МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

МЕХАНІЗМ ПРИЙНЯТТЯ РІШЕНЬ З ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧА В УМОВАХ ЗАГРОЗ

Виконав: студент групи 2К-21
Спеціальності 123 Комп’ютерна інженерія
Андрій ЯКОВЕНКО
Керівник:
Майя ЛЮТА

Черкаси 2025

АНОТАЦІЯ

Кваліфікаційна робота на тему «Механізм прийняття рішень з захисту персональних даних користувача в умовах загроз» складається з вступу, основної частини, що містить 3 розділи, висновку та списку використаних джерел. Загальний обсяг роботи – 57 сторінок. У роботі 17 рисунків та 3 таблиці. Перелік використаних ресурсів налічує 32 одиниць.

Перший розділ. Основи захисту персональних даних. В цьому розділі розглядається поняття персональних даних, атак, загроз, конфіденційність персональних даних та способи її порушення, а також розглядається шкідливе програмне забезпечення.

Другий розділ. Системи підтримки прийняття рішень. В цьому розділі розглядаються типи систем підтримки прийняття рішення, вимоги до управління такими системами, управління ризиками, оцінка ризиків безпеки для підтримки прийняття рішення.

Третій розділ. Механізм прийняття рішень. В даному розділі розглядається механізм прийняття рішення: структура рішення, багато атрибутивні методи прийняття рішення, теорія багатокористувацької корисності, аналітична ієрархія та методи випередження.

В процесі роботи досліджено механізм прийняття рішень з захисту персональних даних користувача, та зроблено висновки.

Ключові слова: ЗАХИСТ, СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, ОЦІНКА РИЗИКІВ.

ABSTRACT

The qualification work on the topic "Decision-making mechanism for protecting user personal data in the face of threats" consists of an introduction, the main part, which contains 3 sections, a conclusion and a list of sources used. The total volume of the work is 57 pages. The work contains 17 figures and 3 tables. The list of resources used has 32 units.

The first section. Fundamentals of personal data protection. This section examines the concept of personal data, attacks, threats, personal data confidentiality and methods of its violation, and also considers malicious software.

The second section. Decision support systems. This section examines the types of decision support systems, requirements for managing such systems, risk management, and assessment of security risks for decision support.

The third section. Decision-making mechanism. This section examines the decision-making mechanism: decision structure, multi-attribute decision-making methods, multi-user utility theory, analytical hierarchy and prediction methods.

In the process of work, the decision-making mechanism for protecting user personal data was investigated, and conclusions were drawn.

Keywords: PROTECTION, DECISION SUPPORT SYSTEMS, RISK ASSESSMENT.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

АРМ – автоматизоване робоче місце

ІСПДн – інформаційна система персональних даних

ОПР – особа яка приймає рішення

ПДн – персональні дані

СУБД – система управління бази даних

ПЗ – програмне забезпечення

СППР – система підтримки прийняття рішення

TOPSIS – technique for order preference by similarity to ideal solution

ВСТУП

Актуальність. Вивчення механізму прийняття рішень з захисту персональних даних користувачів від несанкціонованого доступу третіх сторін є однією з найважливіших задач сьогодення тому, що захист персональних даних для комерційних організацій чи державних установ є пріоритетним завданням адже цього вимагає Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. Кожен рік з'являються нові інформаційні технології, це та безліч інших не менш важливих факторів суттєво ускладнює захист інформації яка підлягає захисту: персональні дані, державна таємниця чи інші дані які не підлягають розголошенню. Захист персональних даних являє собою комплекс методів та засобів які виконуються регулярно з метою забезпечення відповідної надійності інформації, яка зберігається, створюється та/або оброблюється інформаційними системами, а також що передається по будь-яким каналам зв'язку.

Об'єкт дослідження. Заходи щодо захисту персональних даних користувача в умовах загроз.

Предмет дослідження. Механізм прийняття рішень з захисту персональних даних в умовах загроз.

Мета дослідження. Дослідити механізм прийняття рішень з захисту персональних даних користувача в умовах загроз.

Завдання. Під час розробки дипломної роботи було поставлено наступні завдання для виконання:

− Ознайомитися з основами захисту персональних даних;

− Розглянути способи порушення конфіденційності персональних даних;

− Ознайомитися з системами підтримки прийняття рішення;

− Розглянути оцінку ризиків безпеки для підтримки прийняття рішення в умовах загроз;

− Розглянути механізм прийняття рішень в системах підтримки прийняття рішення.

Методи дослідження. Дослідження ґрунтуються на науковій літературі, а також на аналізі нормативно-правових актів в області інформаційної безпеки. Методологічну базу дослідження склали загальнонаукові методи; історичний – при дослідженні процесу появи тих чи інших явищ; методи дедукції, індукції, системно-структурний а також дослідження документів.

Інформаційна база. В першу чергу складається з наукових публікацій по захисту персональних даних. Також в ході виконання роботи були вивчені нормативно-правові акти, які включають в себе Закон України «Про захист персональних даних» від 23.04.2021 № 2297-VI, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 04.07.2020 № 80/94-ВР.

Практичне значення одержаних результатів. В роботі досліджено механізм прийняття рішень з захисту персональних даних користувачів в умовах загроз. Цей механізм може застосовуватися в загальному колі галузей наприклад в медицині, в банківських установах та в багатьох інших системах які обробляють персональні дані користувачів.

РОЗДІЛ 1
ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Історія виникнення питань захисту персональних даних

Ідея захисту персональних даних виникла ще в середині XX сторіччя, коли були прийняті Загальна декларація прав людини та Міжнародний пакт про громадянські і політичні права, які гарантують свободу листування, приватного життя та недоторканість житла. З розвитком інформаційних систем стало зрозуміло, що коли-небудь внесені дані до інформаційних систем можуть передаватися безкінечну кількість разів до того ж безконтрольно. В відповідь на таку загрозу, розвинені країни почали розробляти міжнародні та внутрішні законопроекти для забезпечення контроля обробки, отримання та передачі персональних даних. Починаючи з 1990-х років подібні закони були прийняті також низками країн Східної Європи, Африки та Азії.

В Україні це Закон України «Про захист персональних даних» від 23.04.2021 № 2297-VI. Відповідно до якого Суб'єкт персональних даних має право: знати про джерела збирання, місцезнаходження своїх персональних даних, отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані, пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, відкликати згоду на обробку персональних даних.

З появою нових технологій відкриваються нові можливості для збору, аналізу, передачі, обробки персональних даних, але законодавства країн не в змозі оновлюватися достатньо швидко щоб контролювати і регулювати проблеми захисту персональних даних які виникли внаслідок інновацій технологій.

Всі ми чули вираз «хто володіє інформацією, той володіє світом», всі великі корпорації розуміють, що загрози інформаційної безпеки можуть вплинути на їх

бізнес, відношення клієнтів до них а також призвести до фінансових незручностей. Сьогоденний світ став дуже відкритим завдяки інтернету наприклад зараз одним натиском клавіші мишки можна поділитися своєю думкою з мільйонами, мільярдами людей по всьому земному шару за лічені секунди, а ще кілька десятиліть тому на це б знадобилося значно більше часу.

1.2 Поняття персональних даних та принципів інформаційної безпеки

Відповідно до закону України «Про захист персональних даних» від 23.04.2021 № 2297-VI, персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Отже це означає, що персональними даними можна вважати:

- ім’я;
- адреса;
- номер телефона;
- дата народження;
- ідентифікаційний номер (страхова картка, водійське посвідчення, тощо);
- веб – ідентифікатори наприклад файли cookie або IP – адреса;
- номери банківських карток;
- паспортні дані;
- персональні фотографії.

Інформаційна безпека – це захист інформації та інформаційних систем з метою забезпечення конфіденційності, цілісності та доступності інформації від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення даних.

Цілісність, конфіденційність та доступність – ці три поняття лежать в основі інформаційної безпеки зображені на рисунку 1.1.

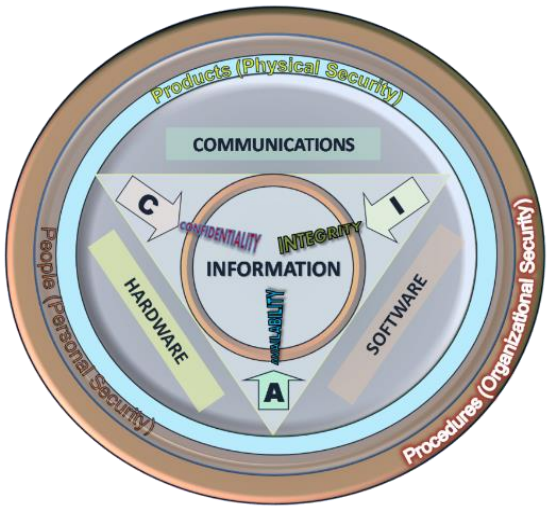

Рисунок 1.1 – Тріада інформаційної безпеки

Цілісність даних обумовлює збереження даних в точності та повноті протягом усього їх життєвого циклу. Тобто це означає інсталяцію засобів контролю безпеки, які будуть гарантувати цілісність даних і те, що дані не будуть змінені або вилучені несанкціонованою особою.

Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Доступність ця риса означає, що будь яка інформаційна система буде корисна тільки тоді, коли вона буде доступна в будь який час. Доступ до комунікаційних каналів, систем зберігання та обробки інформації а також до систем захисту інформації має бути виконаний миттєво після запиту.

Підприємства та їхні клієнти все більше покладаються на системи високої доступності в режимі реального часу цілодобово та без вихідних. Це означає, що фахівці з інформаційної безпеки все більше турбуються про забезпечення доступності, запобігаючи відключенню електроенергії, відмові обладнання та

атакам відмови в обслуговуванні. Доступність розглядається як найважливіша частина успішної програми захисту інформації.

1.3 Способи порушення конфіденційності персональних даних

Спираючись на багаточисленні дані які обробляються в інформаційній системі персональних даних, можна виділити такі наступні методи порушення конфіденційності ПДн:

− публічне несанкціоноване розголошення персональних даних;

− незаконне отримання персональних даних третьою стороною;

− викрадення персональних даних для використання в корисливих цілях;

− передача персональної інформації третій стороні.

1.4 Поняття вразливості систем

Вразливості – це слабкі місця в системі якими користуються зловмисники для виконання команд, отримання доступу до даних та/або проведення атак.

Вразливості присутні в будь яких системах, це можуть бути різноманітні недоліки в апаратному забезпеченні або ж помилки в програмному коді систем, чи помилкове використання невірних політик чи процедур в системі, а також найчастіше, помилки користувачів систем.

Всі системи базуються на двох компонентах: апаратному (hardware) та програмному (software) забезпеченні, які в свою чергу мають безліч недоліків в своїй конструкції. Ідентифікувати апаратні вразливості складно, та ще складніше їх усунути навіть якщо вразливість була знайдена, натомість, вразливості програмного забезпечення можна знайти будь-де наприклад в операційних системах, драйверах чи в прикладному ПЗ. Є декілька факторів які найчастіше

призводять до появи помилок по-перше це не правильне проектування програмного забезпечення, а по-друге це складність програмного забезпечення.

1.5 Поняття загроз

Загроза – це дія, яка використовує слабкі місця системи безпеки і негативно впливає на систему. В основному, загрози походять з двох джерел: людини та природи. Природні загрози, такі як землетруси, урагани, повені та пожежі, можуть завдати серйозних збитків комп'ютерним системам. Для зменшення шкоди від стихійних лих можуть бути впроваджені певні заходи безпеки але запобігти їх не вдасться. Для захисту систем від природних загроз найчастіше роблять резервне копіювання даних, плани аварійного відновлення та плани на випадок непередбачуваних обставин. Людські загрози: – цей клас включає загрози, спричинені діями людини, такими як інсайдери або хакери, які завдають шкоди або ризику в системах. В свою чергу вони складаються з внутрішніх (мають авторизований доступ в системі) та зовнішніх загроз більш детально показано на рисунку 1.2 (особи чи групи осіб які працюють з зовні), ціль яких завдати збитків системі та/або вивести систему з ладу. Також такі загрози поділяють на наступні категорії:

− неструктуровані загрози – складаються в основному з недосвідчених; людей, що використовують доступні хакерські інструменти;

− структуровані загрози. Через те, що люди знають вразливості системи; вони здатні розуміти, розробляти і використовувати коди та сценарії.

Приклад структурованою загрози – Advanced Persistent Threats (APT). APT це потужна мережева атака, націлена на крадіжку цінної інформації наприклад: звіти фінансової промисловості чи національної оборони в комерційних і державних організаціях.

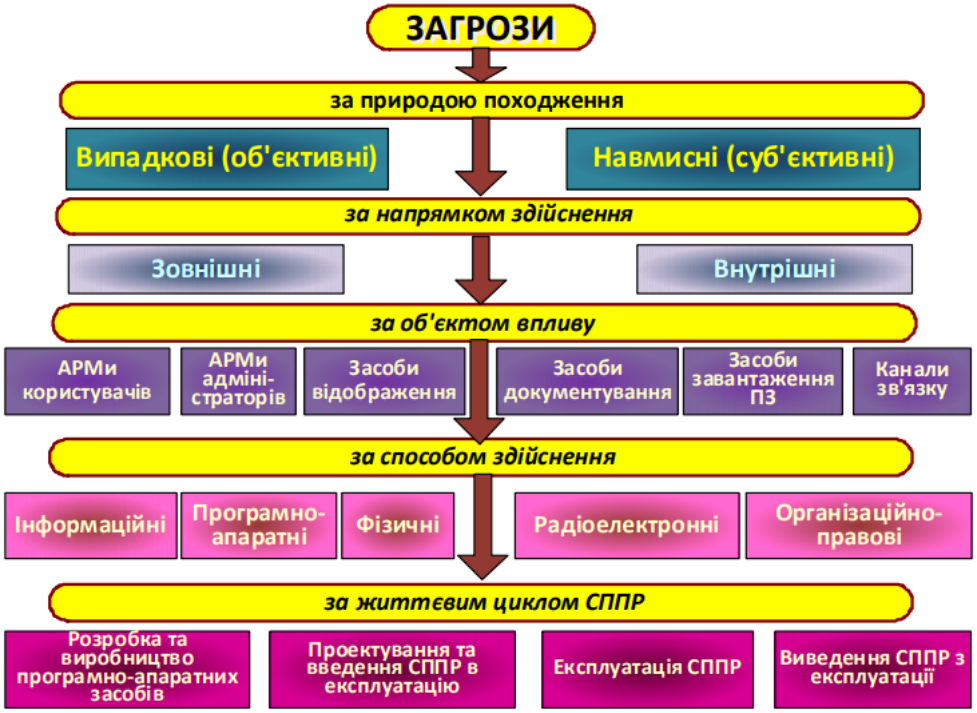

Рисунок 1.2 – Класифікація загроз СППР

Також загрози можна класифікувати по компонентах СППР на які вони націлені показано на рис. 1.3.

Рисунок 1.3 – Альтернативна класифікація загроз СППР

Також крім загальноприйнятих класифікацій загроз існують і класифікації загроз які розроблені різними корпораціями наприклад класифікація загроз STRIDE розроблена Microsoft для побудови моделі загроз при розробці програмного забезпечення її категорії показані в таблиці 1.1.

Таблиця 1.1– Класифікація загроз STRIDE

Місце	Загроза	Визначення	Приклад
Authentication	підміна об'єктів (spoofing identity)	видавання себе за щось чи когось іншого.	наприклад видавання себе за microsoft.com або ntdll.dll
Integrity	модифікація даних (tampering with data)	зміна даних або коду	модифікація DLL на диску або DVD, або пакета даних при проходженні по локальній мережі.
Authorization	підвищення привілеїв (elevation of privilege)	отримати підвищення рівня привілеї без належного доступу	дозвіл віддаленому користувачеві Інтернету запускати команди є класичним прикладом, але перехід від обмеженого користувача до адміністратора це також є підвищенням привілеїв.
Availability	відмова в обслуговуванні (denial of service)	забороняють або погіршують роботу деяких служб системи	збій Windows або веб-сайту, відправка пакета та поглинання секунд процесорного часу або маршрутизація пакетів у чорну діру.
Confidentiality	розголошення інформації (information disclosure)	надавати інформацію особі яка не має права її бачити.	дозвіл комусь читати вихідний код Windows; публікація списку клієнтів на веб-сайті.

1.6 Поняття атак

Атаки – це дії, спрямовані на заподіяння шкоди системі або порушення нормальної її роботи шляхом використання вразливостей використовуючи для цього різні методи та інструменти модель порушника та типи атак показані на рисунку 1.4. Як правило зловмисники здійснюють атаки з метою особистого задоволення, для досягнення певних цілей. Вартість атаки – це час, зусилля, мотивація та ресурси які витратив зловмисник для атаки.

Зловмисники – це особи які становлять загрозу для цифрового світу, такі люди можуть бути хакерами, злочинцями чи навіть урядами країн.

Порушник		
Кваліфікація	**Мотив**	**Технічна оснащеність**
Початківець	**Цікавість, бажання оцінити свої можливості**	**Звичайний домашній комп'ютер**
Спеціаліст	**Образа, бажання помститись**	**Доступ до чужого ком'пютера**
Професіонал	**Бажання збагатитись за рахунок нанесення щкоди іншим**	**Потужний комп'ютер та програмне забезпечення**

Типи атак:

- Атаки відмови в обслуговуванні
- Перехоплення й перенаправлення трафіку
- Впровадженням в комп'ютери шкідливих програм
- Трояни
- Мережеві хробаки
- Віруси
- Шпигунські програми
- Спам

Рисунок 1.4 – Модель порушника та типи атак

Форми атак:

– Активні мережеві атаки - моніторинг не зашифрованого трафіку в пошуку персональних даних чи іншої важливої інформації;

– Пасивні атаки – наприклад моніторинг мережевих комунікацій для дешифрування слабо зашифрованого трафіку та інформацію про автентифікацію;

– Розповсюджені кібератаки:

– Фізичні атаки: при таких атаках підробляються фізичні (апаратні) компоненти систем;

– Розвідувальні атаки – незаконне виявлення та нотування файлів систем, їх вразливостей, тощо. Прикладами таких атак можуть бути, сніферінг пакетів, аналіз трафіку, сканування мережевих портів, отримання даних про IP-адресу за допомогою відсилання запитав;

− Відмова в обслуговуванні (DoS): При таких атаках вузли чи системи мережі спеціально роблять недоступними для користувачів цієї системи;

− Атака доступу – при таких атаках треті обличчя отримують доступ до ресурсів і мереж пристроїв до яких не мають правового доступу. Розрізняють два типи атак доступу:

1. Фізичний доступ – це коли правопорушник може отримати фізичний доступ до обладнання;

2. Віддалений доступ – такий доступ здійснюється за допомогою віддаленого підключення до IP пристроїв мережі.

− Загрози конфіденційності. Захист персональних даних стає все дедалі складнішим. Є декілька загроз конфіденційності:

1. Видобуток даних: при таких загрозах зловмисники можуть виявити інформацію яка може бути не очевидна для певних баз даних;

2. Кібершпигунство: за допомогою використання алгоритмів злому та вірусів, зловмисники шпигують за жертвою для отримання персональних даних чи іншої цінної інформації;

3. Прослуховування: банальне прослуховування мережі для прослуховування розмов між сторонами;

4. Відстеження: За допомогою ідентифікаційного номера пристрою (UID) можна відстежувати місцезнаходження пристрою, чим зловмисники і користуються;

5. Атаки підбором паролю. Хакери намагаються підібрати вірний пароль до облікового запису жертви. Підбирання пароля може відбуватися двома способами:

1) Підбір за словником – використання словника для підбору можливих комбінацій літер та цифр з метою вгадування пароля користувача;

2) Атака грубої сили – за допомогою спеціалізованого програмного забезпечення підбираються всі можливі варіанти пароля для виявлення оригінального пароля користувача.

− Кіберзлочини: зловмисники (хакери) викрадають персональну інформацію або іншу цінну інформацію користувачів систем з метою отримання матеріальної вигоди;

− Атаки диспетчерського контролю та збору даних (SCADA): як представник систем TCP / IP, система SCADA дуже вразлива до безлічі неправомірних атак наприклад будь яким з наведених способів:

1. Атака в відмові обслуговування для виведення системи з ладу;

2. Застосування шкідливого програмного забезпечення для отримання доступу до управління системою.

1.7 Шкідливе програмне забезпечення

Шкідливий програмний засіб, шкідливе програмне забезпечення (англ. malware – скорочення від malicious – зловмисний і software – програмне забезпечення) – програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем [29]. За рівнем небезпечної шкідливі програми розподіляють на безпечні, небезпечні і дуже небезпечні дивитися таблицю 1.2.

Таблиця 1.2 – Розподіл шкідливих програм за рівнем небезпечної дії

Безпечні	Небезпечні	Дуже небезпечні
Проявляються відео та звуковими ефектами, не змінюючи файлову систему комп’ютера, не ушкоджуючи файли, тощо	Призводять до перебоїв в роботі комп’ютера, засмічуючи систему, перезавантажують систему тощо.	Знищують дані з постійної та зовнішньої пам’яті, виконують шпигунські дії, тощо.

Розподіл шкідливих програм за принципом розповсюдження та функціонування зображений на рисунку 1.5.

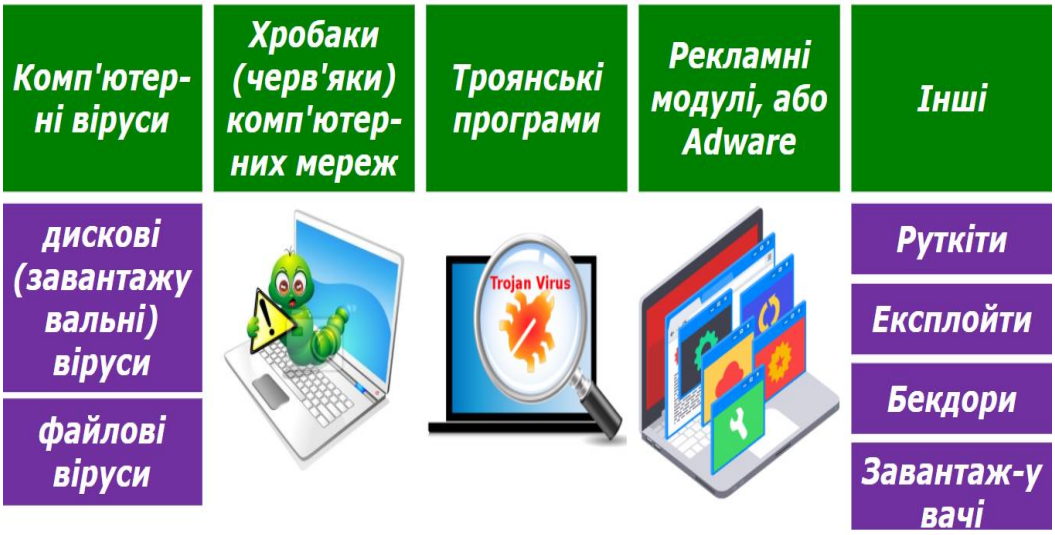

Рисунок 1.5 – Принцип розповсюдження та функціонування шкідливих програм.

Програмне забезпечення може містити різноманітні шкідливі віруси.

Хробаки (Worm) – це програми які клонують саму себе безліч разів, цим самим засмічуючи файлову систему комп’ютера і тим самим сповільнюючи його швидкодію. Однією з фішок таких вірусів є те, що вони можуть ставати частиною іншої не шкідливої програми приклад такого вірусу показано на рисунку 1.6;

Рисунок 1.6 – Програми віруси хробаки

Віруси-маскувальники (Rootkit) – такі віруси найчастіше використовуються для маскування шкідливої активності, тобто вони здатні приховувати віруси для того щоб антивірусна програма не могла їх виявити, приклад програми для виявлення вірусів-маскувальників показаний на рисунку 1.7. Також, для приховання своєї власної присутності в файлах комп'ютера, а також дій зловмисника такі шкідливі програми можуть видозмінювати операційні системні файли;

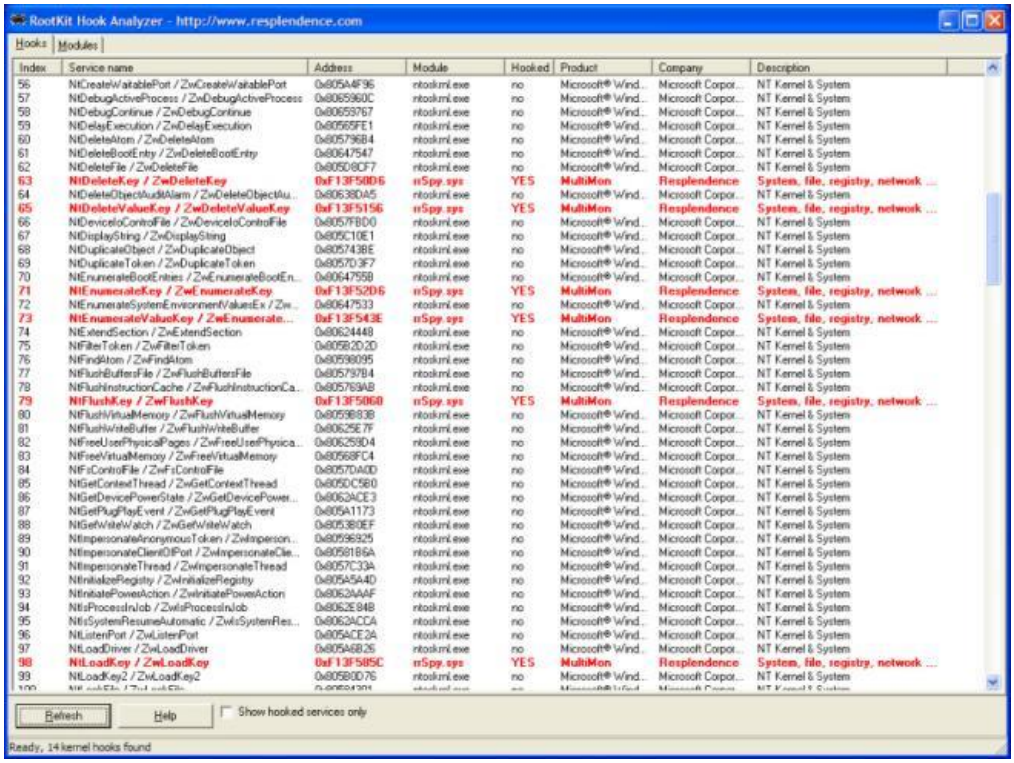

Рисунок 1.7 – приклад роботи програми по виявленню вірусів-маскувальників

Віруси-шпигуни (Spyware) – такі програми збирають персональні дані користувача найчастіше це – паролі, дані кредитних карт, тощо;

Зомбі (Zombie) – саме за допомогою таких вірусів зловмисники можуть керувати комп'ютером жертви. Також комп'ютери заражені такий вірусом можуть збиратися в спільну мережу (ботнет) такі мережі використовують для масових атак на сайти або ж для розсилання спаму. Жертва може навіть і не здогадуватись що її комп'ютер заражений і використовується для «темних справ» зловмисників;

Рекламні віруси (Adware) – віруси-реклами, без дозволу і відома юзерів вбудовуються в ПЗ з метою показання користувачеві різноманітних надокучливих рекламних банерів. Як правило, такі віруси найчастіше присутні в безкоштовному програмному забезпеченні. Також нерідко таке ПО збирає персональні дані користувача і надсилає їх своїм розробникам. Приклад Adware зображений на рисунку 1.8;

Рисунок 1.8 – Робочий стіл комп'ютера зараженого вірусом Adware

Блокуючі-віруси (Winlock) – як зрозуміло з назви, такі програми блокують користувачеві доступ до системи, тобто при завантаженні системи на екрані з'являється вікно мало того, що це вікно неможливо закрити, так в ньому ще й звинувачують користувача в перегляді неліцензійного контенту та вимагають перевести кошти на банківську карту, а якщо користувач цього не зробить, то всі дані комп'ютера будуть знищені приклад такого вікна зображено на рисунку 1.9. Щоправда якщо ж користувач відправляє кошти на вказану картку, то доступу до комп'ютера все одно не отримував. На блокуючі-віруси дуже схожі на інша віруси такі як: віруси-вимагачі, або ж вірус-шантажисти (ransomware) такі програми –

віруси шифрують всі дані на комп'ютері і в подальшому вимагають викуп за відновлення доступу і дешифровку файлів комп'ютера, приклад спливаючого вікна комп'ютера зараженого таким вірусом показано на рисунку 1.10;

Рисунок. 1.9 – Приклад вікна комп'ютера зараженого вірусом типу Winlock

Троянські віруси (Trojan) – Троянський кінь небезпечний не тільки для Трої але ще й для ваших комп'ютерів, адже це самий небезпечний комп'ютерний вірус який маскується в інших нешкідливих програмах, до речі через що й отримав свою назву. Така шкідлива програма не несе ніякої загрози поки користувач не запустить програму в яку вірус замаскувався. Trojan найчастіше використовується для крадіжки персональних даних користувача, але виявити його дуже проблематично, його особливістю є те, що він не здатний самостійно розмножуватися.

Рисунок 1.10 – Спливаюче вікно комп’ютера зараженого вірусом – шантажистом

Задокументовано, що віруси містять код, який призначений для нанесення шкоди комп’ютеру користувача і також для виконання неправомірних дій. Віруси спеціально надсилаються користувачам систем з метою подальшого розповсюдження вірусу для завдання шкоди інформації або ж для її знищення. Шкідливі програми можуть завдавати шкоди по різному наприклад копіювати файли, показувати рекламні банери або ж збирати персональні дані жертв.

Носієм шкідливих програм в ІСПДн може бути апаратний елемент обчислювальної техніки або ж драйвер.

Якщо вірус не асоціюється з якою небудь системною прикладною програмою або ж однією з загальних програм програмного забезпечення ІСПДн, то носієм може вважатися:

− Зовнішній носій: диск, флешка, зовнішній жорсткий диск і тощо.;

− Внутрішні носії інформації: жорсткі диски, операційна пам’ять, мережева карта, відеокарта, блок живлення і тощо;

− Мікросхеми зовнішніх пристроїв (клавіатури, графопобудовники, принтера, монітора, сканера, тощо.);

− В випадку якщо ж шкідлива програма потрапила з повідомленнями, або файлами переданими по мережі, то їх носієм можуть бути:

1. Пакети даних переданих по мережі ІСПДн;

2. Різні файли (текстові, графічні тощо.).

При появі загроз з наведеної вище групи можливе порушення безпеки конфіденційності ПДН.

Висновки до розділу 1

В цьому розділі було розглянуто історію виникнення питань з захисту персональних даних, поняття персональних даних, принципів інформаційної безпеки, способи порушення конфіденційності персональних даних, поняття вразливості систем, загроз та атак, а також було розглянуте шкідливе програмне забезпечення таке як: віруси хробаки, віруси-маскувальники, віруси-шпигуни, зомбі віруси, рекламні віруси, блокуючі-віруси, троянські віруси. Також були розглянуті можливі носії шкідливих програм такі як: зовнішні носії, внутрішні носії, мікросхеми зовнішніх пристроїв, а також пакети даних які передаються мережею.

РОЗДІЛ 2
СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

2.1 Коротка історія систем підтримки прийняття рішень

За останні півстоліття спостерігається стрімкий ріст в області інформаційних систем, зокрема і систем підтримки прийняття рішень. У 1960-х роках системи підтримки прийняття рішень в більшості використовувалися для забезпечення менеджерів структурованими періодичними звітами, а самі СППР базувалися на дуже потужних та дорогих комп’ютерах (мейнфреймах). В той же час створення IBM System 360 а також інших потужних процесорних систем зробило побудову систем управлінської інформації в великих корпораціях більш практичним і економічним.

В 1970-х роках СППР стали значно складнішими комп'ютерними системами, які підтримували ціноутворення, виробництво, маркетинг, логістичні функції.

На початку 1990-х років програмне забезпечення бізнес-аналітики, сховищ даних та OLAP (On-Line Analytical Processing) почали розширювати можливості СППР.

Так, в 1997 році сховище даних стало основою інтеграційного сховища знань, що сприяло більш швидкому і ефективному способу прийняття рішень.

2.2 Визначення та опис систем підтримки прийняття рішень

СППР -це інтерактивна комп’ютерна система яка допомагає особам які приймають рішення використовувати дані і моделі для вирішення неструктурованих, погано структурованих або напівструктурованих проблем.

Згідно з Мора, особа, що приймає рішення, використовує комп’ютерні технології для:

− упорядкування інформації за факторами проблем;

− приєднання всіх атрибутів до моделі;

− використання основи / моделі для імітації альтернатив;

− вибрати найкращий курс дій.

Результати повідомляються як умови параметрів, експериментальні прогнози та / або рекомендовані дії. Типова архітектура СППР Мора та співавторів показана на (рисунку 2.1).

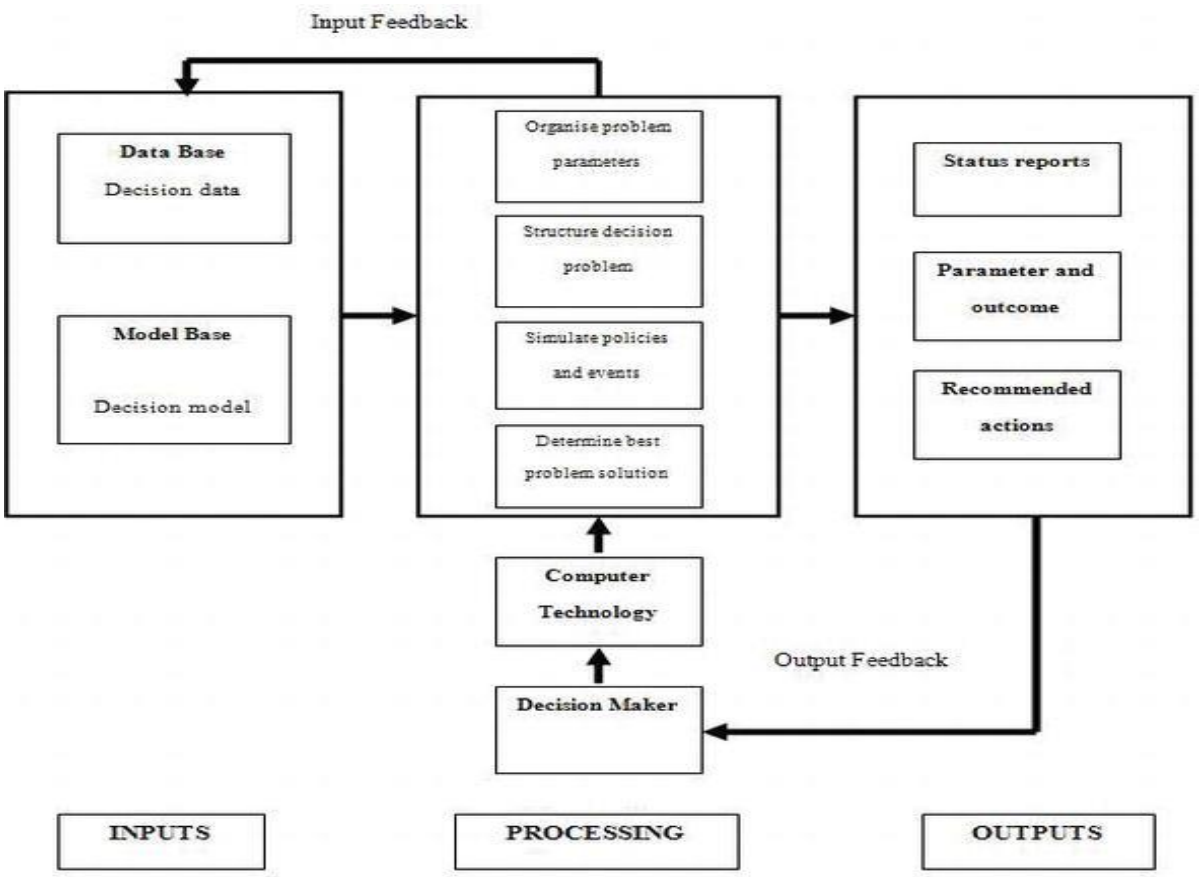

Рисунок 2.1 – Типова архітектура СППР Мора

СППР надає загальний аналіз без великих зусиль програмування тому, що як правило розробляється для використання не технічних користувачів (менеджерів). Такі користувачі використовують СППР для пошуку, аналізу та виокремлення що дозволяє їм побачити всі основні моменти які можуть допомогти їм в прийнятті вірного рішення. Більшість СППР надають можливості не тільки в аналізі даних в

створенні звітів для керівництва а ще й підтримують менеджерів в плануванні спільного аналізу, та в можливому розвитку подій відповідаючи на питання « А що буде якщо».

Отже, СППР підтримує як тактичні так і стратегічні рішення і використовується для того, щоб менеджер спираючись на свій досвід в певній галузі і дані СППР міг прийняти вірне рішення.

СППР відрізняються по масштабу – деякі з них розроблені для використання декількома користувачами (такі системи широко застосовуються в наш час), а інші «самодостатні» (такі системи були популярні в минулому). Також є СППР які орієнтовані на дані, на моделі, а також на комунікацію, основні елементи СППР показано на рисунку 2.2.

Рисунок 2.2 – Основні елементи СППР

2.3 Вимоги до управління систем підтримки прийняття рішень

Вимоги та спосіб використання інформації в кожному рівні управління свій а отже і вимоги до СППР у кожного різні. Найвищі ланки управління компанії як правило керуються більше зовнішньою інформацією, а ніж тою яка була згенерована в СППР, такі ланки управління приймають рішення довготривалого планування чи стратегічного розвитку, а отже для прийняття вірного рішення аналізують інформацію про довгострокові тенденції. Також при прийнятті вірного рішення ключовим фактором є спільний аналіз, тобто менеджерам потрібно багато даних про ризики, та вірогідності тих чи інших подій, та варіанти можливих дій. Стосовно нижчих рівнів управління, там увага приділяється внутрішньо генерований інформації, для короткотермінових цілей. Але так як звіти, та прогнози створені нижчими рівнями керівництва застосовуються для прийняття рішень вищими рівнями керівництва, то дуже важливо щоб СППР підтримувала нижчі ланки керівництва наскільки це можливо адже вони напрями впливають на правильність рішення вищих ланок керівництва.

Отже, інформаційні потреби різних рівнів управління направлені на контроль функцій нижчого керівництва, прийняття тактичних рішень середнього керівництва, а також прийняття стратегічних рішень вищого керівництва.

Окрім цього СППР також використовується для підвищення якості управлінського контролю і повинна вирішувати такі завдання як:

− Розподіл ресурсів між конкретними видами діяльності;

− Нагляд за результатами отриманими в обмін на використані ресурси;

− Оцінка вище зазначених результатів;

− Підготовка звітів про витрачені ресурси, а також про відсоток досягнень цілей;

− Вдосконалення діяльності та розподілу ресурсів відповідно до оцінки результатів.

2.4 Ідеальні характеристики та можливості СППР

Досить тяжко, навіть неможливо визначити стандартні характеристики СППР, але можна узагальнити відмінності СППР від інших систем наступним чином:

− СППР допомагає менеджерам по прийняттю рішень у напівструктурованих та неструктурованих проблемах (які не можливо вирішити процедурними методами або інструментами), використовуючи людські судження та комп'ютери;

− СППР охоплює різні менеджерські рівні;

− СППР оперує різними інструментами аналізу;

− СППР повинна бути адаптивною та гнучкою, щоб користувачі мали змогу додавати, корегувати та видаляти чи реорганізовувати вибрані елементи;

− Підтримка надається всім як групам так і окремим людям, адже інколи бувають такі ситуації які потребують думок декількох людей з різних підрозділів або навіть різних організацій;

− СППР повинна бути зручною для використання;

− СППР повинна підтримувати менеджерів які приймають рішення, а не заміняти їх;

− СППР повинна підвищити ефективність прийняття рішення (доцільність та якість), а не результативність (вартість прийняття рішення);

− Користувачі повинні вміти створювати та модифікувати прості системи, більш складні системи повинні розроблятися експертами;

− СППР найчастіше використовує моделі для аналізу проблем;

− СППР повинна забезпечувати доступ до різних типів та джерел даних;

− СППР може бути впроваджена з іншими системами та може передаватися через мережу або веб-технології. Рисунок 2.3 показує ідеальний набір характеристик СППР.

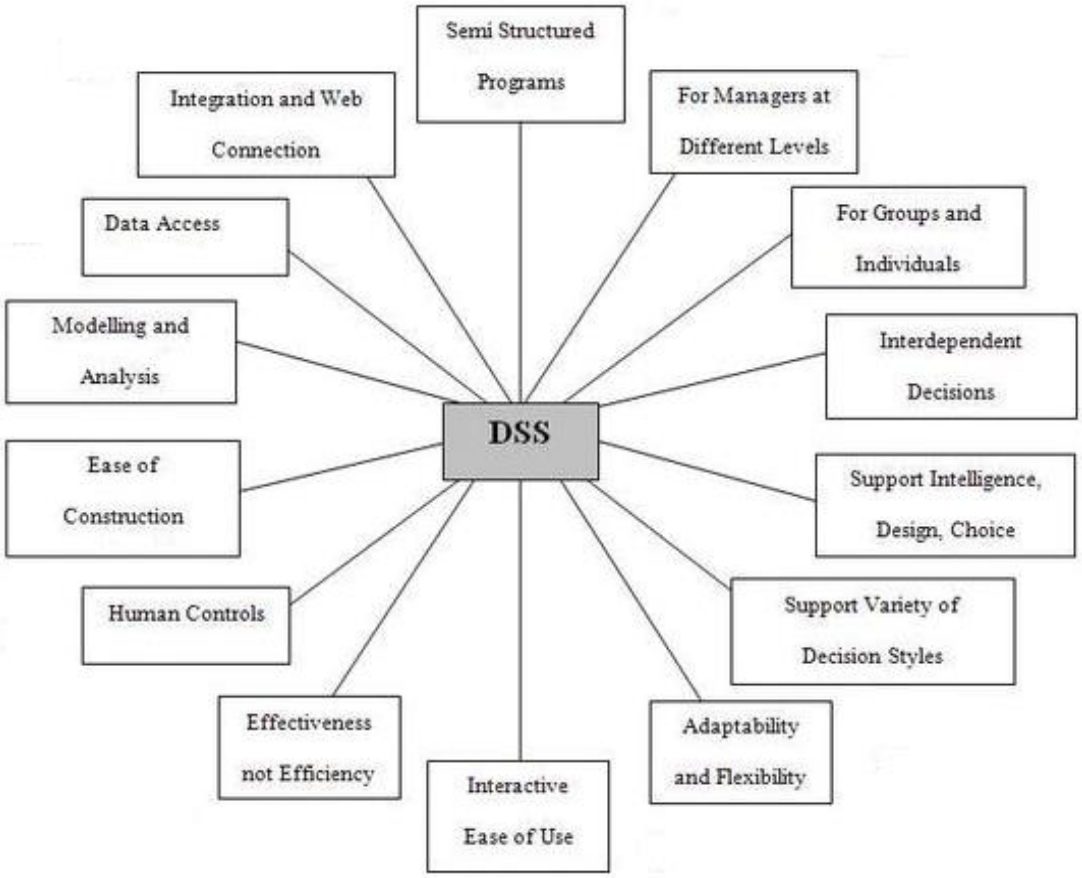

Рисунок 2.3 – Ідеальний набір характеристик СППР

2.5 Типи систем підтримки прийняття рішень

Як зазначалося вище СППР можна розділити на багато категорій наприклад:

− СППР керовані даними (Data driven DSS) – це СППР які фокусуються на доступі до внутрішніх даних компаній, а також коли це потрібно на зовні дані, та маніпулюють ними;

− СППР керовані моделями (Model-Driven).СППР що керуються моделлю яка може походити з різних дисциплін таких: бухгалтерські моделі, моделі оптимізації, фінансові моделі тощо. Такі системи не вимагають великих баз даних адже вони спираються на маніпулювання та доступ до моделі ніж до даних;

− СППР керовані знаннями (Knowledge driven). Такі СППР надають оператору пропозиції та / чи рекомендації засновані на аналізі певної бази знань, це повинно допомогти операторові в прийнятті вірного рішення;

− СППР керовані документами (Document driven). Такі СППР допомагають операторові в керуванні та отриманні неструктурованих документів та веб сторінок впроваджуючи різні технології для обробки та зберігання, щоб забезпечити аналіз та пошук документів. Ці системи надають операторові неструктуровані. Система також має доступ до різних документів наприклад: протоколів засідань компанії, політики компанії, корпоративні записи, специфікація продукції, історичні документи компанії, тощо, а також зазвичай для конкретного завдання керується пошуковою системою;

− СППР керовані комунікацією (Communication driven). Такі СППР ще називають груповими тому, що вони використовують моделі прийняття рішень та комунікацію для прийняття вірного рішення операторами які працюють в групі. Як правило такі СППР підтримують обмін документами, планування та електронну комунікацію для підняття продуктивності а також прийняття рішень, вони також застосовують такі технології як електронна пошта, двостороннє інтерактивне відео, тощо;

− Внутрішні та між організаційні СППР (Inter-and Intra-organization DSS). Такі системи виникли завдяки стрімкому зростанню Інтернету та інших мережевих технологій: WAN, LAN, тощо. Між організаційні СППР застосовуються для обслуговування клієнтів, постачальників компанії, тощо, в той час як внутрішньо організаційні СППР спрямовані на конкретні групи користувачів та людей в компанії.

2.6 Управління ризиками

Ризик – це можливість потенційної шкоди, яка може виникнути в результаті виконуваного процесу або майбутньої події.

Менеджмент ризиків – це дуже важливий процес адже він повинен виявляти можливі неполадки системи, визначати її слабкі місця, загрози при експлуатації системи, а також робити все щоб уникати такі ситуації або ж якщо це неможливо, то зменшити збитки від можливих загроз.

Процес менеджменту ризиків включає в себе аналіз, виявлення та реагування на ризик. Управління ризиками допомагає зрозуміти квінтесенцію всієї системи, визначити її найслабші місця, а також зрозуміти всі її можливості, процес менеджменту ризиків складається з певної послідовності кроків та методів які повинні зменшити вплив і ймовірність незапланованих подій, а також підвищити ймовірність сприятливих подій.

Існує чотири етапи менеджменту ризиків:

− планування: включає в себе розробку плану реагування, ідентифікацію та кількісну оцінку;

− реагування: включає в себе нагляд за ризиками та реагування на події пов’язані з ризиками;

− Оцінка плану ризиків;

− Доопрацювання плану ризиків для покращення плану управління ризиками та механізмів реагування, а також оновлення рівнів ризику.

2.7 Оцінка ризиків безпеки для підтримки прийняття рішення в умовах загроз

Системи оцінки ризиків інформаційної безпеки підтримують тих, хто приймає рішення, в оцінці та розумінні ризиків, яким піддається їх організація.

Цей процес дуже складний та потребує висококваліфікованих працівників, а також потрібні даних та знання з питань безпеки які більшість середніх чи малих організацій зібрати не в змозі. Саме в таких випадках можливо використовувати полегшену систему оцінки ризиків концепція якої показана на рисунку 2.4.

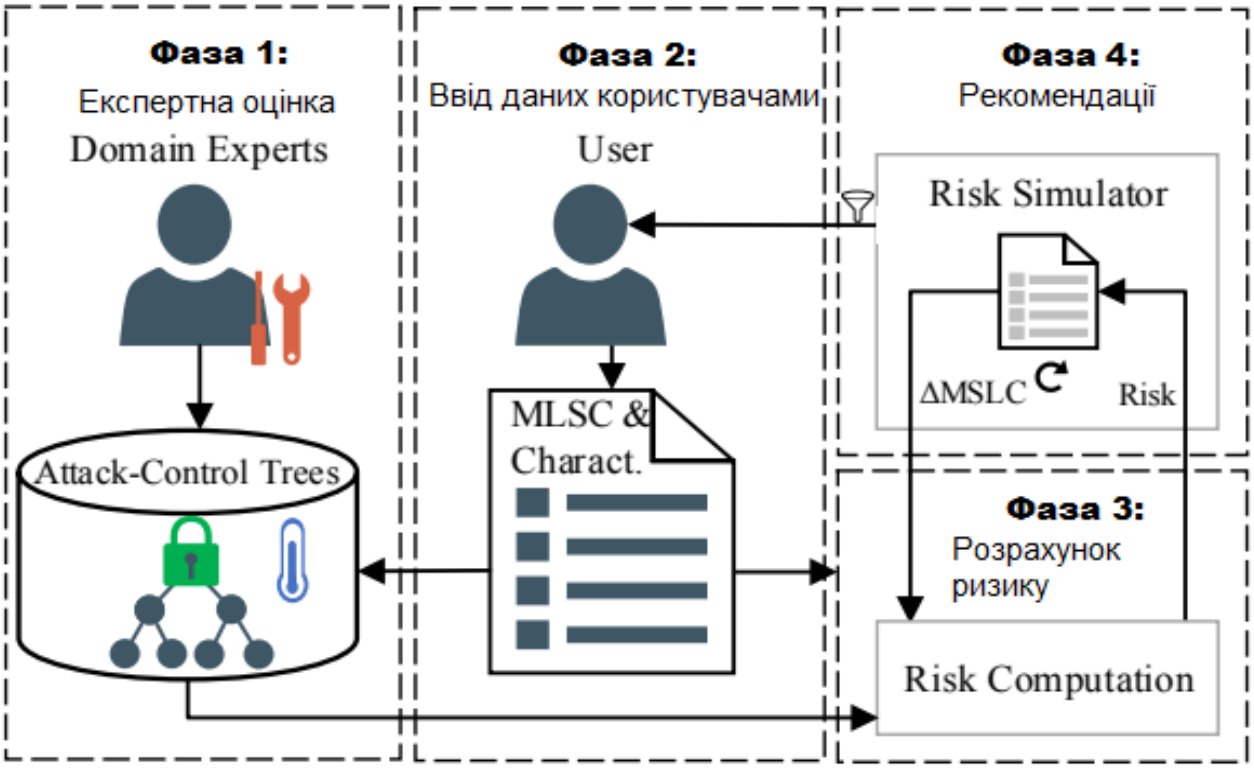

Рисунок 2.4 – Концепція полегшеної системи оцінки ризиків

Така система включає в себе чотири етапи:

– Перша фаза – експертна оцінка. Під Час цього етапу експерти доменів будують дерева атак, пов’язані з контролем за безпекою. В подальшому користувач може обирати домен в якому працює його організація, це робиться для того, щоб оцінка ризику враховувала тільки відповідні дереві атак для певного домену.

– Друга фаза – ввід даних користувачами. Дана фаза потребує тільки ввід користувачами даних про рівні зрілості засобів контроля безпеки підприємства.

Вони використовуються для моделювання реалізованих практик в полегшеній формі.

– Третя фаза – розрахунок ризиків. Перш ніж приступити до розрахунку ризику, необхідно усунути контрольні залежності. Це необхідно, оскільки ефективні рівні зрілості можуть бути нижче фактичних рівнів. Процес розрахунку ризиків показаний на рисунку 2.5.

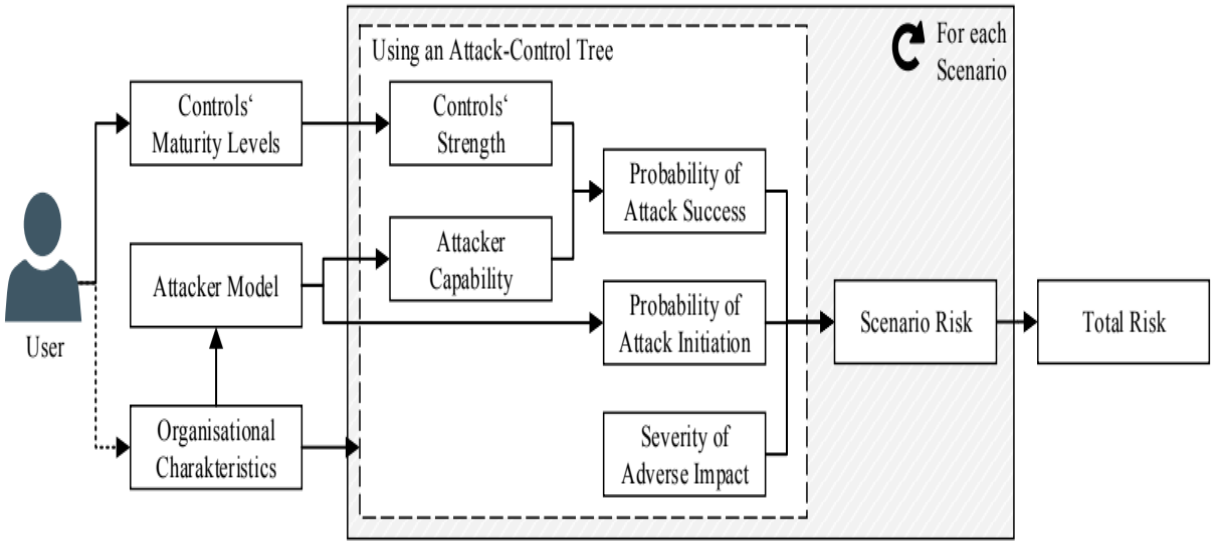

Рисунок 2.5 – Процес розрахунку ризиків

По-перше, загальний ризик визначається з сценарних ризиків які розраховуються на основі як ймовірності несприятливого впливу так і його серйозності. Ймовірність несприятливого впливу – це ймовірність того, що атака буде ініційована, та завершиться успіхом. Ці фактори розраховуються за допомогою дерев атак.

Четверта фаза – рекомендації. Система надає найбільш ефективні та найбільш економічно ефективні заходи щодо забезпечення безпеки.

2.7.1 Фази системи оцінки ризиків

Перша фаза

Експертна оцінка. Спочатку експерти встановлюють рамки для конкретної області. Вони збирають інформацію щодо можливих сценаріїв атак і на основі отриманих даних створюють дерева атак, та підключають до них відповідні засоби контролю безпеки – дерева контролю атак. Дерева контролю атак дозволяють визначити на скільки і як ефективно застосовувані засоби безпеки захищають від атак, сценаріїв атак, та пов’язаних з ними негативних наслідків. Для забезпечення актуальності системи, експерти регулярно або ж при необхідності оновлюють дані.

Експертна оцінка включає в себе наступні етапи:

− Ідентифікація сценаріїв атак. Загалом цей процес не забирає багато часу адже як правило експерти вже мають колекцію сценаріїв атак, оскільки більшість підходів до оцінки ризиків в управлінні безпекою засновані на сценаріях.

− Оцінка несприятливого впливу. Оцінка впливу є важливим фактором при розрахунку ризику, оскільки вона відображає ймовірні втрати, які можна очікувати від сценарію атаки.

− Створення дерев атак. Підтверджені сценарії атак перетворюються в дерева атак. Дерева атак мають методи аналізу загроз і ризиків для систематичного аналізу можливих шляхів атак.

− Після того як дерева атак побудовані, активи призначаються відповідним вузлам. Зіставлення між активами і кроками атаки дозволяє дізнатися, які атаки або кроки атаки вимагають застосування яких активів для успішного завершення. Це використовується на наступному етапі для індивідуалізації дерев атак.

− Призначення засобів контролю. Засоби контролю безпеки застосовуються на дерева атак щоб отримати дерева контролю атак що зв'язують захист і атакуючу перспективу. З цього слідує, що дерева контролю атак дозволяють визначити, в якій мірі запроваджені засоби контролю безпеки захищають від сценаріїв атак і пов'язаних з ними негативних наслідків.

− Оцінка ефективності контролю. Після побудови дерев вони параметризуються, починаючи з ефективності контролю. Цей параметр відображає, наскільки ефективно контроль буде в середньому (в даній області) захищати від дій зловмисника при правильній реалізації. Наприклад, навіть дуже розвинена програма підвищення обізнаності про безпеку може бути дуже ефективною в навчанні співробітників розпізнавати фішингові атаки, але вона може бути набагато менш ефективною проти більш специфічних і складних атак. Це показує, що параметр не залежить від фактичного рівня реалізації контролю.

− Оцінка витрат на атаку. Під витратами на атаку розуміється не тільки в грошовому сенсі, а й також у сенсі необхідних ресурсів. Передбачається, що жодна атака не може бути здійснена безкоштовно. У розрахунку ризику фаза, витрати на атаку об’єднуються по дереву відповідно до передбачуваної моделі зловмисника.

Друга фаза

Після того, як структура була визначена експертами домену, експерти користувачі можуть вказати свої методи забезпечення безпеки і організаційні характеристики. Другу фазу можна розділити на наступні етапи:

− Оцінка рівнів зрілості. Безпека представлена рівнями зрілості засобів контролю безпеки організації. Рівні зрілості використовуються в якості заходів для кількісної оцінки статусу реалізації контролю безпеки. Чим вище рівень зрілості контролю, тим вище ймовірність того, що він є ефективним і безпечним. Таким чином він вносить великий внесок в організаційну безпеку.

− Опис специфічних організаційних характеристик. За потреби користувач введення описує специфічні організаційні потреби та інфраструктуру характеристик які впливають на рівень організаційного ризику. Користувачі мають можливість вибрати домен організації, а також створити, адаптувати і / або видалити дерева контролю атак, які використовуються для оцінки власної організації. Всі впровадження зроблені компаніями можуть бути вивчені експертами домену, щоб нові або модифіковані дерева могли бути використані і іншими організаціями. Таким чином, існує ітеративний процес поліпшення, який забезпечує хору якість.

Третя фаза

Розрахунок ризику**.** Загальний ризик визначається з сценарних ризиків, які розраховуються на основі як ймовірності несприятливого впливу так і його серйозності. Дана фаза включає в себе такі етапи:

− Дозвіл залежності управління. Заходи безпеки організації представлені засобами контролю безпеки, але багато елементів контролю залежать один від одного, тому їх ефект не може бути оцінений незалежно. З цього слідує, що, їх залежності повинні бути усунені якщо залежний елемент управління недостатньо розвинений, він може перешкодити іншим, більш зрілим, елементам управління бути більш ефективними. Наприклад, дуже досконалий і зрілий контроль периметра фізичної безпеки може виявитися марним, якщо відсутній контроль політики доступу. В подальшому ми будемо розрізняти сильні і слабкі залежності. При сильній залежності один елемент управління строго вимагає реалізації іншого елемента управління. Наприклад, обов'язкова умова захисту території за допомогою фізичного периметру безпеки є реалізація політики контролю доступу, таким чином, це сильна залежність. З іншого боку, залежність від політики організації в області інформаційної безпеки, наприклад, зазвичай є слабкими тому що ця політика, яка повинна бути визначена і затверджена керівництвом, впливає на інші елементи управління в меншій мірі. Для усунення цих залежності між елементами управління застосовується функція залежності.

− Оцінка ймовірності початку атаки. Коли залежності усунені, починається розрахунок ризиків. Першим кроком є оцінка ймовірності ініціації атаки, PI є [0,1]. вона відображає ймовірність вибору конкретного варіанту атаки, оскільки (в разі операцій АБО) атакуючий може вибирати між різними варіантами атаки. Припускається, що атакуючий завжди вибирає варіант атаки, який максимізує його корисність. Тобто окреслюються одномоментні атаки, коли атакуючий виконує тільки кращу атаку. Це моделюється наступним обмеженням, визначальним. що сума зважених рішень для під дерева дорівнює 1, це відображено в рівняння 2.1.

$$\sum_{i \epsilon J} PI_{ij} = 1 \tag{2.1}$$

− Оцінка ймовірності успіху атаки. Визначаємо ймовірність успіху атаки, PS є [0,1], як ймовірність того, що атака або крок атаки, будучи розпочатою, увінчається успіхом. Таким чином, вона також визначається ймовірністю початку атаки. Він розраховується за допомогою деревоподібного алгоритму, мета якого – визначити в якій мірі запроваджені засоби контролю безпеки захищають від сценаріїв атаки або етапів атаки після початку атаки.

− Агрегування витрат на атаку. У більшості випадків рішення про атаку приймаються під впливом вартості атаки. Тому необхідно оцінити вартість атаки для кожного етапу атаки в дереві атак, для цього, спочатку зібрані витрати на атаку для дій атакуючого об’єднуються вгору по дереву. У разі внутрішніх вузлів з операціями І атакуючий повинен виконати обидва кроки атаки, тому витрати на атаку підсумовуються. В разі операцій АБО очікування витрат на атаку для успішної атаки розраховуються шляхом зважування витрат на атаку з ймовірністю ініціації. Таким чином витрати на атаку об’єднуються так само, як і ймовірність успіху атаки.

− Оцінка ризику. Ризик для окремого сценарію R_s є [0,1], визначається як добуток ймовірності успіху атаки і величини несприятливого впливу для сценарію s. PS_s та I_s відносяться до кореневого вузла сценарію s, відповідно до рівняння 2.2.

$$R_s = PS_s I_s \tag{2.2}$$

Загальний ризик, R є [0,1], підсумовує зважений ризик для кожного сценарію, відповідно до рівняння 2.3.

$$R = \sum_{s \in S} (PI_s R_s) \tag{2.3}$$

Четверта фаза

Рекомендації. Після того як ризик обчислений, визначені заходи щодо забезпечення безпеки. Одним з варіантів є ручна перевірка результатів аналізу ризику. Якщо загальний ризик вказує на необхідність вжиття заходів, можна пройтися по списку сценаріїв, щоб визначити сценарії з високим ризиком.

Потім користувачі можуть вручну перевірити відповідні дерева контролю атак, наприклад, щоб визначити найбільш впливових елементів управління для цих сценаріїв з високим ризиком. Ручна перевірка також дозволяє оцінити ризик для дуже специфічних кроків атаки.

Однак більш швидкий і об'єктивний підхід для всебічного аналізу є використання рекомендаційного додатку, який автоматизує процес перевірки. Додаток може використовуватися для отримання рекомендацій по найбільш ефективним і найбільш економічно вигідним заходам щодо забезпечення безпеки. Дана фаза включає в себе такі етапи:

− Спочатку рекомендаційний додаток визначає найбільш ефективні заходи щодо забезпечення безпеки;

− Потім визначається найбільш економічно ефективні заходи щодо забезпечення безпеки. Рекомендаційна програма заснована на аналізі витрат та користі співвідносить список першого рекомендаційного додатки (що містить найбільш ефективні заходи щодо забезпечення безпеки) з відповідними витратами на забезпечення безпеки;

− Останній етап надання прозорих рекомендацій. Користувачам крім самих рекомендацій, видається також обґрунтування рекомендацій з допомогою графічного інтерфейсу пояснення. Пом'якшувальні ефекти

рекомендацій представлені користувачеві різними способами. Він може вибрати між перспективою, орієнтованої на сценарій, і перспективою, орієнтованої на рекомендації. Сценарно-орієнтована перспектива протиставляє ефекти всіх рекомендацій для конкретного сценарію, в той час як перспектива, орієнтована на рекомендації, ілюструє пом'якшувальні ефекти конкретної рекомендації для кожного сценарію.

Висновки до розділу 2

В даному розділі було розглянуто історію виникнення систем підтримки прийняття рішень, опис та визначення систем підтримки прийняття рішень, вимоги до управління систем підтримки прийняття рішення, ідеальні характеристики та можливості СППР, типи систем підтримки прийняття рішень таких як: СППР керовані даними, СППР керовані моделями, СППР керовані знаннями, СППР керовані документами, СППР керовані комунікацією, внутрішні та міжорганізаційні СППР. Також було розглянуто управління ризиками та фази спрощеної системи оцінки ризиків.

Оцінка ризиків інформаційної безпеки є однією з основних обов'язків осіб, які приймають рішення в області інформаційної безпеки.

Цей процес дуже складний та потребує висококваліфікованих працівників, а також потрібні даних та знання з питань безпеки які більшість середніх чи малих організацій зібрати не в змозі

РОЗДІЛ 3
МЕХАНІЗМИ ПРИЙНЯТТЯ РІШЕНЬ В СИСТЕМАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ

3.1 Класифікація загроз безпеки при обробці персональних даних в типових інформаційних системах персональних даних

Під загрозами безпеки персональних даних під час їх обробки в ІСПДн вважається перелік факторів та певних умов за яких можливе створення небезпеки витоку персональних даних та/або неправомірного доступу до ІСПДн або ж не навмисні дії на систему. Отже, це означає, що загроза безпеці персональних даних при їх обробці може виникнути через не навмисні дії персоналу ІСПДн, або ж може здійснюватися навмисно певними групами, організаціями чи окремими громадянами.

Загрози безпеки персональних даних в ІСПДн можна розділити по таких ознаках:

− за типами вірогідних джерел загроз;

− за способами реалізації загроз;

− за видом ІСПДн, на які направлена загроза;

− по об'єкту впливу;

− за типом неправомірних дій здійснюваних щодо персональних даних;

− по використаній вразливості.

Для ІСПДн виділяють такі типи загроз безпеки персональних даних:

− Відносно джерела загрози виділяють:

1. Загрози зумовлені навмисними або не навмисними діями осіб, що мають доступ до певних ресурсів ІСПДн, також такі загрози включають користувачів, які можуть стати причиною загроз в самій ІСПДн;

2. Загрози зумовлені навмисними або не навмисними діями осіб, що мають зовнішній доступ до певних ресурсів ІСПДн і обумовлюють загрози зовнішніх мереж зв’язку та/ або міжнародного обміну даними;

3. Загрози які виникають через властивості і певні можливості обладнання яке використовується в ІСПДн;

4. Загрози пов’язані за стихійними лихами.

Також загрози можуть виникати через шкідливе програмне забезпечення.

− За видом ІСПДн на які націлена загроза, необхідно розглянути такі види загроз:

1. Загрози безпеці даних, оброблюваних в ІСПДн на базі автоматизованих робочих місць;

2. Загрози безпеці даних, оброблюваних в ІСПДн на базі локальних інформаційних систем;

3. Загрози безпеці даних, оброблюваних в ІСПДн на базі розподілених систем.

− За способом реалізації загроз:

1. Загрози неправомірного доступу до персональних даних а також загроза появи шкідливого програмного забезпечення;

2. Загроза втрати персональних даних технічними каналами зв’язку;

3. Загроза навмисного тиску на ІСПДн;

− Згідно з застосованою вразливістю виділяють такі загрози:

1. Загрози які використовують «діри» в системному програмному забезпеченні;

2. Загрози які використовують програмні помилки прикладного програмного забезпечення;

3. Загрози які виникають через вразливості мережевих протоколів та каналів зв’язку;

4. Загрози які виникають через помилки в технічній організації захисту персональних даних від несанкціонованого доступу;

5. Загроза втрати персональних даних технічними каналами зв’язку;

6. Загрози які використовують недоліки в засобах захисту інформації.

− Спираючись на об’єкт впливу можна виділити наступні загрози:

1. Загрози персональним даним, оброблюваним в АРМ;

2. Загрози безпеки персональних даних які передаються мережею;

3. Загрози програмному забезпеченні яке гарантує функціонування ІСПДн.

3.2 Характеристика джерел загроз безпеки персональних даних в інформаційних системах персональних даних

Існують такі типи загроз безпеки персональних даних в ІСПДн:

− Антропогенні джерела загроз безпеки персональних даних;

− Техногенні джерела загроз безпеки персональних даних;

− Стихійні джерела загроз безпеки персональних даних.

Джерелом антропогенної загрози може бути суб’єкт який має правомірний або ж неправомірний доступ до системи або її компонентів, що може призвести до порушення безпеки персональних даних. В відношенні до ІСПДн такі загрози можуть бути як зовнішні так і внутрішні. В зовнішніх загрозах виділяють випадкові і невипадкові джерела.

− Випадкові – такі загрози з’являються від незнання чи неуважності персоналу обслуговуючого ІСПДн, тощо до джерел таких загроз можна віднести помилки та вразливості які виникли при проектуванні і впровадженні ІСПДн, різні неполадки та перебої в роботі ІСПДн;

− Не випадкові (навмисні) джерела – при таких загрозах зловмисники навмисно виводять системи з ладу, змінюють або видаляють чи викрадають інформацію шляхом несанкціонованого доступу до ІСПДн;

Основний персонал, чи персонал служби безпеки, допоміжний чи технічний персонал, це як правило спеціалісти в області програмного забезпечення чи захисту даних можуть бути внутрішніми джерелами загроз тому, що вони мають доступ до штатного обладнання та до первинного коду програм.

Особливе місце також займають загрози які виникли внаслідок порушень правил експлуатації, чи внаслідок неправильних дій персоналу, що мають доступ до ІР ІСПДн, зокрема до таких відносяться:

− Ненавмисне перероблення або видалення програмних компонентів системи;

− Імплементація і використання неперевірених/непідтверджених програм;

− Ігнорування правил при роботі з ресурсами ІСПДн, особливо з засобами захисту інформації. Наприклад:

1. Недотримання правил зберігання інформації обмеженого доступу, котра застосовується при роботі з засобів захисту інформації;

2. Надання не уповноваженим особам доступ до засобів захисту інформації, чи до інших програмних чи технічних засобів захисту інформації;

3. Налаштування та конфігурація засобів захисту інформації, чи будь-яких інших програм яка б суперечила нормативній чи технічній документації;

4. Замовчування факту крадіжки будь якої важливої інформації.

Очевидно що найбільшу загрозу становлять навмисні дії, звідки б вони не походили чи то з зовнішніх чи внутрішніх джерел. Варто приділити увагу таким внутрішнім антропогенним загрозам:

− Загрози які спричинені навмисними діями певних осіб, які в свою чергу мають правомірного доступу до ІСПДн. Такими внутрішніми порушниками можуть бути користувачі ІСПДн чи працівники які працюють з ІСПДн;

− Загрози які спричинені навмисними діями певних осіб, які в свою чергу не мають правомірного доступу до ІСПДн, і загрожують системі з зовнішніх мереж.

Техногенні джерела загроз також можуть бути як зовнішніми так і внутрішніми.

Зовнішні – це всі елементи інфраструктури ІСПДн: мережі інженерних комунікацій (каналізація, опалення, водопостачання, тощо), засоби зв’язку (мережі передачі даних, телефонні лінії, тощо).

Внутрішні – це програмні та технічні засоби, які використовуються в ІСПДн, а також засоби обробки інформації та інші засоби (телефонії, охорони, тощо) і також шкідливе програмне забезпечення.

3.3 Визначення задач системи підтримки прийняття рішень для організації захисту персональних даних

Після повного аналізу процесів забезпечення безпеки персональних даних можна чітко виділити основні задачі системи підтримки прийняття рішень.

Серед них варто виділити три основні задачі:

− Систематизація і накопичення знань про інформаційну систему в якій виконується обробка персональних даних;

− Підтримка прийняття рішення при розробці системи захисту персональних даних;

− Підтримка прийняття рішення при використанні системи захисту персональних даних.

Кожна з виділених задач також може включати в себе під задачі. Отже, в одній виділеній задачі підтримки прийняття рішення при розробці потрібно звернути увагу і вирішити такі під задачі підтримки прийняття рішення при виділенні і класифікації ІСПДн підтримки прийняття рішення при розгляді загроз безпеки ПДн а також їх актуальності підтримки прийняття рішення при визначенні необхідних засобів захисту проведення аналізу ризиків.

Узагальнену схему принципу роботи СППР зображено на рисунку 3.1

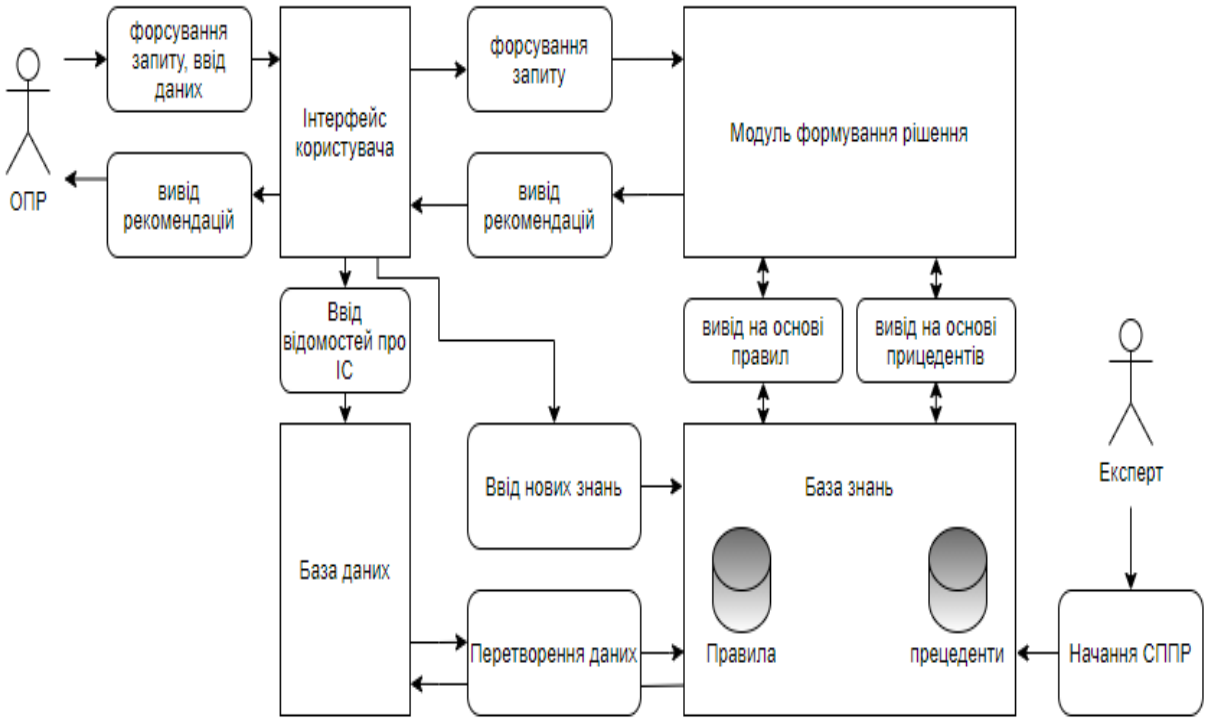

Рисунок 3.1 – Узагальнена схема принципу роботи СППР

Використання СППР виконується наступним чином: ОПР заносить в СППР дані відносно змін в інформаційній системі і створює запит на отримання рекомендацій або ж на отримання аналізу ризиків. Зважаючи на отримані результати СППР проводить аналіз і визначає яким чином зміни відобразилися на структурі ІСПДн, загрозах безпеки персональних даних або ж засобів захисту і видає відповідні рекомендації. Якщо особа яка приймає рішення, затверджує рекомендації, то вони вносяться до бази даних.

Навчання бази знань відбувається наступним чином: для формулювання рекомендації найчастіше використовуються дві системи перша на основі правил а друга на основі прецедентів в випадки коли не вдається знайти рішення при використанні правил то виконується пошук в базі прецедентів. Якщо пошук по базі прецедентів безрезультатний, то користувачу системи надається можливість створити новий прецедент.

3.4 Система управління базою даних

СППР буде продуктивною тільки тоді коли вона підтримуватися добре розробленою та спроектованою базою даних. А це означає, що щоб СППР функціонувала на всі «сто» відсотків повинна бути розроблена структура для збереження, маніпулювання, доступу та отримання гігантських об’ємів даних. Хороша СУБД повинна забезпечувати цілісність даних, логічність черговості даних, доступність даних.

Найчастіше при розробці СППР надають перевагу реляційним базам даних. Насамперед це пов’язано з тим що застосовуючи реляційні бази даних можна зменшити дублювання даних, а також через багатогранні можливості налаштування таких баз даних, також це обумовлено тим, що такі бази даних можуть запам’ятовувати зв’язки між об’єктами, та робити аналіз інформації.

3.5 Механізм прийняття рішення в СППР

Вибір рішення найчастіше відображається як вибір: це може бути вибір напряму дії, стратегії дій, вибір який в кінці повинен привести нас до певної бажаної цілі. Це дає нам точно зрозуміти, що вибір рішення є цілком не випадковим тому, що потрібно вибрати один напрям серед мільйонів стратегій, в свою чергу СППР створюється для пришвидшення та спрощення цього тяжкого і вартісного процесу.

Процес прийняття рішення включає в себе три ключові етапи: ідентифікація проблеми, її вивчення та вибір. Хоча Тюрбан казав що також потрібна стадія реалізації, адже якщо її не буде, то процес прийняття рішення так і зостанеться тільки на папері.

Етап ідентифікації це процес при якому вже є усвідомлення того, що бажаний результат не відповідає поточному. Особа яка приймає рішення докладає всі зусилля для виявлення суті проблеми яку необхідно вирішити.

На етапі вивчення особа яка приймає рішення повинна аналізувати можливі альтернативні варіанти з метою отримання корисних знань а також для розуміння їх можливих наслідків.

На етапі вибору особа яка приймає рішення вибирає одну з наданих альтернатив які вивчалися в період другого етапу. Іноді буває так, що жодна з альтернатив не підходить, в такому випадку все повертається до фази вивчення, або ж якщо після проведення аналізу можливих варіантів контекст проблеми змінився, то все повертається до першого етапу ідентифікації проблеми.

Останній етап – реалізація, тобто всі відібрані рішення повинні бути виконані. Якщо проблема вирішена то процес прийняття рішення завершується якщо ж ні, то вона вважається невдачею і переходить до попереднього етапу.

3.5.1 Структура рішення

Спираючись на конкретні фактори використовуючи які можна класифікувати рішення. Оцінка рішень здатна допомогти особам, які приймають рішення, зрозуміти, які знання та будуть потрібні в системі підтримки прийняття рішень. Саймон описував, що рішення можуть поділятися від високо структурованих до повністю не структурованих. Рішення також можуть бути класифіковані як одноетапні та багатоступеневі, з ризиком, визначеністю чи невизначеністю результату.

Структуровані рішення приймаються за умови якщо добре відомі процедури, можуть легко бути впроваджені до всіх етапів прийняття рішення.

Вони описуються певними критеріями прийняття рішення такими як: обмеженою кількістю альтернатив, наслідки яких можуть бути оброблені без ускладнень.

Напівструктуроване рішення приймається, коли деякі, але не всі фази прийняття рішення структуровані. Але також можливе застосування стандартних процедур вирішення.

Якщо ні один з етапів прийняття рішення не структурований, то отримані рішення класифікуються як неструктуровані.

Якщо є проблема є невизначеною (погано структурованою), то рішення приймаються як напівструктуровані та неструктуровані. Таблиця 2.1 відображає особливості структурованих та неструктурованих рішень.

Таблиця 3.1– Структурованість рішень

Структуровані рішення	Неструктуровані рішення
Звичайні, повторювані	Несподіваний, не частий
Сформований та стабільний контекст	Виниклий та бурхливий контекст
Зрозумілі альтернативи	Незрозумілі альтернативи
прямолінійні наслідки альтернатив	невизначені наслідки альтернатив
чітко визначені критерії вибору	Критерії вибору неоднозначні
Потрібні конкретні знання	Конкретні знання потребують невідомості
Необхідні знання, легко доступні	Потрібні знання недоступні
Результат спеціалізованих стратегій (тобто процедур, які чітко попередньо визначають повний набір кроків, яких слід дотримуватися для прийняття рішень	Результат загальних стратегій (наприклад, аналогія, латеральне мислення, мозковий штурм, синтез, що використовується під час прийняття рішень)
Опора на традиції	Опора на дослідження, креативність, проникливість, винахідливість

3.5.2 Багато атрибутивні методи прийняття рішення

В випадках коли потрібен суворий підхід який застосовує знання предметної області до неструктурованих (адаптивних) проблем, щоб описати їх як структуровані проблеми використовують інструмент MADM Multi-attribute decision-making.

Квінтесенцією багато атрибутивні методології прийняття рішень є матриця рішення з m критеріями та n альтернативою (див. рисунок 3.2). В матриці Ci, ..., Cm та Ai, .., An вказують критерії та альтернативи відповідно: кожен рядок належить критерію, а кожен стовпець описує ефективність альтернативи.

Зазвичай вважається, що більш висока оцінка означає кращі показники.

		x_1	·	·	x_n
		$\mathbf{A}_1$	·	·	$\mathbf{A}_n$
w_1	$\mathbf{C}_1$	a_{11}	·	·	a_{m1}
·	·	·	·	·	·
·	·	·	·	·	·
w_m	$\mathbf{C}_m$	a_{m1}	·	·	a_{mn}

Рисунок 3.2 – Матриця рішення

Wi, ..., Wm присвоюються критеріям. Wi відображає відносну важливість критеріїв Ci для прийняття рішення і вважається позитивною.

3.5.3 Теорія багатокористувацької корисності

Теорія багатокористувацької корисності базується на використанні службових функцій. Службові функції використовуються для кількісної оцінки переваг того, хто приймає рішення, шляхом розподілу числового індексу для різних ступенів задоволеності, оскільки розглянутий атрибут приймає значення між найбільшою та найменш визначеною межею

Значення корисності оцінюються шляхом нормалізації результатів симульованих тестів. Нормалізація показників ефективності проводиться з використанням мінімальних і максимальних обмежень, отриманих в результаті моделювання.

3.5.4 Аналітична ієрархія

Метод аналітичної ієрархії належить до адаптивних методів зважування, і включає в себе три етапи:

− декомпозицію;

− порівняння судження;

− синтез пріоритетів.

Щоб визначити прихильність користувачів застосовують шкалу величин від 1 до 9, де 1 – це найменша прихильність, а 9 – це найвища прихильність.

Порівняння відображають транзитивною матрицею, щоб i, j > j та j > k , то i > k, де i, j та k є елементами дії. Для кожного j > k > i відповідних $a_{ij} = 1 / a_{ji}$.

За рахунок нормалізації матриці обчислюють переваги для вектору пріоритету відповідно до рівняння (3.1).

$$AW = \lambda max. W, \tag{3.1}$$

де A – матриця порівняння,

W – власний вектор, λmax – власне, максимальне значення матриці.

Для визначення того чи порушують транзитивність рішення і в якій мірі, використовують індекс CI. Якщо значення перевищують показник 0.10, то значення CI розраховують за коефіцієнтом згідності відповідно до рівняння (3.2).

$$CR = \frac{CI}{RI}, \tag{3.2}$$

де RI – індекс коефіцієнта.

CI вираховується відповідно до рівняння (3).

$$CI = \frac{\lambda - n}{n-1}, \tag{3.3}$$

де λ max – власне, максимальне значення матриці,

n – це розмірність.

3.5.5 Методи випередження

Метод випередження діє як одна з альтернатив для вирішення складних проблем вибору з кількома критеріями та кількома учасниками. Найпопулярнішими методами випередження це: ELECTRE та PROMETHEE.

Основною задачею метода ELECTRE є вибір альтернативи, яка поєднує дві умови з узгодженості переваг на багатьох оцінках з конкурентом, а

розбіжність переваг контролювалася багатьма варіантами порівняння. Основою є дані матриці рішення, що передбачає, що сума ваг дорівнює 1 .

Відповідно до рівняння (3.4) , для впорядкованої пари альтернатив (A_j, A_k) індекс відповідності C_{jk} це сума всіх ваг для тих атрибутів, де загальна продуктивність A_j є найменшою за A_k.

$$C_{jk} = \sum_{a_{ij} \geq a_{ik}} w_i, \tag{3.4}$$

де $j, k = 1, \dots, n, j \neq k$

Індекс відповідності повинен знаходитись від 0 до 1.

Більш складним є розрахунок d_{jk} . Якщо A_j працює краще, ніж A_k за всіма критеріями, індекс невідповідності буде нульовим. Якщо ж ні, то буде розраховуватися відповідно но рівняння (3.5):

$$d_{jk} = max \frac{a_{ik} - a_{ij}}{max\, a_{ij} - min\, a_{ij}}, \tag{3.5}$$

де $j, k = 1, \dots, n, j \neq k$

Метод PROMETHEE. В цьому методі оцінки (оцінка вказує на кращі показники) таблиці рішень не обов'язково повинні бути нормалізовані або перетворені у безрозмірну шкалу. Також, передбачається, що з кожним атрибутом зв’язана функція переваги $PF_i(A_j, A_k)$ яка відображає степінь переваги варіанта A_j порівняно з A_k по критерію C_i :

– $0 \leq PF_i(A_j, A_k)$, і

– $PF_i(A_j, A_k) = 0$, без переваги байдужості;

– $PF_i(A_j, A_k) \approx 0$, слабка перевага;

– $PF_i(A_j, A_k) \approx 1$, сильна перевага, і;

– $PF_i(A_j, A_k) = 1$, сувора перевага.

В множині правдоподібних випадків PF_i є функцією відхилення $d = a_{ij} - a_{ik}$, дивитися рівняння (3.6):

$$PF_i(A_j, A_k) = PF_i(a_{ij}, a_{ik}), \tag{3.6}$$

де PF_i є функцією, що не зменшується

$PF_i(d) = 0$ для $d \leq 0$ і $0 \leq PF_i(d) < 1$ для $d > 0$.

В рівнянні (3.7) багатокритеріальний індекс переваги $\pi(A_j, A_k)$, A_j над A_k може бути обчислений з урахуванням усіх атрибутів:

$$\pi(A_j, A_k) = \sum_{i=1}^{M} w_i P_i(A_j, A_k) \tag{3.7}$$

Значення цього індексу становить від 0 до 1 і характеризує загальну інтенсивність переваг між парами вибору.

Для встановлення альтернатив використовуються наступні потоки випередження рівняння (3.8), та рівняння (3.9).

Позитивний потік випередження:

$$\varphi^{+}(A_j) = \frac{1}{n-1} \sum_{k=1}^{\Pi} \pi(A_j, A_k) \tag{3.8}$$

Негативний потік випередження:

$$\varphi^{-}(A_j) = \frac{1}{n-1} \sum_{k=1}^{\Pi} \pi(k, A_j) \tag{3.9}$$

Позитивний коефіцієнт вищого рейтингу описує, наскільки кожен варіант перевищує інші. Чим вище $\varphi^{+}(A_j)$, тим краща альтернатива.

Негативний потік випередження показує, наскільки кожна альтернатива перевершує інші. Чим менше $\varphi^{-}(A_j)$, тим краща альтернатива.

Методи TOPSIS. Це одні з найчастіше використовуваних методів для прийняття рішення.

Ключовою ідеєю методі являється те, що в геометричному сенсі вибраний варіант повинен знаходитися якомога ближче до сприятливого ідеального рішення, і якомога далі від несприятливого ідеального рішення.

Приклад цього метода модна показати наступними кроками:

1. Потрібно визначити ефективність n альтернатив над m атрибутами дивитися рівняння (3.10).

$$p_{ij} = \frac{x_{ij}}{\sqrt{{x_{ij}}^2}} \tag{3.10}$$

i = 1, …, m,

j = 1, …, n;

2. Використовуючи рівняння (3.11), оцінити зважені нормовані оцінки.

$$p_{ij} = w_j p_{ij} \quad (3.11)$$

w_j- віга j-го атрибута.

3. Потрібно знайти позитивно-ідеальну альтернативу A+.

4. Потрібно отримати негативно-ідеальну альтернативу A-.

5. Потрібно встановити відстані до кожного позитивно-ідеального (Si+), і до негативно-ідеального (Si−) елемента.

6. Знайти відношення C_i^+ відповідно до рівняння (3.12).

$$C_i^+ = \frac{S_i^-}{S^{i^-} + S^{i^+}} \quad (3.12)$$

Розширивши коефіцієнт з шостого кроку, впорядкувати кожен з варіантів.

Висновки до розділу 3

В даному розділі було розглянуто механізм прийняття рішень в системах підтримки прийняття рішення, була розглянута класифікація загроз безпеки при обробці персональних даних в типових інформаційних системах персональних даних, визначення задач систем підтримки прийняття рішень для формування захисту ПДн, система управління базою даних, та механізм прийняття рішень в системах підтримки прийняття рішень.

Процес прийняття рішення включає в себе три ключові етапи: ідентифікація проблеми, її вивчення та вибір. Прийняття рішення дуже важливий процес, адже від його точності буде залежати збереження персональних даних користувачів що в свою чергу тісно пов'язане з довірою людей до обраної ними організації, та на імідж компанії в цілому.

ВИСНОВКИ

Системи підтримки прийняття рішень стали одними з ключових елементів роботи як державних так і приватних організацій не тільки для захисту персональних даних, а в багатьох інших напрямках наприклад освіта, управління кадрами, виробництво, тощо. Також потрібно чітко розуміти, що з одного боку системи СППР можуть бути дуже корисними для різних організацій, а з іншого можуть бути причиною плутанини та не точного аналізу тому, що такі системи призначені для прийняття оперативних рішень, а аж ні як для виявлення «неправильних» рішень, і вся відповідальність за прийняте рішення лежить на операторові системи.

Отже на основі проведених досліджень можна зробити такі висновки:

Ціль роботи була виконана – на основі теоретичного дослідження були досліджені механізми захисту персональних даних користувачів в умовах загроз, показана актуальність проблеми і важливість впровадження подібних систем.

Було розглянуто основи захисту персональних даних а саме: історію виникнення питань з захисту персональних даних, поняття персональних даних, принципів інформаційної безпеки, способи порушення конфіденційності персональних даних, поняття вразливості систем, загроз та атак, а також було розглянуте шкідливе програмне забезпечення таке як: віруси хробаки, віруси-маскувальники, віруси-шпигуни, зомбі віруси, рекламні віруси, блокуючі-віруси троянські віруси. Також були розглянуті можливі носії шкідливих програм такі як: зовнішні носії, внутрішні носії, мікросхеми зовнішніх пристроїв, а також пакети даних які передаються мережею.

Також було розглянуто історію виникнення систем підтримки прийняття рішень, опис та визначення систем підтримки прийняття рішень, вимоги до управління систем підтримки прийняття рішення, ідеальні характеристики та можливості СППР, типи систем підтримки прийняття рішень таких як: СППР керовані даними, СППР керовані моделями, СППР керовані знаннями, СППР

керовані документами, СППР керовані комунікацією, внутрішні та міжорганізаційні СППР.

Також було розглянуто управління ризиками та чотири фази спрощеної системи оцінки ризиків такі як експертна оцінка, ввід користувачів, розрахунок ризику та рекомендації.

Також було досліджено механізм прийняття рішень в системах підтримки прийняття рішення, була розглянута класифікація загроз безпеки при обробці персональних даних в типових інформаційних системах персональних даних, визначення задач систем підтримки прийняття рішень для формування захисту ПДн, система управління базою даних, та механізм прийняття рішень в системах підтримки прийняття рішень. Процес прийняття рішення включає в себе три ключові етапи: ідентифікація проблеми, її вивчення та вибір.

Прийняття рішення дуже важливий процес, адже від його точності буде залежати збереження персональних даних користувачів, що в свою чергу тісно пов'язане з довірою людей до обраної ними організації, та на імідж компанії в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. .Description theory and choices: a complexity approach. 2010. 267 p.

2. Aalast W. M. Process mining. Discovery, performance and enhancement of business process. 2011. 370 p

3. adzic F. Mining of data with complex structures. 2011. 348 p.

4. Alex Berson, Stephen J. Smith Data Warehousing, Data Mining, and OLAP (Data Warehousing/Data Management). McGraw-Hill. 2010.

5. Alter S.A. A Study of Computer-aided Decision Making in Organizations : дис. докт. філос. наук. 1975.

6. Alter S.A. Decision Support Systems: Current Practices and Future Challenges. 1979.

7. Alter S.L. Decision support systems: current pactice and continuing challenges. 1980.

8. Bonczek, R., Holsapple C. and Whinston A., Foundations of Decision Support Systems. New York: Academic. 1981

9. Druzdzel M.J., Flynn R.R. Decision Support Systems. Encyclopedia of Library and Information Science. 1999.

10. George M. Marakas, Decision Support Systems in the 21st Century, 2nd Edition. Prentice Hall. 2002.

11. Golub, A. L. Decision Analysis: An Integrated Approach. New York. 1997.

12. Golub, A. L. Decision Analysis: An Integrated Approach. New York. 1997.

13. Holsapple C.W. Decision Support Systems (a knowledge bases approach). New York. 860p.

14. Hopple, G.W. The state of the decision support systems. USA. 1988. 246 c.

15. Keen P.G.W. Decision support systems: an organizational perspective. 1978.

16. Malware. TechTerms. URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/14337 (дата звернення: 07.06. 2025).

17. Mirkin B. Core concepts in data analysis: summarization, correlation and visualization. 2011. 412 p.

18. Sprague R.H. A Framework for the Development of Decision Support Systems. 1980.

19. Бідюк П.І. Проектування комп’ютерних інформаційних систем підтримки прийняття рішень : навч. посіб. Київ: КПІ. 2010. 340 с.

20. Волошин О.Ф. Моделі і методи прийняття рішень: Навч.посіб.для студ. вищ. навч. закл. Київ. 2010. 336 с.

21. Гайворовський М.В. Безпека інформаційно-комунікаційних систем: підручн. 2009. 608 с.

22. Гнатієнко Г.М. Експертні технології прийняття рішень. 2008. 444 с.

23. Демиденко М.А. Управління проектами інформатизації: навч. посібн. Дніпропетровськ: НГУ, 2014. 118 с

24. Кидираліна, Ахметов, Лахно. Моделювання процедури прийняття рішень щодо фінансування засобів кібербезпеки інформаційно-освітнього середовища університету. Захист інформації, Північна Америка, 20, чер. 2018. URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/12864 (дата звернення: 07.06.2025).

25. Коломицев, Носок, Тоцький. Порівняльний аналіз моделей оцінки зрілості інформаційної безпеки. Захист інформації, Північна Америка, 21, груд. 2019. URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/14337 (дата звернення: 07.06. 2025).

26. Корнеев В.В. Базы данных. Интеллектуальная обработка информации. 2000. 352 с.

27. Марценюк, Сверстюк. Про модель кібер-фізичної системи з атаками стану та вимірювань на основі стохастичних різницевих рівнянь. Захист

інформації, Північна Америка, 21, бер. 2019. URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/13543 (дата звернення: 07.06.2025).

28. Марченко А.В. Проектування інформаційних систем. 2015. 50 с.

29. Пушкар О. І. Системи підтримки прийняття рішень: навч. посібник. Харків: Інжек. 2006. 304 с.

30. Самохвалов, Браіловський. Оцінка інформаційної безпеки організації за критерієм впевненості. Захист інформації, Північна Америка, 21, бер. 2019. URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/13445 (дата звернення: 07.06.2025).

31. Ситник В.Ф. Системи підтримки прийняття рішень: навч. посіб. Київ: КНЕУ. 2009. 614 с.

32. Ткач Ю.М. Моделі систем захисту інформаційної сфери держави. Сучасна спеціальна техніка. 2020. №2 (61). С.59-66.