22) Користувачі проінструктовані про порольну політику і про дії у випадках втрати або компрометації паролів?

23) Чи здійснюється резервне копіювання оброблюваних ПДн та інших даних?

24) Чи здійснюється розмежування доступу до налаштувань режимів засобів захисту?

25) Здійснюється резервування ключових елементів АС?

26) Чи підключені до всіх ключових елементів АС джерела безперебійного живлення?

27) Чи встановлена пожежна сигналізація?

28) Користувачі проінструктовані про дії у разі виникнення позаштатних ситуацій?

29) Чи інформовані користувачі про порядок роботи з даними, а так само підписали Угоду про нерозголошення?

30) У АС чи існує передача інформації по каналах зв'язку?

31) Чи застосовуються стійкі паролі?

32) Чи встановлені на всіх комп'ютерах локальної мережі антивірусні засоби із засобами виявлення вторгнень?

2.11 Приклад моделі загроз для автоматизованої системи класу 2

Нижче в таблиці 2.2 наведений приклад генерації моделі загроз для АС класу 2

Таблиця 2.2 – Приклад генерації моделі загроз

Найменування загрози	Реалізованість загроз	
	Коефіцієнт реалізованості загрози (n)	Коефіцієнт реалізованості загрози
1 Загрози щодо витоку через технічні канали		
1.1 Загроза витоку акустичних інформації	0.25	низька
1.2 Загрози витоку видової інформації	0.25	низька
1.3 Загрози витоку інформації каналами ПЕМВН	0.25	низька
2 Загрози несанкціонованого доступу до інформації.		
2.1 Загрози знищення, розкрадання апаратних засобів ІСПДн носіїв інформації шляхом фізичного доступу до елементів ІСПДн		
2.1.1 Крадіжка ПЕОМ	0.25	низька
2.1.2 Крадіжка носіїв інформації	0.35	середня
2.1.3 Крадіжка ключів і атрибутів доступу	0.35	середня
2.1.4 Крадіжки, модифікації, знищення інформації	0.25	низька
2.1.5 Висновок з ладу вузлів ПЕОМ, каналів зв'язку	0.25	низька

2.1.6 Несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищення) вузлів ПЕОМ	0.5	середня
2.1.7 Несанкціоноване відключення засобів захисту	0.5	середня
2.2 Загрози розкрадання, несанкціонованої модифікації або блокування інформації за рахунок несанкціонованого доступу (НСД) із застосуванням програмно-апаратних і програмних засобів (в тому числі програмно-математичних впливів).		
2.2.1 Дії шкідливих програм (вірусів)	0.75	висока
2.2.2 Декларованих можливостей системного ПЗ та ПЗ для обробки персональних даних	0.25	низька
2.2.3 Установка ПЗ не пов'язаного з виконанням службових обов'язків	0.25	низька
2.3 Загрози не навмисних дій користувачів і порушень безпеки функціонування ІСПДн і СЗПДн в її складі через збої в програмному забезпеченні, а також від погроз неантропогенного (збоїв апаратури через ненадійність елементів, збоїв електроживлення) і стихійного (ударів блискавок, пожеж, повеней та т.п.) характеру.		
2.3.1 Втрата ключів і атрибутів доступу	0.25	низька
2.3.2 Ненавмисна модифікація (знищення) інформації співробітниками	0.25	низька
2.3.3 Ненавмисне відключення засобів захисту	0.35	середня
2.3.4 Вихід з ладу апаратно-програмних засобів	0.25	низька
2.3.5 Збій системи електропостачання	0.25	низька
2.3.6 Стихійне лихо	0.25	низька
2.4. Загрози навмисних дій внутрішніх порушників		
2.4.1 Доступ до інформації, модифікація, знищення осіб не допущених до її обробці	0.25	низька
2.4.2 Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробці	0.25	низька
2.5 Загрози несанкціонованого доступу по каналах зв'язку.		
2.5.1 Загроза «Аналіз мережевого трафіку» з перехопленням передається з ІСПДн і прийнятої із зовнішніх мереж інформації:	0.25	низька
2.5.1.1 Перехоплення за переділами з контрольованої зони	0.25	низька
2.5.1.2 Перехоплення в межах контрольованої зони зовнішніми порушниками	0.25	низька
2.5.1.3 Перехват в межах контрольованої зони внутрішніми порушниками	0.25	низька
2.5.2 Загрози сканування, спрямовані на виявлення типу або типів використовуваних операційних систем, мережевих адрес робочих станцій ІСПДн, топології мережі, відкритих портів і служб, відкритих з'єднань та ін.	0.35	висока
2.5.4 Загрози нав'язування помилкового маршруту мережі	0.25	низька
2.5.5 Загрози підміни довіреної об'єкта в мережі	0.25	низька
2.5.6 Загрози впровадження помилкового об'єкта як в ІСПДн, так і в зовнішніх мережах	0.25	низька

2.5.7 Загрози типу «Відмова в обслуговуванні»	0.25	низька
2.5.8 Загрози віддаленого запуску додатків	0.25	низька
2.5.9 Загрози впровадження по мережі шкідливих програм	0.25	низька

2.12 Заходи щодо протидії загрозі для автоматизованої системи класу 2

Нижче приведена таблиця 2 моделі загроз інформації та протидії цим загрозам для автоматизованої системи класу 2

Таблиця 2.3 - Загрози безпеці

Найменування загрози	Заходи з протидії загрозі	
	Технічні	Організаційні
1. Загрози щодо витоку через технічні канали.		
1.1 Загроза витоку акустичних інформації	-	Інструкція користувача, технологічний процес
1.2 Загрози витоку видової інформації	Жалюзі на вікна, Розташування монітора	Інструкція користувача, технологічний процес
1.3 Загрози витоку інформації каналами ПЕМВН	-	-
2. Загрози несанкціонованого доступу до інформації.		
2.1 Загрози знищення, розкрадання апаратних засобів ІСПДн носіїв інформації шляхом фізичного доступу до елементів ІСПДн		
2.1.1 Крадіжка ПЕОМ	-	Пропускний режим, охорона
2.1.2 Крадіжка носіїв інформації	Зберігання в сейфі, Шифрування даних за допомогою ManageEngine Key Manager Plus SafeDisk	пропускний режим, охорона, акт встановлення засобів захисту, облік носіїв інформації, інструкція користувача
2.1.3 Крадіжка ключів і атрибутів доступу	Зберігання в сейфі	Інструкція користувача
2.1.4 Крадіжки, модифікації, знищення інформації	Шифрування даних за допомогою ManageEngine Key Manager Plus SafeDisk	Пропускний режим, охорона, акт встановлення засобів захисту

	Система захисту від НСД Personal Firewall	
2.1.5 Висновок з ладу вузлів ПЕОМ, каналів зв'язку	-	Пропускний режим, охорона
2.1.6 Несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищення) вузлів ПЕОМ	Шифрування даних за допомогою ManageEngine Key Manager Plus SafeDisk	Ремонт допущеними співробітниками установи
2.1.7 Несанкціоноване відключення засобів захисту	Налаштування засобів захисту	Інструкція адміністратора безпеки, технологічний процес обробки
2.2 Загрози розкрадання, несанкціонованої модифікації або блокування інформації за рахунок несанкціонованого доступу (НСД) із застосуванням програмно-апаратних і програмних засобів (в тому числі програмно-математичних впливів).		
2.2.1 Дії шкідливих програм (вірусів)	Антивірусне ПЗ Avast	інструкція користувача, інструкція відповідального, інструкція адміністратора безпеки, технологічний процес обробки, інструкція з антивірусного захисту, інструкція при зараженні
2.2.2 Декларованих можливостей системного ПЗ та ПЗ для обробки персональних даних	Налаштування засобів захисту	Придбання у довіреної організації
2.2.3 Установка ПО не пов'язаного з виконанням службових обов'язків	Налаштування засобів захисту	Інструкція користувача, інструкція відповідального, інструкція адміністратора безпеки, технологічний процес обробки
2.3 Загрози не навмисних дій користувачів і порушень безпеки функціонування ІСПДн і СЗПДн в її складі через збої в програмному забезпеченні, а також від погроз неантропогенного (збоїв апаратури через ненадійність елементів, збоїв електроживлення) і стихійного (ударів блискавок, пожеж, повеней та т.п.) характеру.		
2.3.1 Втрата ключів і атрибутів доступу	Зберігання в сейфі	Інструкція користувача, інструкція

		адміністратора, безпеки, журнал обліку паролів
2.3.2 Ненавмисна модифікація (знищення) інформації співробітниками	Налаштування засобів захисту	Інструкція користувача
2.3.3 Ненавмисне відключення засобів захисту	Доступ до встановлення режимів роботи засобів захисту надається лише адміністратору безпеки, налаштування засобів захисту	інструкція користувача, інструкція адміністратора безпеки, інструкція з антивірусного захисту
2.3.4 Вихід з ладу апаратно-програмних засобів	-	-
2.3.5 Збій системи електропостачання	Пожежна сигналізація	-
2.3.6 Стихійне лихо	Пожежна сигналізація	Інструкція щодо дій у разі виникнення нештатної ситуації
2.4 Загрози навмисних дій внутрішніх порушників		
2.4.1 Доступ до інформації, модифікація, знищення осіб не допущених до її обробці	Шифрування даних за допомогою ManageEngine Key Manager Plus SafeDisk Personal Firewall	Акт встановлення засобів захисту, дозвільна система допуску
2.4.2 Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробці	-	Зобов'язання про нерозголошення, інструкція користувача
2.5 Загрози несанкціонованого доступу по каналах зв'язку.		
2.5.1 Загроза «Аналіз мережевого трафіку» з перехопленням передається з ІСПДн і прийнятої із зовнішніх мереж інформації:	-	-
2.5.1.1 Перехоплення за переділами з контрольованої зони	-	-
2.5.1.2 Перехоплення в межах контрольованої зони зовнішніми порушниками	-	-
2.5.1.3 Перехват в межах контрольованої зони внутрішніми порушниками	-	-
2.5.2 Загрози сканування, спрямовані на виявлення типу або типів використовуваних операційних систем, мережевих адрес робочих станцій ІСПДн, топології мережі, відкритих портів і служб, відкритих з'єднань та ін.	Personal Firewall	висока

2.5.3 Загрози виявлення паролів по мережі	Personal Firewall	-
2.5.4 Загрози нав'язування помилкового маршруту мережі	Personal Firewall	-
2.5.5 Загрози підміни довіреної об'єкта в мережі	Personal Firewall	-
2.5.6 Загрози впровадження помилкового об'єкта як в ІСПДн, так і в зовнішніх мережах	Personal Firewall	-
2.5.7 Загрози типу «Відмова в обслуговуванні»	Personal Firewall	-
2.5.8 Загрози віддаленого запуску додатків	Personal Firewall	-
2.5.9 Загрози впровадження по мережі шкідливих програм	Personal Firewall, Антивірусне ПЗ Avast	-

2.13 Висновок

Запропонована система підтримки прийняття рішень для моделювання загроз інформації для АС класу 2, дозволить зробити початкову оцінку систем захисту АС класу 2 і побудує модель загроз інформації. Ціль процесу обробки загроз – максимально знизити рівень загроз до прийнятного. При цьому переоцінку загроз треба робити систематично, аби не випустити момент, коли прийнятий загроз перестає бути безпечним у зв’язку зі змінами певних зовнішніх та внутрішніх умов.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Робота передбачає впровадження системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2.

Однією з головний цілей захисту інформаційних ресурсів від внутрішніх загроз є мінімізація збитків від порушення інформаційної безпеки підприємства. Але з іншого боку слід вважати, що захист цих ресурсів потребує деяких витрат.

Економічно доцільним слід вважати, якщо витрати на забезпечення інформаційної безпеки не перевищують збитків від реалізації загрози її порушення.

Щоб обґрунтувати економічну доцільність впровадження системи підтримки прийняття рішень для моделювання загроз інформації для АС класу 2 розрахуємо величину витрат на впровадження СППР.

3.1 Розрахунок капітальних витрат.

До капітальних витрат відносяться:

- витрати на створення комплексу методів;
- витрати на впровадження комплексу методів.

3.1.1 Розрахунок витрат на створення комплексу методів.

Часова заробітна плата фахівця розраховується за формулою (3.1):

$$Зп.д=(Зп + nal)/n, \quad (3.1)$$

де Зп – заробітна плата, Зп =11000 грн.;

nal – налог, nal =22%;

n –кількість робочих годин за місяць, n=160 год.;

Отже, часова заробітна плата фахівця складе:

$$(11000+2420)/160=83,88 \text{ грн/ч.}$$

Вартість створення системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2 розраховується за формулою (3.2):

$$Ств=(Ф*На/Т)+(W+Цее), \quad (3.2)$$

де Ф – первісна вартість комп'ютера, Ф=25000 грн;

На – норма амортизації, На=0,33;

Т – кількість годин роботи фахівця, Т=720 год;

W – потужність комп'ютера, W=0,4кВт;

Це – вартість електроенергії, Це=1,44грн/кВт;

Отже, витрати на створення системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2 розраховується за формулою (3.3):

$$Ств = (25000*0,33/720)+(0,4*1,44)=12,04 \text{ грн/ч.} \quad (3.3)$$

Капітальні витрати на створення СППР розраховується за формулою(3.4):

$$Ссппр=t*(Ств+Зп). \quad (3.4)$$

Отже витрати на створення СППР складуть:

$$Ссппр=720*(12,04+83,88)=69062,40 \text{ грн.}$$

3.2 Розрахунок експлуатаційних витрат

Річні експлуатаційні витрати на СППР визначаються за формулою (3.5):

$$С = Св + Ск, \quad (3.5)$$

де $С_в$ – вартість відновлення й модернізація системи, грн.;

$С_к$ – витрати на керування системою в цілому, грн.

Витрати на відновлення й модернізацію СППР визначається на підставі фактичних даних для АС класу 2.

Витрати на відновлення й модернізацію СППР дорівнює 1% від капітальних витрат на проектування та впровадження, що становить:

Св = 609,62 грн.

Витрати на керування СППР визначається за формулою (3.6):

$$Ск = С_а + С_{ел}, \quad (3.6)$$

де $С_а$ – річний фонд амортизаційних відрахувань, грн.;

$С_{ел}$ – вартість електроенергії, що споживається апаратурою СППР протягом року, грн.

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів.

Річний фонд амортизаційних відрахувань:

$$Са = 69062,40 * 0,33 = 22790,59 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою СППР протягом року, визначається за формулою (3.7):

$$Сел = Р * Fр * Це, \quad (3.7)$$

де Р – встановлена потужність апаратури СППР, кВт;

$F_р$ – річний фонд робочого часу СППР, годин;

$Ц_е$ – тариф на електроенергію, грн / кВт годин.

Вартість електроенергії, що споживається апаратурою СППР протягом року:

$$Сел = 0,4 \cdot 720 \cdot 1,44 = 414,72 \text{ грн.}$$

Витрати на керування СППР:

$$Ск = \ 22790,59+414,72 \ = 23205,31 \text{ грн.}$$

Річні експлуатаційні витрати на функціонування СППР:

$$С = 609,62 + 23205,31 = 23814,93 \text{ грн.}$$

3.3 Економічне обґрунтування

Чиста початкова вартість, розраховується за формулою (3.8):

$$ЧТС = \sum_{i=1}^{n} \left(\frac{У-С}{(1+r)^n}\right) - К, \tag{3.8}$$

де ЧТС - чиста поточна вартість;

r – відсоток кредитування , r= 36%;

С – річні експлуатаційні витрати на СППР;

К – витрати на створення СППР.

$$(У - С) \sum_{i=1}^{n} \frac{1}{(1+r)^n} - K \geq 0 \tag{3.9}$$

Звідси знаходимо У за формулою (3.10):

$$У \geq \frac{K}{\sum(1+r)^n} + C \tag{3.10}$$

$$У \geq \frac{69062,40}{\sum(1+36\%)^1} + 23814,93$$

$$У \geq 105405,35 \text{ грн.}$$

3.4 Висновок

Розробка і впровадження системи підтримки прийняття рішень для моделювання загроз інформації для АС класу 2 є економічно доцільним, якщо $У \geq 105405,35$ грн.

Капітальні витрати склали: К=69062,40 грн.

Поточні витрати склали: С= 23814,93 грн.

ВИСНОВКИ

В ході виконання роботи було досліджено систему підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2, були розглянуті та проаналізовані СППР, основні уразливі елементи автоматизованої системи класу 2.

В роботі була розроблена СППР, етапи роботи СППР, алгоритм, що дозволяє зробити початкову оцінку системи захисту автоматизованої системи класу 2, та після аналізу всіх даних має збудувати попередню модель загроз для АС.

Результати роботи в подальшому можна використовувати при розробці та впроваджені систем підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2.

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу / ДСТСЗІ СБ України – Київ, 1999.

2 НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

3 НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

4 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України – Київ, 1999.

5 Ситник В.Ф. Системи підтримки прийняття рішень. Навчальний посібник. – К.: КНЕУ, 2004. – 614 с.

6 Системи підтримки прийняття рішень та технології штучного інтелекту (Електрон. ресурс) /Спосіб доступу: URL: http://study2.academy.sumy.ua/files/a.yarovenko104390l.pdf - Загол. з екрану.

7 Братушка С.М. Системи підтримки прийняття рішень: Навчальний посібник для самостійного вивчення дисципліни. - Суми: ДВНЗ "УАБС НБУ", 2010. – 265 с.

8 Бідюк П.І. Комп'ютерні системи підтримки прийняття рішень: Навчальний посібник. – Київ: КНУТД, 2004. – 112 с.

9 Сфери застосування і приклади використання СППР (Електрон. ресурс) /Спосіб доступу: URL: http://ua.textreferat.com/referat-7752-2.html - Загол. з екрану.

10 Бідюк П.І. Проектування комп'ютерних інформаційних систем підтримки прийняття рішень: Навчальний посібник. – Київ: ННК «ІПСА» НТУУ «КПІ», 2010. – 340 с.

11 Закон України «Про інформацію» / Спосіб доступу: URL: http://zakon1.rada.gov.ua/laws/show/2657-12

12 Стандарт ISO/IEC 27001 / Спосіб доступу: URL: https://ru.wikipedia.org/wiki/ISO/IEC_27001

13 Призначення та класифікація протоколів маршрутизації / Спосіб доступу: URL: http://posibnyky.vntu.edu.ua/kom_m/4.1.html

14 Протоколи управління мережою / Спосіб доступу: http://www.voyageurs.com.ua/

15 Мережевий протокол ICMP / Спосіб доступу: https://ru.wikipedia.org/wiki/ICMP

16 Ginzberg M.I., Stohr E.A. Decision Support Systems: Issues and Perspectives // Processes and Tools for Decision Support / ed. by H.G. Sol.. — Amsterdam: North-Holland Pub.Co, 1983.

17 Golden B., Hevner A., Power D.J. Decision Insight Systems: A Critical Evaluation // Computers and Operations Research, 1986. — v. 13. — N2/3. — p. 287—300.

18 Haettenschwiler P. Neues anwenderfreundliches Konzept der Entscheidungs-unterstutzung. Gutes Entscheiden in Wirtschaft, Politik und Gesellschaft. Zurich: Hochschulverlag AG, 1999. — S. 189—208.

19 Holsapple C.W., Whinston A.B. Decision Support Systems: A Knowledge-based Approach. — Minneapolis: West Publishing Co., 1996.

20 Keen P.G.W. Decision support systems: a research perspective. Decision support systems : issues and challenges. G. Fick and R. H. Sprague. Oxford ; New York: Pergamon Press, 1980.

21 Keen P.G.W. Decision Support Systems: The next decades // Decision Support Systems, 1987. — v. 3. — pp. 253—265.

22 Keen P.G.W., Scott Morton M. S. Decision support systems : an organizational perspective. Reading, Mass.: Addison-Wesley Pub. Co., 1978.

23 Little J.D.C. Models and Managers: The Concept of a Decision Calculus // Management Science, 1970. – v. 16. – N 8.

24 Marakas G. M. Decision support systems in the twenty-first century. Upper Saddle River, N.J.: Prentice Hall, 1999.

25 Power D. J. “What is a DSS?” // The On-Line Executive Journal for Data-Intensive Decision Support, 1997. – v. 1. – N3.

26 Power D. J. Web-based and model-driven decision support systems: concepts and issues. Americas Conference on Information Systems, Long Beach, California, 2000.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	30	
6	А4	2 Розділ	43	
7	А4	3 Розділ	5	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу магістра на тему:
Система підтримки прийняття рішень для моделювання загроз інформаційній безпеці в автоматизованій системі класу 2
Дунаєва Яна Олексійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 95 сторінках та містить 4 рисунків, 4 таблиць, 26 джерел та 4 додатка.

Об'єкт дослідження: автоматизована система класу 2.

Предмет дослідження: синтез системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2.

У спеціальній частині розглянуто основні принципи і технології функціонування системи підтримки прийняття рішень, розглянуті моделі систем підтримки прийняття рішень, уразливість основних елементів АС та класифікація загроз безпеки.

В економічному розділі виконано розрахунок вартості заходів щодо впровадження системи підтримки прийняття рішень для моделювання загроз інформації для автоматизованої системи класу 2.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник