МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«19» 02 2024 р.

Кваліфікаційна робота
на правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА

Розробка моделей і алгоритмів побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконав: студент 6 курсу групи 6366м
Пархоменко Богдан Ігорович _____

Керівник:
д.т.н., професор кафедри КТІБ

Передерій Віктор Іванович _____

Миколаїв – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми, к.т.н.,
доцент, доцент кафедри КТІБ
_____ Турти М.В.
«19» 02 2024 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Пархоменко Богдан Ігорович

Курс:6

Група: 6366м

Ступінь вищої освіти: магістр

Галузь знань: 14 Електрична інженерія

Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: Розробка моделей і алгоритмів побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки.

затверджена наказом НУК від «14» жовтня 2024 р. № 1075 - уч

2. Вихідні дані до роботи: Моделі та алгоритми побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки.

3. Перелік питань, які необхідно розробити:

1.Провести аналіз та визначити основні особливості побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки.

2. Провести аналіз структурної організації розподілених адаптивних БД з забезпеченням комплексної інформаційної безпеки.

3. Визначити основні вимоги та постановку задачі побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки.

4. Розробити інформаційні та математичні моделі оцінки комплексної інформаційної безпеки при формуванні запитів в адаптивній розподіленій БД.

4. Терміни виконання завдання:

термін видачі завдання: «04» вересня 2024 р.

термін подання роботи: «19» грудня 2024 р.

6. План-графік виконання кваліфікаційної роботи

№ п/п	Заходи	Дата		Готовність	Відмітка про виконання
		Навч. тиждень	Контрольна дата		
1.	Наукове стажування	1 - 8	25.10.2024	Звіт з наукового стажування	
2.	Організаційні збори	9	31.10.2024	Попередній варіант змісту КР	
3.	Рубіжний контроль	10	05.11.2024	Попередній варіант оглядових розділів	
4.	Рубіжний контроль	13	28-29.11.2024	1. Попередній варіант повної КР. 2. Попередній варіант презентації.	
5.	Рубіжний контроль	15	12.12.2024	Доповідь на 12-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2024»	
6.	Перевірка на плагіат	15	12-13.12.2024	Електронний варіант кваліфікаційної роботи	
7.	КЕ на рівень « магістра»	16	17-18.12.2024	Здавання державного екзамену зі спеціальності на ступінь бакалавра	
8.	Кафедральний захист	16	19.12.2024	1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).	
9.	Подання документів на захист	16	20.12.2024	1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР. 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Електронний варіант та роздрукована презентація в кількості 5 примірників. 4. Електронний варіант КР на диску	
10.	Захист ДР	17	24,26,27, 28.12.2024	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.	

ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.

Керівник
д.т.н., професор кафедри КТІБ _____ В.І. Передерій

Студент _____ Б.І. Пархоменко

АНОТАЦІЯ

У даній роботі розроблені моделі та алгоритми побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки. Для забезпечення довгострокової та безвідмовної роботи АРБД в складі СППР розроблено комплекс заходів та програмне забезпечення до складу якого входять дві групи захисту.

Розроблена математична модель оцінки комплексної інформаційної безпеки та алгоритми функціонування розподіленої БД при формуванні запитів, з використанням теорії ймовірності Байесовської мережі довіри.

Проведено ряд експериментів з оцінки інформаційної безпеки та захищеності АРБД, результати досліджень яких показали значну перевагу запропонованих моделей і алгоритмів в порівняні з існуючими.

Ключові слова: безпека інформаційної інфраструктури, інформаційна захищеність, комплексна інформаційна безпека, Байесовські мережі довіри, теорії ймовірності, адаптивна база даних, розподілена база даних, система підтримки прийняття рішень, система управління базою даних, Інтелектуальний аналіз даних.

ANOTATION

In this work, models and algorithms for building a distributed adaptive database with comprehensive information security have been developed. To ensure long-term and trouble-free operation of the ARDB as part of the DSS, a set of measures and software has been developed, which includes two groups of protection measures.

A mathematical model for assessing comprehensive information security and algorithms for the functioning of a distributed database when forming queries has been developed, using the probability theory of the Bayesian trust network.

A number of experiments have been conducted to assess the information security and security of an adaptive distributed database, the results of which have shown a significant advantage of the proposed models and algorithms in comparison with existing ones

Keywords: information infrastructure security, information security, comprehensive information security, Bayesian trust networks, probability theories, adaptive database, distributed database, decision support system, database management system, Data mining.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БД – база даних

АБД – адаптивна база даних

РБД – розподілена база даних

АРБД – адаптивна розподілена база даних

ППП – пакет прикладних програм

ПЗ – програмне забезпечення

СППР – система підтримки прийняття рішень

БМ – Байєсівські мережі

БМД – Байєсівські мережі довіри

СУБД – система управління базою даних

БЗ – база знань

ІПС – інформаційно-пошукова система

CASE – Computer Aided System Engineering

ОПР - - Особа що Приймає Рішення

ІБ - - Інформаційна безпека

СОТО - - Складний організаційно-технічний об’єкт

ІАД - - Інтелектуальний аналіз даних

СОД - - Система обробки даних

ІАС - - І нформаційно-аналітична система

WEB - - Веб - середовище

SQL - - structured query language

ВСТУП

Актуальність. Сучасні БД - це складні багатофункціональні програмні системи, що працюють у відкритому розподіленому середовищі. Вони вже сьогодні доступні для використання в діловій сфері і виступають не просто в якості технічних і наукових рішень, але і як завершені продукти, надають розробникам потужні засоби управління даними і інструментарій для створення прикладних програм і систем.

Розподілені бази даних (РБД) з'явилися як наслідок розвитку розподілених систем різного призначення і, в першу чергу, інформаційно-пошукових систем (ІПС), інтегруючих, як правило, безліч БД, орієнтованих на різні предметні області. Проектування таких БД являє собою досить складне завдання, оскільки, крім проблем власне інтеграції та проектування локальних класичних, з'явилися нові проблеми, характерні саме для розподілених БД.

У відповідності до цього сформувалися нові вимоги, з'явилися нові технології їх проектування. Виникла потреба в новій концепції створення та застосування розподілених БД, яка б враховувала все це розмаїття технологій і нових вимог, з одного боку, і непристосованість для проектування застарілих інструментальних засобів, з іншого.

На даний час відсутні такі технології, незважаючи на величезний обсяг публікацій з проблем створення та застосування АРБД. Тому необхідність розробки нових методів оцінювання рівня їх захищеності, із застосуванням інтелектуальних технологій, на даний час є актуальним. Виходячи з цього робота набуває актуальності

Об'єкт дослідження: Методи та моделі побудови розподіленої адаптивної бази даних з забезпеченням комплексної інформаційної безпеки.

Предмет дослідження: Інформаційні технології та практичні аспекти застосування теорії м'яких обчислень для розробки моделей та алгоритмів побудови АРБД з забезпеченням комплексної інформаційної безпеки.

Мета дослідження: є розробка та дослідження моделей і алгоритмів побудови захищеної розподіленої адаптивної БД на основі методів м’яких обчислень.

Завдання дослідження:

– Проаналізувати сучасний стан побудови розподіленої адаптивної Бази даних.

– Розробити моделі і алгоритми побудови захищеної розподіленої адаптивної Бази даних на основі методів м’яких обчислень.

– Провести оцінку комплексної інформаційної безпеки розподіленої адаптивної Бази даних.

Методи дослідження: Системний аналіз, графо-аналітичні методи Байесовської мережі довіри, теорія експертних оцінок, інформаційно-когнітивні технології.

Практичне значення одержаних результатів: Розроблені моделі і алгоритми нових методів побудови та оцінювання рівня захищеності розподілених адаптивних Баз даних, із застосуванням інтелектуальних технологій, що дасть можливість оперативно приймати рішення з ліквідації виникнення загроз.

Наукова новизна роботи: є розробка нових адаптивних моделей і алгоритмів для побудови та оцінки ступеня захищеності розподілених адаптивних Баз даних.

Апробація результатів роботи. Положення і результати магістерської роботи можуть застосовуватись при побудові адаптивних БД в комп’ютерних мережах з розподіленим доступом.

1. ОСНОВНІ ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ТА ПРОВЕДЕННЯ ОЦІНКИ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Правові основи безпеки та оцінки безпеки інформаційної інфраструктури України.

Основні правові основи безпеки та оцінки безпеки інформаційної інфраструктури України визначені:

- Законом України про критичну інфраструктуру від 16.11.2021:

Цей Закон визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. [1]

- Законом України про національну безпеку України від 24.11.2021:

Цей Закон визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз. Також цим Законом визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони. [2];

- Рішенням Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" та Указом Президента України про цю Стратегію від 26.08.2021 Стратегія ґрунтується на положеннях Конституції України, законів України "Про національну безпеку України" та "Про основні засади забезпечення кібербезпеки України", Конвенції про захист прав людини і основоположних свобод, Конвенції про кіберзлочинність,

Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392, Концепції боротьби з тероризмом в Україні,16 затвердженої Указом Президента України від 5 березня 2019 року № 53, інших нормативно-правових актів. [3];

- Законом України Про основні засади забезпечення КБ від 15.12.2021:

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. [4];

- Законом України «Про інформацію» регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. [5]

- Законом України «Про захист інформації в інформаційно телекомунікаційних системах», де в статті 8 стверджують, що Інформація, яка є власністю держави, або інформація з обмеженим доступом, (вимога щодо захисту якої встановлена законом), повинна оброблятися із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. [6]

- «Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», що затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 п.16 та свідчать про те, що для забезпечення захисту інформації в системі створюється як комплексна система захисту інформації, яка призначається для захисту інформації від: витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і

комунікацій; несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів; спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування. [7]

- Законом України «Про захист персональних даних» регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних. [8]

- Законом України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. [9]

1.2 Загальні підходи до оцінки інформаційної захищеності об’єктів критичної інфраструктури.

В даний час існує понад 30 міжнародних стандартів типу ISO/IEC 27000, пов'язаних з інформаційною безпекою, які спільно опубліковані Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Зокрема:

- ISO 27001 – це міжнародний стандарт, розроблений Міжнародною організацією зі стандартизації, який описує, як управляти інформаційною безпекою в компанії. Остання версія цього стандарту була опублікована в 2013 році, і його повна назва на сьогодні

– ISO/IEC 27001:2013. Перша версія стандарту, опублікована в 2005 році, базувалася на Британському стандарті BS 7799-2;

- ISO/IEC 27004 містить рекомендації щодо оцінки інформаційної безпеки. Цей стандарт добре поєднується з ISO 27001, тому що пояснює, як визначити, чи досягла система управління інформаційної безпеки своїх цілей;

- ISO/IEC 27005 містить рекомендації для управління ризиками порушення інформаційної безпеки. Це дуже гарний додаток до стандарта ISO

27001, тому що містить деталі того, як здійснювати оцінку та обробку ризиків. ISO 27005 з'явився на основі британського стандарту BS 7799-3. Та Українські Нормативні документи технічного захисту інформації: - НД ТЗІ 1.1-003-99 - НД ТЗІ 2.5-004- 99 - НД ТЗІ 2.5-005-99 Ці стандарти є обов'язковими, проте їх значимість у сучасному соціумі складно переоцінити. В основі, вони відображають особливості сучасного рівня інформаційних технологій, але не містять наскрізних шкал цінності та переліків вимог безпеки систем захисту інформації, що супроводжує цим об'єктам інфраструктури. Тому будь-який процес оптимізації з позицій захисту критично важливих об'єктів, від технології розробки до етапу кінцевої реалізації та подальшої експлуатації, бажано починати з експертної оцінки (ЕО) задіяних технічних, програмних та програмно-апаратних засобів захисту інформації (ЗЗІ), що супроводжує ці об'єкти інфраструктури. Реалізація останніх починається з побудови моделі пізнання гіпотетичних інформ-об'єктів з апріорним захистом від можливих кібератак і інциндентів. Від різноманітних загроз природного та штучного походження. Виправдано вважається, що основою забезпечення безпеки інформаційної системи є три складові у вигляді конфіденційності, цілісності, доступності, а процес успішного захисту інформації в інформаційній системі залежить від рівня розвитку апаратного забезпечення, програмного забезпечення та рівня комунікації забезпечення зв'язку.

Використані процедури (механізми) захисту від потенційних загроз поділяють на фізичний рівень захисту, на рівень захисту персоналу та організаційний рівень, а саме поняття «інформаційна безпека» вводять з погляду або діяльності, спрямованої на забезпечення захищеного стану об'єкта, у цьому значенні частіше використовується термін «захист інформації», або стану як якості певного об'єкта, як об'єкт може виступати і інформація, і дані, і ресурси автоматизованої системи, і сама автоматизована система, та інформаційна система підприємства, суспільства, держави. [10].

Очевидно, що дії кібер-зловмисників (хакерів) за допомогою шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого

комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу, як правило, забезпечується за допомогою різних типів мереж, серед яких найбільш бажаною є абстрактна мережева модель для комунікацій і розробки мережевих протоколів типу OSI [11]

Очевидно, що загрози виникають у разі наявності у систем захисту вразливостей, які можуть призвести до порушення безпеки. У свою чергу характер уразливості залежить від джерела виникнення, місця прояву в життєвому циклі КВО з підсистемами захисту, ступеня прояву потенційних ризиків у процесі експлуатації об'єкта, що охороняється, та СЗІ. Тому визначенню переліку загроз та побудові моделі порушника приділяється серйозна увага на такому обов'язковому етапі як побудова оцінної моделі не тільки запланованої системи захисту, а й безпосередньо СЗІ, завдяки яким може бути спровоковано та проведено успішну атаку на безпеку всієї кіберсфери.

Маючи правову базу, можемо визначитись з основними термінами та поняттями для подальшого дослідження поставленого завдання.

Отже, якщо «інформаційна безпека» - це стан захищеності інформаційного середовища, то захист інформації - являє собою діяльність із запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, тобто процес, спрямований на досягнення цього стану. При цьому розрізняють інформаційну безпеку організації, як стан захищеності інформаційного середовища організації, що забезпечує її формування, використання та розвиток та інформаційна безпека держави, як стан збереження інформаційних ресурсів держави та захищеності законних прав особи та суспільства в інформаційній сфері.

Найчастіше поняття «інформаційної безпеки» та «кібер-безпеки» використовують як синоніми, оскільки їх родовий зв'язок визначений через поняття «безпека». Проте, ці два терміни істотно помітні незалежно від використання терміна «безпека», яке грає чи не найголовнішу роль переважають у всіх життєвих процесах: біологічних, політичних, економічних, технічних, територіальних та інших. Тому слід акцентувати на правильне використання

цього поняття та його похідних відповідно до їх призначення. Так, наприклад, у [12] озвучено, що «безпека – галузь науки, що вивчає природні, техногенні, соціальні, економічні та інші процеси освіти, розвитку та взаємодії суб'єктів, об'єктів довкілля та їх комбінацій з метою виявлення джерел небезпек, визначення їх характеристик та формування законів та інших нормативних актів, що встановлюють поняття, вимоги, рекомендації та методики, виконання яких має гарантувати захищеність інтересів окремої особи та суспільства загалом від усіх виявлених та вивчених джерел небезпеки». У такому разі за аналогією слідує, що кібербезпека - розділ безпеки, що вивчає процеси формування, функціонування та еволюції кібероб'єктів, з метою виявлення як джерел кібернебезпеки, які можуть завдати їм шкоди, так і формування законів та інших нормативних актів, що регламентують терміни, вимоги, правила, рекомендації та методики, виконання яких має гарантувати захищеність кібероб'єктів від усіх відомих та вивчених джерел кібернебезпеки. Безпосередньо поняття захищеності об'єкта вказує на його захист від зовнішніх джерел небезпеки, у той час як безпека об'єкта – це внутрішня властивість об'єкта не бути джерелом небезпеки для навколишнього середовища. З таких позицій слід розрізняти ці два терміни:

«кібербезпека об’єкта» та «кіберзахищенність об’єкта», що відповідають в англійській інтерпретації «cyber safety object» та «cyber security object». Звідси - кіберзахищеність об'єкта - властивість об'єкта, що характеризує його зовнішні можливості запобігати утворенню збитків від кібератак або обмежувати його величину допустимими нормами. Тоді «інформаційна захищеність це захист конфіденційності, цілісності та доступності інформації», а інформаційну безпеку слід розглядати як забезпечення стану захищеності:

- особи, суспільства, держави від впливу недоброякісної інформації;
- інформації та інформаційних ресурсів від неправомірного та несанкціонованого впливу сторонніх осіб;
- інформаційні права і свободи громадянина і людини [13].

Зазвичай СЗІ КВО поєднують засоби отримання, доставки, зберігання та безпосереднього захисту задіяної інформації. Остання, з погляду [14] – це

сенсове у фундаменті буття, що забезпечує достовірність і цілісність у пізнавальної, науково-практичної, виробничої, побутової та інших сферах життєдіяльності людини. Все інше, у тому числі і будь-яке її спотворення, свідоме чи ненавмисне, доцільно розглядати як повідомлення, яке може бути помилковим.

Все викладене вище дозволяє судити про багатокритеріальний характер безпеки життєдіяльності суспільства та його соціуму.

Згідно Закону України «Про основні засади забезпечення кібербезпеки України» [4] прийнято розуміти, що:

- кіберінцидент - подія або ряд несприятливих подій ненавмисного характеру, природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору, або таких, що мають ознаки можливої потенційної кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем, у тому числі зриву або блокування роботи системи, або управління її ресурсами, ставлять під загрозу безпеку електронних інформаційних ресурсів;

- кібербезпека – це захищеність життєво-важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

- кібератака - спрямовані дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій, включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання, та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються в комунікаційних або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму

функціонування комунікаційних або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

- кіберпростір – це середовище, яке надає можливості для здійснення комунікацій або реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних.

При цьому Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури, де безпосередньо підприємства, установи та організації, які віднесені до об’єктів критичної інфраструктури, безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки [4].

1.3 Основні особливості побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки.

Розподілена база даних це сукупність логічно взаємопов'язаних БД, розподілених у комп’ютерній мережі, де зв'язок забезпечує система управління, яка дозволяє управляти розподіленою БД таким чином, щоб створювати у користувачів ілюзію цілісної БД.

Система управління розподіленою БД складається з набору вузлів прийому запитів і набору вузлів збереження даних, які реалізують прозорий інтерфейс доступу до даних, та приховують фрагментацію даних між вузлами.

Можна виділити наступні основні різновиди архітектури програмно-технічних засобів розподіленої СУБД, як:

1. Архітектура однорангової мережі.

Якщо всі комп'ютери мережі є серверами та на кожному комп'ютері розміщено розподілену СУБД і БД. Дана архітектура буде архітектурою однорангової мережі.

2. Архітектура з багатьма незалежними серверами.

Якщо існують багато серверів, що мають доступ до своїх локальних БД, то у цьому випадку на комп'ютерах клієнтів буде зберігатись інформація про дані на яких серверах розташовані, що дає змогу розкласти запити для їхнього виконання на різних серверах а потім об'єднати їх результати.

3. Клієнт-серверна архітектура.

При цій архітектурі передбачено єдиний комп'ютер-сервер і багатьох комп'ютерів-клієнтів, що взаємодіють між собою через канали зв'язку. На сервері розташована СУБД та інтегрована БД. На клієнтських комп'ютерах виконуються додатки, які працюють із серверною базою даних.

4. Архітектура із взаємодіючими серверами.

У цьому випадку передбачається, що кожен сервер містить повну інформацію стосовно того, які дані та на яких серверах зберігаються розподілені запити. У разі потреби кожний сервер може звернутися до іншого для одержання необхідних даних.

5. Принципи розподілу даних.

Розподіл даних між вузлами збереження даних забезпечується на основі механізмів фрагментації та реплікації. Фрагментація здійснюється за принципами, що дозволяють наблизити дані до місць їх найбільш інтенсивного використання [25].

На сьогодні є дві причини, що змушують приділяти увагу на захист БД.

1. Кіберзлочинність. Поява нових програм-вимагачів, безфайлові способи проникнення і ризик того, що хтось зі співробітників виконає дії, що несуть загрозу конфіденційної інформації. За розвитком злочинних технологій розвиваються і рішення, що допомагають захистити таємні відомості. Важливо вживати превентивні заходи, такі як налаштування конфігурації брандмауера,

для обмеження доступу до вхідного і вихідного підозрілого трафіку, а також реалізувати рішення і процедури на випадок небажаного порушення безпеки.

2. Проблема відповідності. Відповідальність за недоторканність конфіденційних відомостей покладається на організації, які їх збирають в процесі своєї діяльності, в залежності від галузі та типу інформаційних активів [7].

Забезпеченням інформаційної безпеки [8].

Безпека даних включає методи виявлення та оцінки загроз безпеки і зниження ризиків, пов'язаних з захистом конфіденційної інформації. При цьому розуміється, що захист даних і безпека БД — це не одне і те ж.

Процес захисту даних, інформаційної бази, передбачає забезпечення безпеки. Захист систем баз даних — це сукупність методів, програмних засобів, процесів, програм та технологій, застосування яких забезпечує безпеку інформації від несанкціонованого електронного доступу, модифікацій, випадкового розкриття, порушення, знищення, копіювання т.ін.

Безпека БД в основному стосуються політики та конфіденційності. Захист БД повинен бути багаторівневим, щоб запобігати несанкціонованому доступу або копіювання. Чим більше рівнів захисту, тим більше зусиль і програмних засобів знадобиться зловмисникові для злому. Захист бази полягає в умінні розподіляти процеси, привілеї та права доступу [28].

1.3.1 Основні фактори забезпечення безпеки.

Основними факторами безпеки є конфіденційність, цілісність та доступність [29].

– Конфіденційність це недопущення несанкціонованого доступу до конфіденційної інформації.

– Цілісність це захист від неправильного видалення або зміни.

– Доступність це засоби контролю, комп'ютерні системи і програмне забезпечення, які повинні працювати таким чином, щоб забезпечити доступність послуг і інформаційних систем в разі потреби.

– Фізичний захист це набір необхідних заходів блокування кімнат, в яких знаходяться термінали та сервера.

– Криптографія це Шифрування або криптографічний захист бази даних є одним з найбільш ефективних методів забезпечення безпеки БД.

Процес захисту БД неможливий без управління паролями, що має використовувати актуальні методи дво- або багатофакторної аутентифікації, надавати користувачам обмежений час для введення облікових даних.

Адміністрування БД - передбачає виконання функцій, спрямованих на забезпечення надійного та ефективного функціонування системи БД, адекватності її змісту потребам користувачів.

Управління безпекою в СУБД – на сьогодні стали основним інструментом, що забезпечує зберігання великих масивів інформації. У зв'язку з цим увага приділяється проблемам забезпечення інформаційної безпеки, яка визначає ступінь безпеки організації та установи в цілому.

Інформаційна безпека – це захищеність інформації від випадкових і навмисних впливів природного або штучного характеру, що можуть призвести нанесенням шкоди користувачам інформації. Тому захищеність БД охоплює і обладнання, і програмне забезпечення, і персонал, і дані.

В процесі проведення аналізу слід зазначити, що захист БД передбачає запобігання будь-яких навмисних і ненавмисних загроз з використанням комп'ютерних та некомп'ютерних засобів контролю.

Наведемо основні програмно-технічні заходи, застосування яких дозволить вирішити перераховані вище проблеми [ ]:

Ідентифікація і аутентифікація - це привласнення суб'єктам доступу унікальних ідентифікаторів і порівняння таких ідентифікаторів з переліком можливих.

Аутентифікація та ідентичність - це перевірка автентичності користувача найчастіше здійснюється або через відповідні механізми операційної системи, або через певний SQL-оператор: користувач ідентифікується своїм ім'ям, а засобом аутентифікації служить пароль. Аутентифікація - механізм визначення

того, чи є користувач тим, за кого він себе видає. При всьому різноманітті існуючих механізмів аутентифікації, найбільш поширеним з них залишається парольний захист.

Управління доступом – це метод обмеження доступу до об'єктів, заснований на обліку особистості суб'єкта або груп, до якої суб'єкт входить. Група - це іменована сукупність користувачів; об'єднання суб'єктів у групи полегшує процес адміністрування даних, і будується на основі формальної структури організації. Управління доступом базується на реалізації набору дій:

- довільне керування доступом;
- забезпечення безпеки повторного використання об'єктів;
- використання міток безпеки;
- примусове управління доступом.

Підтримка цілісності – основні принципи забезпечення цілісності за редакцією Кларка і Вілсона [31]:

- Коректність транзакцій.
- Аутентифікація користувачів.
- Мінімізація привілеїв.
- Розподілення обов'язків.
- Аудит подій, що відбулися.
- Об'єктивний контроль.
- Керування передачею привілеїв.

При побудові систем захисту від загроз порушення цілісності інформації використовуються наступні криптографічні примітиви: цифрові підписи; криптографічні хеш-функції; коди перевірки автентичності.

Криптографічні хеш-функції - для обчислення необхідно знати секретний ключ. Використання ключа дозволяє гарантувати неможливість підміни об'єктів що захищаються: зловмисник, не зможе вирахувати хеш для нового файлу. У якості кодів перевірки автентичності часто використовуються модифікації симетричних криптографічних систем [28].

Висновки до першого розділу: У розділі наведені основні особливості організації та проведення оцінки захищеності об’єктів критичної інфраструктури, та розглянуті правові основи безпеки і оцінки безпеки інформаційної інфраструктури України. Визначені загальні підходи до оцінки інформаційної захищеності об’єктів критичної інфраструктури, та зазначено понад 30 міжнародних стандартів типу ISO/IEC 27000, пов'язаних з інформаційною безпекою, які спільно опубліковані Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC).

Розглянуто основні особливості побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки, та визначено розподілену базу даних як сукупність логічно взаємопов'язаних БД, розподілених у комп’ютерній мережі, де зв'язок забезпечує система управління, яка дозволяє управляти розподіленою БД таким чином, щоб створювати у користувачів ілюзію цілісної БД. Також розглянуті основні фактори безпеки як конфіденційність, цілісність та доступність, що є найбільш впливовими при функціонуванні розподіленої адаптивної БД.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ПОБУДОВИ РОЗПОДІЛЕНОЇ АДАПТИВНОЇ БД З ЗАБЕЗПЕЧЕННЯМ КОМПЛЕКСНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Огляд і аналіз задач, що підлягають розробці в роботі.

Класична система підтримки прийняття рішень (СППР) складається з підсистеми даних, яка має дві основні частини: БД та систему управління базою даних (СУБД). Технології СППР акцентуються на: обробку неструктурованих і слабо структурованих завдань потребує деякі специфічні вимоги до цих елементів комп'ютерної системи. Насамперед це необхідність виконувати значний обсяг операцій з не структурованими даними. Для цього потрібно передбачити можливість завантаження і подальшої обробки даних із зовнішніх джерел; функціонування СУБД у середовищі СППР на відміну від звичайної технології обробки інформації в системах управління. Це стосується також і БД.

АРБД формує дані на окремі частини, які сегментують збережену інформацію і переміщають окремі її блоки ближче до потрібних клієнтів, для того щоб можна було помістити таблиці на різних комп'ютерах або використовувати кілька ідентичних сховищ. У даному випадку сервери взаємодіють один з одним для підтримки синхронізації. Якщо на одному з серверів відбувається оновлення даних, воно поширюється і на всі інші сервери.

До недоліків таких розподілених баз даних можна віднести зростання складності управління ними. Але переваг, все ж більше. Головне з них це підвищення продуктивності, так як дані швидше обробляються декількома серверами, а крім того, розташовуються ближче до тих користувачів, які частіше з ними працюють.

Адаптивні властивості архітектури РБД забезпечуються за рахунок інтелектуалізації їх архітектури, основною складовою таких архітектур є постійно розвиваюча модель предметної області, підтримувана в спеціальній Базі знань (БЗ).

Таким чином, при розробці адаптивної БД доцільно розділити її функції на два типи:

a) функції, які легко алгоритмизовувати;

b) функції, які можна віднести до інтелектуальних (прийняття рішень).

Відповідно до даних функцій, адаптивну БД можна розділити на дві частини:

a) підсистема обробки, зберігання і відображення даних;

b) підсистема інтелектуальної обробки даних.

В результаті адаптивна БД має дві незалежні підсистеми, які взаємодіють один з одним.

Перевага даної адаптивної БД полягає в тому, що можна редагувати БЗ і впливати на роботу СППР в цілому, тобто змінювати критичні алгоритми або дані, які беруть участь при виборі рішення. Структура інтелектуальної частини системи є універсальною і не залежить від її наповнення. Отже, дану частину системи можна використовувати в різних адаптивних інформаційних системах без будь-яких змін.

На сьогоднішній день існують такі аспекти захисту інформації, як:

- цілісність

– захист інформації від несанкціонованої модифікації;

- конфіденційність – захист від несанкціонованого ознайомлення з інформацією;

- доступність

– захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію. Відповідно, до даних аспектів захисту інформації, виділяють наступні загрози інформації:

- загрози цілісності (знищення та модифікація інформації);

- загрози доступності (блокування та знищення інформації);

- загрози конфіденційності (несанкціонований доступ (НСД), витік та розголошення інформації).

Головним завданням БД є збереження значних обсягів інформації. Дані в БД повинні зберігатися з гарантування безпеки та конфіденційності. Інформація не повинна бути загубленою або викраденої. Загрози втрати конфіденційної інформації на сьогодні стали звичайним явищем у сучасному комп'ютерному світі. Якщо в системі захисту є недоліки, то інформації може бути завдано шкоди, наприклад, такої як:

- порушення цілісності даних;
- втрата важливої інформації;
- попадання важливих даних стороннім особам і т.д.

Кожен збій роботи БД може паралізувати роботу цілих об'єктів, що призведе до великих матеріальних втрат. Методи захисту БД в СУБД можна виділити на дві групи: основні та додаткові. До додаткових засобів захисту БД можна віднести:

- вбудовані засоби контролю даних;
- забезпечення цілісності зв'язків таблиць;
- організація спільного використання об'єктів БД в мережі.

До основних методів захисту відносять:

- захист паролем;
- шифрування;
- розділення прав доступу до об'єктів БД;
- захист полів і записів таблиць БД.

Захист паролем це самий простий спосіб захисту БД від несанкціонованого доступу. Паролі можуть бути встановленні користувачами або адміністраторами. Їх облік і зберігання виконується СУБД. Паролі зберігаються в спеціальних файлах СУБД в зашифрованому вигляді. Після введення пароля користувачу надається доступ до необхідної інформації. Не дивлячись на простоту парольного захисту, він має ряд недоліків. По-перше, пароль є вразливим, особливо якщо він не шифрується при зберіганні в СУБД.

По-друге, користувачу потрібно запам’ятати пароль, а при недбалому відношенні до запису пароль може стати надбанням інших. Більш доцільним методом захисту є шифрування. Шифрування представляє процес обробки інформації за певним алгоритмом в вигляді непридатного для читання, в цілях захисту від несанкціонованого перегляду або використання. Важливою особливістю будь-якого алгоритму шифрування є використання ключа, який стверджує вибір якогось конкретного методу кодування із всіх можливих. Розрізняють два основні методи шифрування: симетричне й асиметричне. В симетричному шифрування один і той же ключ використовується і для шифрування, і для дешифрування. В асиметричних методах застосовуються два ключі. Один з них, несекретний, використовується для шифрування і може публікуватися разом з адресою користувача, другий, секретний, застосовується для дешифрування і відомий тільки одержувачу. Шифрування забезпечує всі три аспекти безпеки даних: конфіденційність, цілісність і доступність. В цілях контролю використання основних ресурсів СУБД в багатьох СППР є засоби розділення прав доступу до об’єктів БД. Адміністратори БД мають всі права, решта користувачів мають ті права і рівні доступу до об’єктів, якими їх наділили. Дозвіл на доступ до конкретних об’єктів БД зберігається в файлі робочої групи. Файл робочої групи містить дані про користувачів групи і зчитується під час запуску, та зберігає наступну інформацію:

- імена облікових записів користувачів;- паролі користувачів;

- імена груп, в які входять користувачі.

Всі вище описані методи є основними, але не гарантують повного зберігання даних. Для підвищення рівня безпеки інформації в БД рекомендується використання комплексних заходів.

Процедури ідентифікації, аутентифікації і авторизації в СУБД.

Для будь-якої захищеної БД обов’язковими є процедури ідентифікації, аутентифікації та авторизації. Сутність процедури ідентифікації полягає в призначенні користувачу БД – імені користувача яким є унікальна мітка, що відповідає прийнятим угодам і забезпечує однозначну ідентифікацію об’єктів у

реальному часі, що відображаються. Сутність процедури аутентифікації полягає в підтвердженні автентичності користувача, що представив ідентифікатор. На сьогодні у ряді сучасних СУБД використовується:

- біометрична аутентифікація – процес доведення і перевірки автентичності заявленого користувачем імені через пред'явлення ним своїх біометричних характеристик (відбитки пальців, звуки голосу, обличчя, особливості роботи на клавіатурі, електронний цифровий підпис);

- парольна аутентифікація – процес доведення і перевірки автентичності заявленого користувачем імені шляхом введення ним пароля або парольної фрази. Заходами, що дають змогу підвищити надійність парольного захисту є: накладання технічних обмежень, управління терміном дії паролів, обмеження доступу до файлу паролів, обмеження кількості невдалих спроб входу в систему, використання програмних генераторів паролів;

- аутентифікація із застосуванням токенів. Токен – це предмет або пристрій, володіння яким підтверджує автентичність користувача.

Ефективність процедур ідентифікації та аутентифікації істотним чином впливає на ефективність функціонування системи безпеки в цілому. В процесі авторизації встановлюється набір можливих операцій з даними, які може здійснювати користувач.

2.2 Аналіз структурної організації АРБД в складі СППР з забезпеченням комплексної інформаційної безпеки.

На тепершній час можна виділити найбільш застосовні типи архітектур зберігання даних:

1. Функціональна архітектура БД.
2. Незалежні вітрини даних.
3. Дворівневе сховище даних.
4. Трирівневе сховище даних.

Функціональна архітектура БД - (рис. 2.1) є найбільш простою архітектурною структурою БД. Ці системи часто зустрічаються особливо в

організаціях з невисоким рівнем аналітичної культури і недостатньо розвиненою інформаційною інфраструктурою.

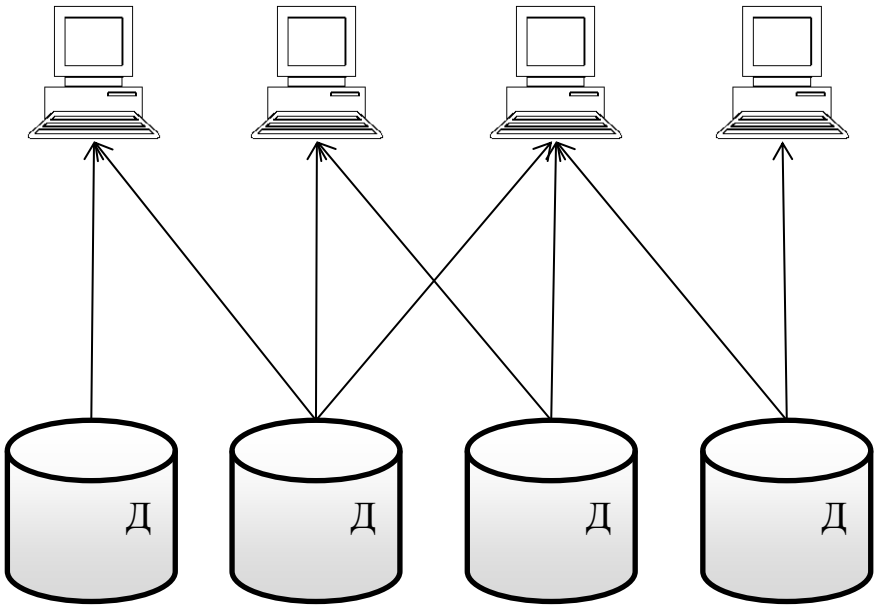


Рисунок 2.1 - Функціональна архітектура БД

У даній архітектурі є те, що аналіз здійснюється з використанням даних з оперативних систем.

При цьому дана архітектура має деякі переваги:

1. Швидке впровадження за рахунок відсутності етапу перевантаження даних у спеціалізовану систему;

2. Мінімальні витрати за рахунок використання однієї платформи.

Разом з тим має деякі недоліки:

1. Єдине джерело даних, потенційно звужуюче коло питань, на які може відповісти система;

2. Оперативні системи характеризуються дуже низькою якістю даних з точки зору їх ролі в підтримці прийняття стратегічних рішень. У силу відсутності етапу очищення даних, дані функціональної архітектури БД, як правило, володіють невисокою якістю;

3. Велике навантаження на оперативну систему. Складні запити можуть призвести до зупинки роботи оперативної системи, що дуже небажано.

Архітектура Незалежні вітрини даних - (Рис. 2.2) часто зустрічаються у великих організаціях з великою кількістю незалежних підрозділів, та мають свої власні відділи інформаційних технологій.

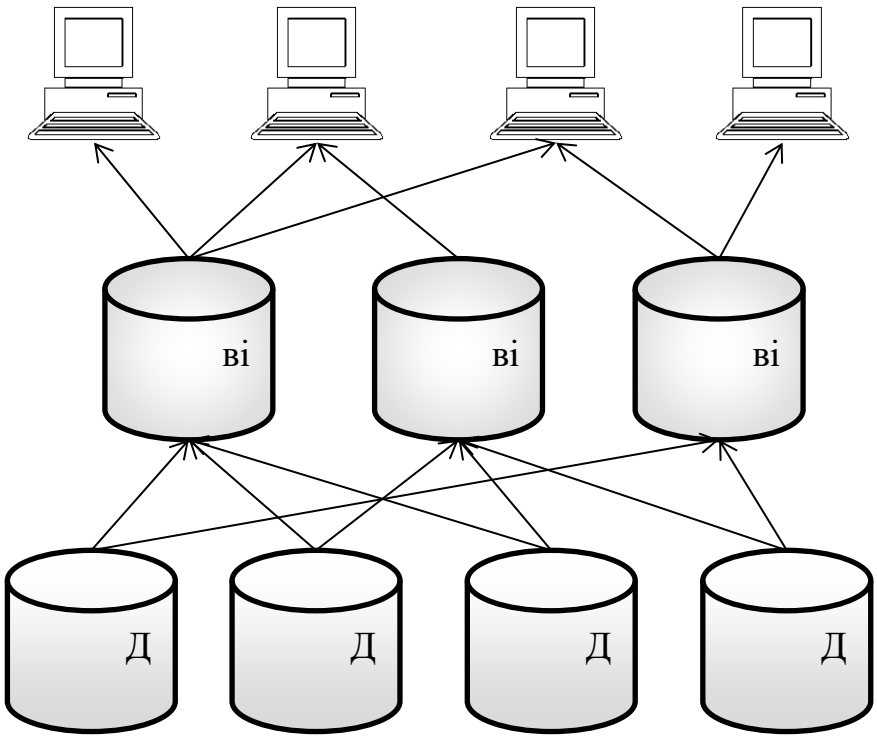


Рис. 2.2 - Незалежні вітрини даних

До переваг даної архітектури можна віднести:

1. Вітрини даних можна впроваджувати досить швидко;

2. Вітрини проектуються для відповідей на конкретний ряд питань;

3. Дані у вітрині оптимізовані для використання певними групами користувачів, що полегшує процедури їх наповнення, а також сприяє підвищенню продуктивності.

До недоліків відноситься:

1. Дані зберігаються багаторазово в різних вітринах даних, що призводить до дублювання даних і, як наслідок, до збільшення витрат на зберігання і потенційним проблемам, пов'язаним з необхідністю підтримки несуперечності даних;

2. Потенційно дуже складний процес наповнення вітрин даних при великій кількості джерел даних;

3. Дані не консолідуються на рівні підприємства, таким чином, відсутня єдина картина бізнесу.

Архітектура дворівневого сховища даних - (Рис. 2.3) будується централізовано для надання інформації в рамках компанії. Для підтримки даної архітектури необхідна команда професіоналів в області БД, яка повинна узгодити всі визначення і процеси перетворення даних.

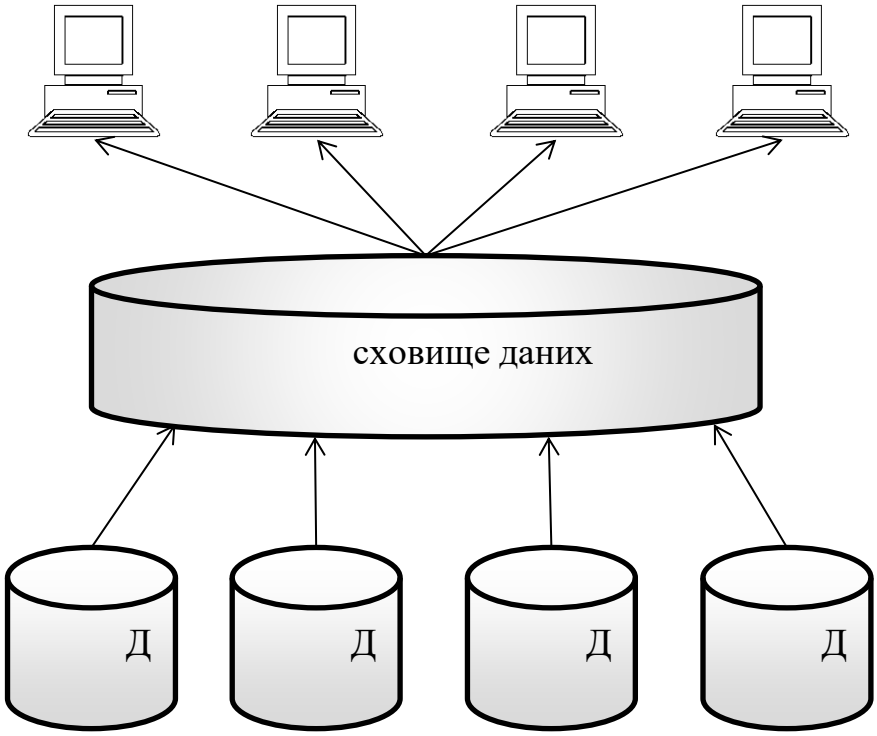


Рис. 2.3 - Дворівневе сховище даних.

Дана архітектура має переваги:

1. Дані зберігаються в єдиному екземплярі;

2. Мінімальні витрати на зберігання даних;

3. Відсутні проблеми, пов'язані з синхронізацією декількох копій даних;

4. Дані консолідуються на рівні підприємства, що дозволяє мати єдину картину бізнесу.

До недоліків слід віднести:

1. Дані не структуруються для підтримки потреб окремих користувачів або груп користувачів;

2. Можливі проблеми з продуктивністю системи;

3. Можливі труднощі з розмежуванням прав користувачів на доступ до даних.

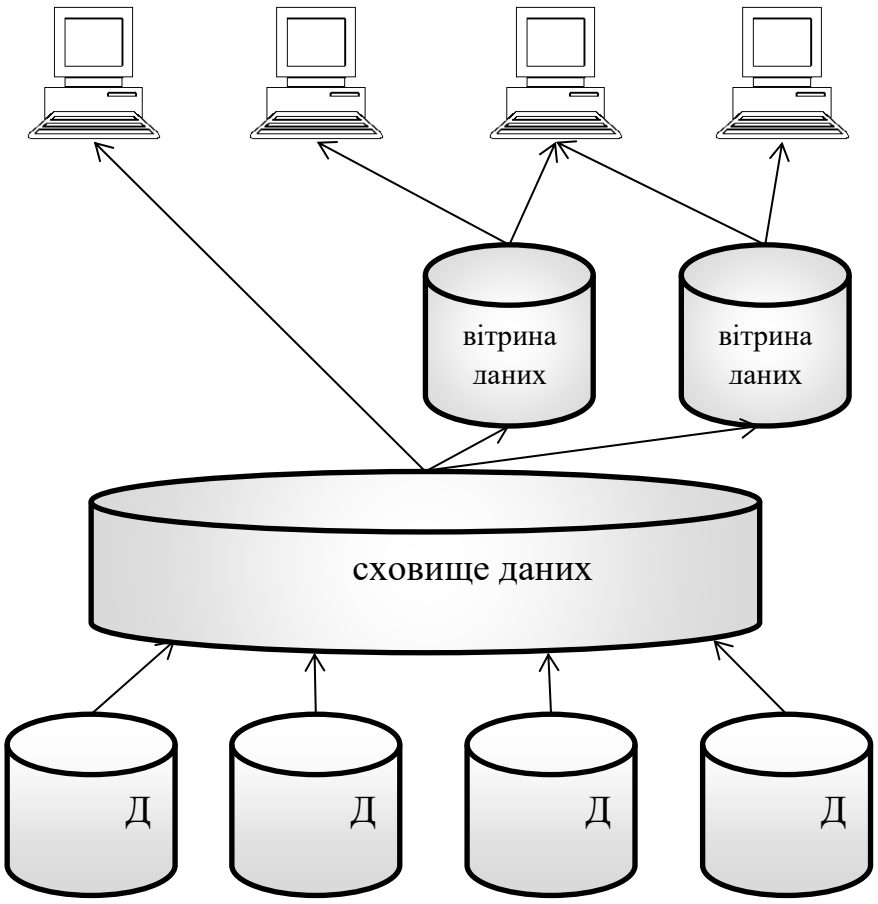


Рис. 2.4 - Трирівневе сховище даних

Архітектура трирівневого сховища даних - являє собою єдине централізоване джерело корпоративної інформації. Вітрини даних представляють підмножини даних зі сховища, організовані для вирішення завдань окремих підрозділів компанії.

Дана архітектура має переваги:

1. Створення і наповнення вітрин даних спрощено, оскільки наповнення відбувається з єдиного стандартизованого надійного джерела очищених нормалізованих даних;

2. Вітрини даних синхронізовані і сумісні з корпоративним поданням. Існує корпоративна модель даних та можливість порівняно легкого розширення сховища і додавання нових вітрин даних;

3. Гарантована продуктивність.

До недоліків слід віднести:

1. Існує надмірність даних, ведуча до зростання вимог на зберігання даних;

2. Потрібна узгодженість з прийнятою архітектурою багатьох областей з потенційно різними вимогами (наприклад, швидкість впровадження іноді конкурує з вимогами слідувати архітектурному підходу).

2.3. Основні вимоги та постановка задачі побудови захищеної розподіленої адаптивної БД.

Виходячи з проведеного аналізу можна зробити висновки, що адаптивні розподілені бази даних з'явилися як наслідок розвитку розподілених систем різного призначення і, в першу чергу, інформаційно-пошукових систем (ІПС), інтегруючих, як правило, безліч баз даних, орієнтованих на різні предметні області. Проектування таких АРБД являє собою досить складне завдання, оскільки, крім проблем власне інтеграції та проектування локальних класичних БД, з'явилися нові проблеми, характерні саме для розподілених БД. Це проблеми:

- Оптимізації розміщення розподілених АБД по вузлах мережевої структури системи, що не дозволені в даний час сучасними CASE - системами (Computer Aided System Engineering);

- Мережевий масштабованості БД для географічно розподілених систем;

- Проектування та реалізації (використання) комунікаційного середовища системи пам'яті, як основи для занурення розподіленої БД;

- Оптимізації розміщення даних в розподілених БД для забезпечення балансу завантаження;

- Синхронізації доступу до даних і паралельної обробки запитів для забезпечення необхідної продуктивності системи;

- Підтримання копій даних в декількох вузлах мережі для скорочення пересилань при виконанні розподілених запитів;

- Фрагментації об'єктів БД і розширення простору пошуку варіантів виконання запитів;

- Управління транзакціями (наприклад, коректне завершення розподілених транзакцій), багаторівневого захисту даних в БД і реалізації можливості отримання різноманітної за структурою і змістом інформації від різних типів джерел.

Відповідно до цього сформувалися нові вимоги до розподілених БД, з'явилися нові технології їх проектування. Виникла потреба в новій концепції створення та застосування розподілених БД, яка б враховувала все це розмаїття технологій і нових вимог, з одного боку, і непристосованість для проектування БД застарілих інструментальних засобів, з іншого.

Концепції такого типу в даний час відсутні, незважаючи на величезний обсяг публікацій з проблем створення та застосування розподілених БД.

Постільки адаптивна розподілена БД розрахована на будь-якого, в тому числі на непрофесійного користувача, зростають вимоги до адаптації для різних користувачів.

Розроблювана АДБ повинна базуватися на передових технологіях, легко управлятися та конфігуруватися, мати високий рівень написаного програмного коду, бути надійно захищеною від різних атак зловмисників для викрадення або підміни даних.

Вимоги до адаптивної БД:

– застосування найбільш типових і перспективних архітектур БД і програмних засобів;

– застосування методів логічного висновку, нейронних мереж, нейрокомп'ютерів та ін;

– застосування єдиного інтерфейсу експертів для роботи з різними компонентами даних і додатків;

– постійна актуалізація зрозумілої моделі для урахування нових понять, що виникають при зміні прикладних задач;

– динамічне адміністрування розподіленої АБД при зміні частоти використання, модифікації структури і зміні розміщення даних та ін.;

– рішення повинні бути записані в загальному вигляді;

– поповнення БД проводиться тільки експертом, який має права доступу;

– мати можливість поповнення даними з WEB;

– надавати доступ для моніторингу системи;

– експертам має надаватися повний доступ для управління даними (додавати, змінювати або видаляти);

– вміти відсортувати і вибрати кращі рішення з БД;

– Процес адаптації повинен проводитися для будь-яких рішень;

– Адаптація виконується на основі вхідних даних про ОПР;

– Мати захист допуску до БД;

– Встановлювати захищений канал зв'язку при передачі даних по зовнішніх лінях зв'язку.

А також БД повинна бути розподілена на основі фрагментованої структури. Оскільки перетинання різної інформації в одній БЗ призводить до переповнення і великому навантаженні на СУБД. Внаслідок цього використання фрагментованої структури БД зменшує навантаження на СУБД. Дані розподіляються на окремих БД своєї сфери використання.

Виходячи з вимог, можна сформулювати задачі до системи комплексної інформаційної безпеки АРБД, яка повинна виконувати наступні методи захищеності:

- Перевіряти на цілісність даних;
- Перевіряти на доступність даних;
- Перевіряти на конфіденційність даних;
- Оцінювати узгодженість даних;
- Перевіряти посилальну цілісність даних;
- Перевіряти на зовнішній вплив;
- Перевіряти відмови апаратного забезпечення;
- Перевіряти відмови програмного забезпечення;
- Перевіряти дії співробітників;
- Перевіряти дії адміністраторів;
- Аналізувати дані на захищеність;
- Перевіряти призначення прав доступу.
- Комплексна ІБ повинна сканувати всі елементи системи;
- Комплексна ІБ додатково повинна проводити такі методи захищеності:
- Аналізувати систему на віруси;
- Виконувати попередню підстановку даних в запит і перевіряти на SQL-ін'єкції;
- Моніторити апаратні збої;
- Моніторити доступність даних і ресурсів;
- Моніторити некоректні дії користувачів;
- Перевіряти дані на цілісність (використовуючи хеш);
- Перевіряти інформацію на присутність підміни даних.

Висновки до другого розділу: У розділі проведений аналіз сучасних підходів до побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки. По результатам аналізу зазначено, що переваги адаптивної БД полягають в тому, що можна редагувати БЗ і впливати на роботу

СППР в цілому, тобто змінювати критичні алгоритми або дані, які беруть участь при виборі рішення. А також, що структура інтелектуальної частини системи є універсальною і не залежить від її наповнення. Отже, дану частину системи можна використовувати в різних адаптивних інформаційних системах без будь-яких змін.

У розділі також проведений аналіз структурної організації АРБД в складі СППР з забезпеченням комплексної інформаційної безпеки, де виділено найбільш застосовні типи архітектур зберігання даних такі як функціональна архітектура БД, незалежні вітрини даних, дворівневе сховище даних, трирівневе сховище даних та інш.

Виходячи з проведеного аналізу зазначені висновки, що адаптивні розподілені БД з'явилися як наслідок розвитку розподілених систем різного призначення і, в першу чергу, інформаційно-пошукових систем (ІПС), інтегруючих, як правило, безліч БД, орієнтованих на різні предметні області. Проектування таких АРБД являє собою досить складне завдання, оскільки, крім проблем власне інтеграції та проектування локальних класичних БД, з'явилися нові проблеми, характерні саме для розподілених БД.

Також зазначено, що БД повинна бути розподілена на основі фрагментованої структури. Оскільки перетинання різної інформації в одній БЗ призводить до переповнення і великому навантаженні на СУБД. В наслідок цього використання фрагментованої структури БД зменшує навантаження на СУБД, де дані розподіляються на окремих БД своєї сфери використання.

Виходячи з цих вимог, сформульовані задачі до системи комплексної інформаційної безпеки АРБД, яка повинна використовувати відповідні методи захищеності.

РОЗДІЛ 3. РОЗРОБКА МОДЕЛЕЙ І АЛГОРИТМІВ ПОБУДОВИ КОМПЛЕКСНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РОЗПОДІЛЕНОЇ АДАПТИВНОЇ БД

3.1. Розробка інформаційної моделі комплексної ІБ АРБД в складі СППР.

Система підтримки прийняття рішень, без елементів захисту інформації, що зберігається в БД, а також всіх інформаційних потоків є не актуальною в наш час. При нинішніх технологіях розробки обчислювальних систем стає все серйозніше питання про Комплексний Інформаційний Захист, так як виконати злом ключів захисту або шифрування даних є не суттєвою проблемою. Для злому або підбору ключа необхідно відносно невеликий час в порівнянні з використанням обчислювальних машин минулого десятиліття.

Для поліпшення інформаційної Безпеки (ІБ) розробляються різні інтелектуальні системи захисту інформації. Такі системи включають в себе використання різних моделей і методів таких як: біометричні сканери або аналіз і запам'ятовування послідовності дій користувача, що зрештою згенерує спеціальні засоби захисту інформації.

У розробці інформаційної безпеки АРБД в складі СППР, а також складний організаційно-технічний об’єкт (СОТО) розроблено спеціальний засіб, заснований на використанні методів оцінки та запобігання різних родів атак, як з боку користувачів, так і з боку адміністраторів або зловмисників. Також враховуються фактори впливу на системи такі як: відмова апаратного забезпечення або облік доступності даних.

На рисунку 3.1 показано основну інформаційну модель вбудованої інформаційної безпеки. Аналізуючи розроблену структуру, слід зазначити, що модулі оцінки різних видів загроз зв'язуються з усією системою, включаючи СОТО і АРСППР. Комплексна ІБ має в собі вбудовані засоби підвищення рівня ІБ, а також засоби оцінки інформаційної безпеки по кожному з видів методів захисту.

У групі СОТО зібрані всі модулі і блоки, які розроблені на підприємстві і виконують всі технологічні процеси по об’єкту. В інформаційній моделі групу СОТО представлено як абстрактна група умовних технологічних вузлів.

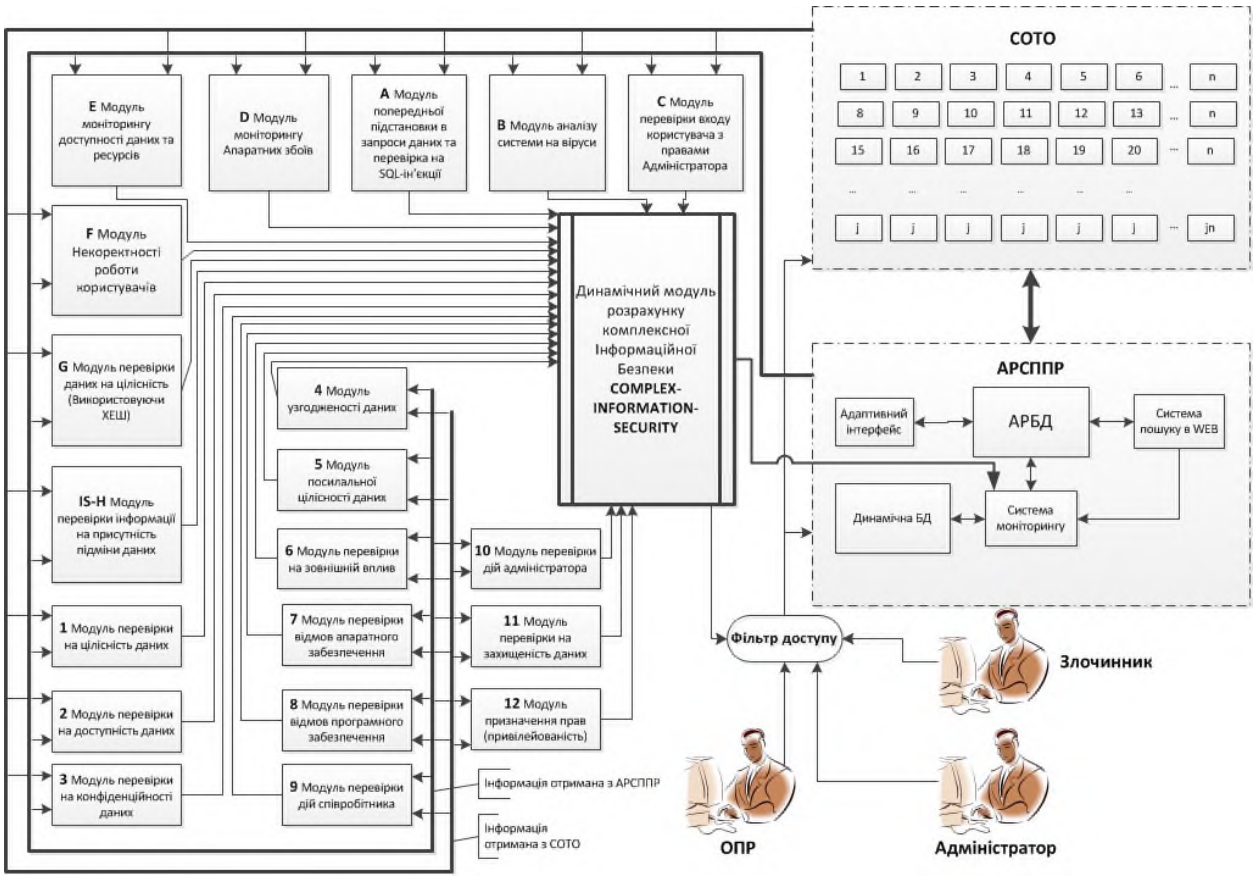


Рисунок 3.1 – Інформаційна модель комплексної ІБ АРБД в складі СППР.

В групі АРСППР представлено основні компоненти СППР. До їхнього складу входять:

- Адаптивний Інтерфейс – інтерфейс користувача (ОПР);
- Адаптивно-Розподілена База Даних – БД, яка призначена для зберігання рішень, знань та автоматичного поповнення;
- Система пошуку в WEB – пошуковий модуль, завдяки якому відбувається пошук і автоматична фільтрація рішень і знань, яких немає в Адаптивно-Розподіленій БД;
- Динамічна БД – спеціальна БД, в якій тимчасово зберігаються рішення.

Система має два основних інформаційних потоки в спеціальні вузли оцінки ІБ:

1. Інформаційний потік від групи об'єктів СОТО;

2. Інформаційний потік від групи модулів АРСППР.

Вся зібрана інформація аналізується спеціальними модулями різного призначення:

- Модуль моніторингу входу користувача з правами Адміністратора;
- Модуль аналізу системи на віруси;
- Модуль попередньої підстановки даних, та перевірка на SQL-ін'єкції;
- Модуль моніторингу апаратних збоїв;
- Модуль моніторингу доступності даних та ресурсів;
- Модуль некоректності роботи користувачів;
- Модуль перевірки даних на цілісність (використовуючи хеш);
- Модуль перевірки інформації на присутність підміни даних.

Також до складу комплексної ІБ входять засоби оцінки та підвищення захисту АРБД. Це такі вузли, як:

- Модуль перевірки на цілісність даних;
- Модуль перевірки на доступність даних;
- Модуль перевірки на конфіденційність даних;
- Модуль узгодженості даних;
- Модуль посилальної цілісності даних;
- Модуль перевірки на зовнішній вплив;
- Модуль перевірки відмов апаратного забезпечення;
- Модуль перевірки відмов програмного забезпечення;
- Модуль перевірки дій співробітників;
- Модуль перевірки дій адміністраторів;
- Модуль перевірки на захищеність даних;
- Модуль призначення прав (привілейованість).
- Модуль моніторингу входу користувача з правами Адміністратора – виконує аналіз стану привілейованості користувача (клієнта Ці права дозволяють реалізувати повний контроль над можливостями клієнтів.

3.2 Розробка інформаційно логічної моделі розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки.

АРБД містить у собі набори модулів, субмодулів та інших ділянок програмних рішень різних завдань. Для проведення допомоги ОПР під час критичних станів системи, СППР має інтегрований засіб АРБД.

АРБД не тільки зберігає в БД інформацію у вигляді альтернатив, вона проводить облік прямих і непрямих даних, які будь-яким чином впливають на процес роботи СППР та прийняття релевантного рішення. Повна структура інформаційної моделі показано на рисунку 3.2.

Для коректної роботи в АРБД зберігається наступна інформація:

- інформація про стан технологічного процесу на об’єкті;
- інформація про психологічні та когнітивні характеристики ОПР (результати тестування методами Люшера і т. п.)
- інформація про характеристики зовнішнього навколишнього виробничого середовища, яка безпосередньо впливає на ОПР (рівень шуму, температура, низькочастотні вібрації, рівень освітленості і т.д.).

Перед відправкою запиту на пошук рішень, всю необхідну інформацію систематизує Адаптивний інтерфейс ОПР і відправляє їх разом із запитом. Дані приймаються і спеціальним методом расконкатиновуються. Метод расконкатенації представлений на рисунку 3.3.

Вхідний потік даних позначений як змінна «R» проходить три етапи (етап 1, етап 2 і етап 3). Перший етап представляє собою функцію (F1) відділення від основного потоку множини «Z», яка несе в собі інформацію про характеристики зовнішнього навколишнього середовища впливу на ОПР. Ця функція обробляє потік R на змінний потік R1 і масив значень Z. Функція (F1) формулюється як:

$$Z = R / R1 \tag{3.1}$$

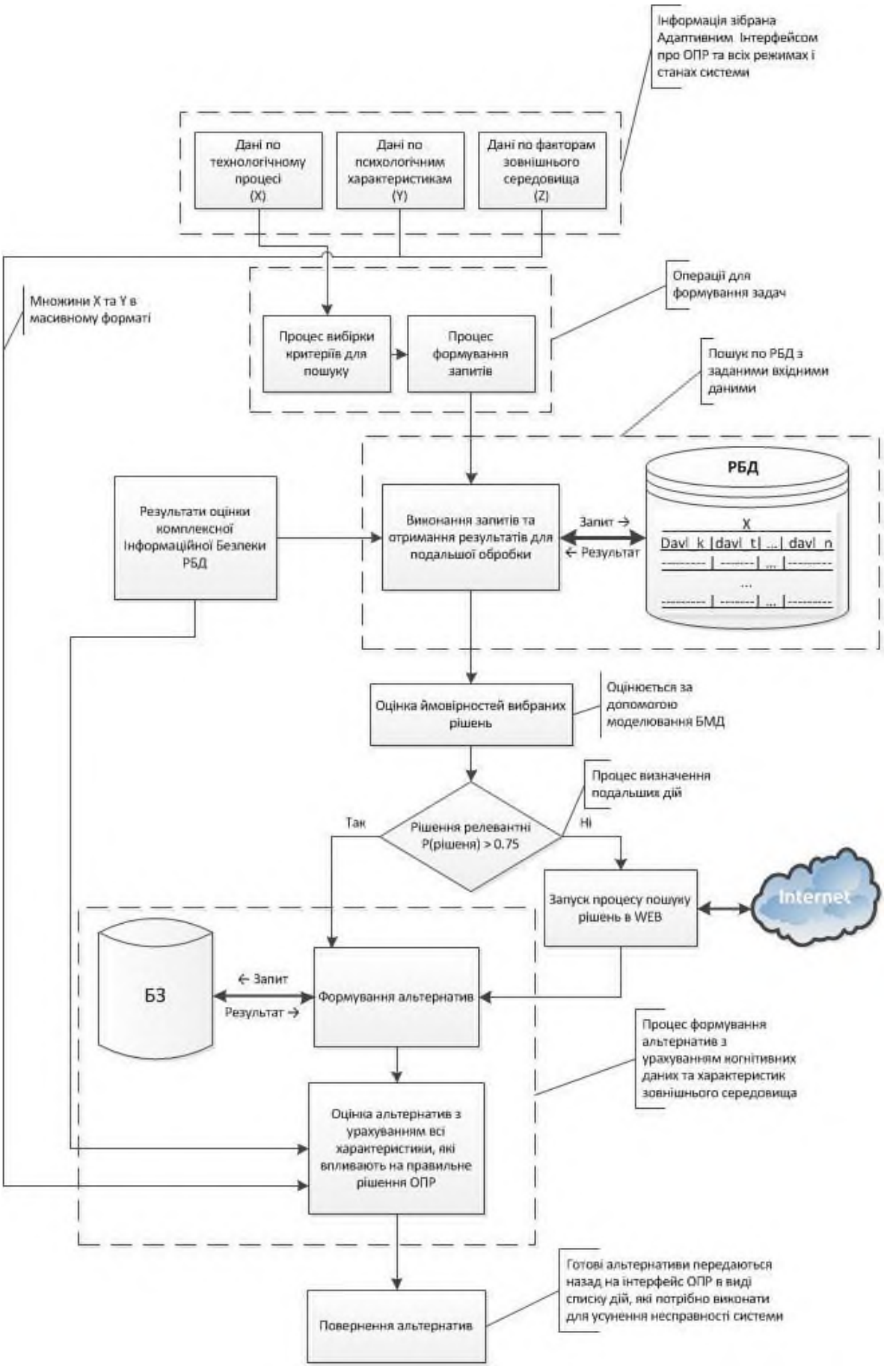


Рисунок 3.2 – Інформаційно логічна модель АРБД з забезпеченням КІБ.

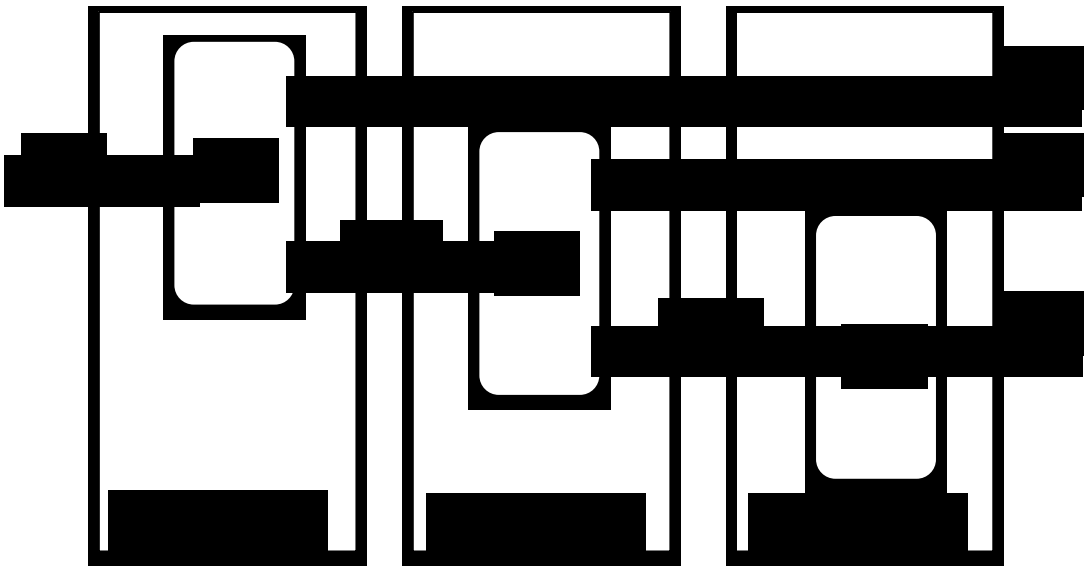


Рисунок 3.3 – Метод расконкатенації вхідного потоку даних в АРБД.

Другий етап являє собою функцію (F2) відділення від змінного потоку R1 множини «Y», в якій збережено інформацію про психологічні характеристики ОПР. Ця функція обробляє потік R1 на змінний потік R2 і масив значень Y. Функція (F2) формулюється як:

$$Y = R1 / R2 \tag{3.2}$$

Третій і останній етап даного методу представлений функцією (F3) перетворення змінного потоку R2 в множини «X», в якій збережено інформацію про технологічний процес. Ця функція обробляє потік R2 в масив значень X. Функція (F3) формулюється як:

$$X = R2 \tag{3.3}$$

Представлення даних, які передаються вузлами X, Y і Z:

X - інформація про технологічний стан системи має наступний синтаксис: Ім'я_змінної: значення: стан.

3.3 Розробка математичної моделі оцінки стану комплексної інформаційної безпеки СППР з розподіленою адаптивною БД.

В даній роботі розглядається вирішення вказаних вище проблемних питань з використанням математичного апарата Байесовської мережі довіри (БМД).

Баєсові мережі - це графові моделі імовірнісних і причинно-наслідкових зв'язків між змінними в статистичному інформаційному моделюванні. У Баєсових мережах, можуть органічно поєднуватися емпіричні частоти, появи різних значень змінних, суб'єктивні оцінки «очікувань» і теоретичні уявлення про математичні ймовірності тих чи інших наслідків з апріорної інформації. Це являється важливою практичною перевагою і відрізняє Баєсові мережі від інших методик інформаційного моделювання. [8]

У математичній частині взаємозв'язку ймовірностей різних типів інформація представляється у формі графа. Повноцінна модель графа оцінки комплексної інформаційної та кібернетичної безпеки адаптивної розподіленої БД показана на рисунку 3.4.

БМД являють собою графічні моделі подій і процесів на основі об'єднання деяких виводів теорії ймовірностей і теорії графів [8], основу яких становлять пари $<G,B>$, де перший компонент G – це спрямований ациклічний граф, що відповідає випадковим змінним, а друга B – безліч параметрів, що визначають систему.

Повна загальна ймовірність БМД обчислюється по формулі:

$$P_B(X^{(1)},...,X^{(N)}) = \prod_{i=1}^{N} P_B(X^{(i)} \mid P_A(X^{(i)})), \qquad (3.4)$$

де: A – безліч станів середовища; $N = (x_1,...,x_N)$ – вектор параметрів їх розподілів.

Умовна ймовірність події визначається співвідношенням:

$$p(E|H_k) = \frac{p(E \cap H_k)}{p(H_k)}, \tag{3.5}$$

де: E й H_k – зв'язані між собою змінні. Ця залежність дозволяє визначити, яка буде ймовірність події E, якщо має місце конкретна подія H_k.

Взаємовиключні події формують вичерпну безліч, якщо

$$\bigcup_{i=1}^{n} E_i = \Omega. \tag{3.6}$$

Дві змінні не перетинаються, якщо вони не мають однакових значень. Теорія побудови мереж Байеса ґрунтується на припущенні, що події є вичерпними і не перетинаються. У цьому випадку ймовірність події E можна обчислити за допомогою умовних імовірностей:

$$p(E) = \sum_{i=1}^{n} p(E \cap H_i) = \sum_{i=1}^{n} p(E \mid H_i) \cdot p(H_i). \tag{3.7}$$

Використовуючи формулу (3.5), імовірність перетинання подій E і H можна виразити в такий спосіб:

$$p(E \cap H_k) = p(E \mid H_k) \cdot p(H_k) = p(H_k \mid E) \cdot p(E),$$

звідки одержуємо:

$$p(H_k \mid E) = \frac{p(E \mid H_k) \cdot p(H_k)}{p(E)}. \tag{3.8}$$

З урахуванням формули (3.6) і (3.8) можна представити так:

$$p(H_k \mid E) = \frac{p(E \mid H_k) \cdot p(H_k)}{\sum_{i=1}^{n} p(E \mid H_i) \cdot p(H_i)}. \quad (3.9)$$

Аналізуючи послідовність надходження і обробки інформації, по мережі Байєса, надалі описується поетапна побудова мережі в порядку як проходить інформація в системі.

Вузол з ідентифікатором 12 - це вузол розрахунку ймовірності призначення прав доступу (привілейовані). Призначення прав (привілейованість) - процес визначення прав (дозволу) доступу до РБД або СУБД. Привілейованість побудовано за ієрархічною структурою. Призначення прав в СУБД має дуже гнучкий сценарій, що дозволяє максимально покращити безпеку БД.

Вузол з ідентифікатором 9 - це ймовірність впливу дій співробітників, що працюють в СППР. Ненавмисні дії співробітника - це дії, в результаті яких відбувається поломка технічних засобів або зміна параметрів, алгоритмів функціонування системи. Умисні дії співробітника - це дії спрямовані на отримання несанкціонованого доступу до інформації або порушення режиму роботи системи, які стають можливі при недостатній реалізації системи організаційного контролю за діями персоналу.

Для обліку працездатності апаратного забезпечення системи в граф доданий вузол з ідентифікатором 7. Цей вузол описує ймовірність впливу на нормовану роботу системи з урахуванням виходу з ладу апаратного забезпечення. Відмови апаратного забезпечення - це збої обладнання, фізичні впливи на систему або електричний вплив на цілісність обладнання.

Система, маючи різні ступені захищеності від зовнішнього впливу, не гарантує повний захист даних або працездатність всієї системи. Тому враховувати зовнішній вплив необхідно в будь-якому випадку. Для цього призначений вузол з ідентифікатором № 6. Даний вузол надає ймовірність стану системи, оцінюючи ступінь зовнішнього впливу. Вузол № 6 впливає на вузли, що

надають Технологічний процес (X), Психологічні характеристики ОПР (Y) і Фактори зовнішнього впливу на ОПР (Z).

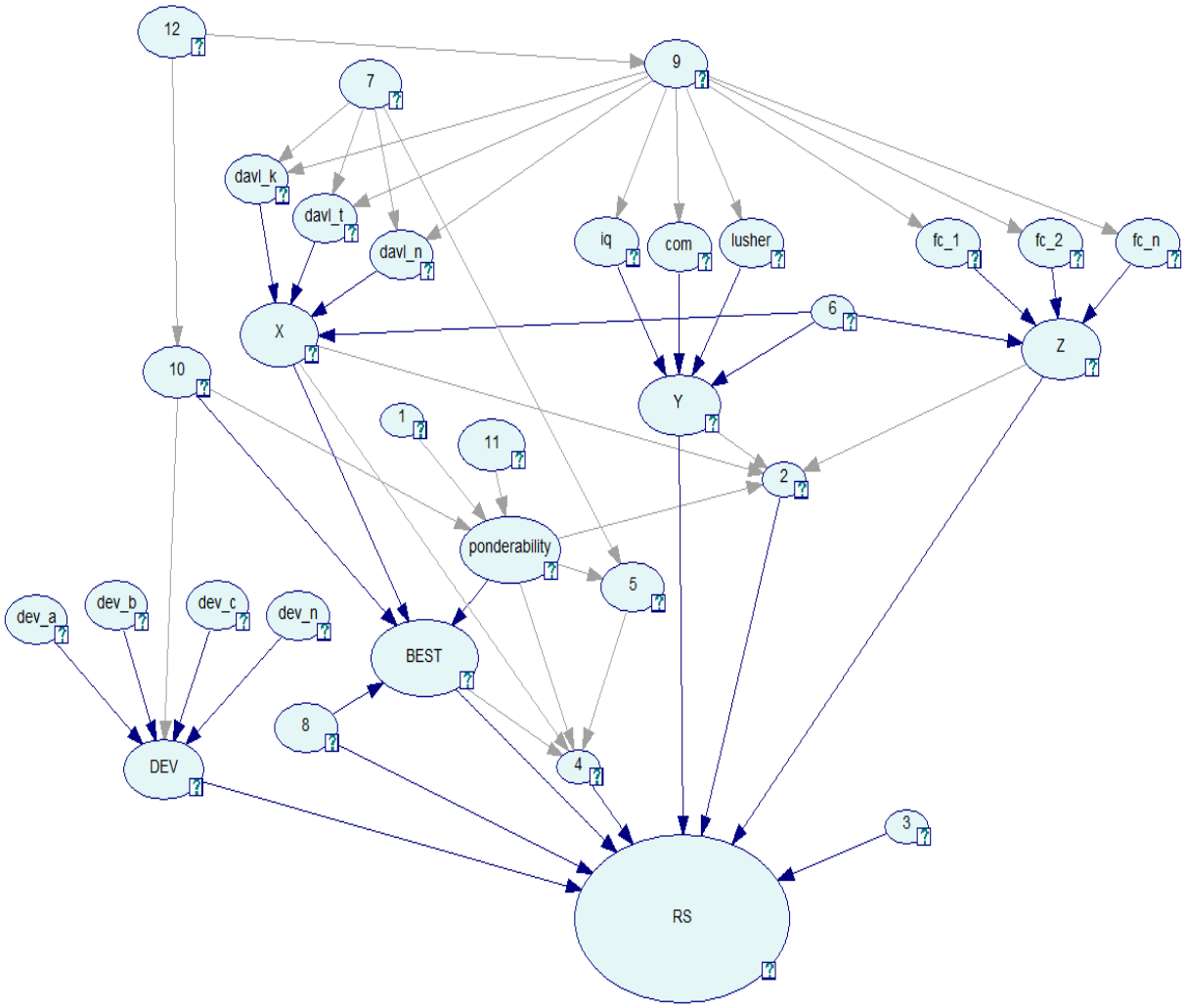


Рисунок 3.4 - Повна модель графа БМД системи.

3.3.1 Розробка математичної моделі оцінки стану комплексної інформаційної безпеки розподіленої адаптивної БД.

Визначення життєздатності побудованої моделі визначається використанням методу експертних оцінок та побудови і дослідження Байєсівської мережі довіри. Стан комплексної інформаційної безпеки розподіленої адаптивної БД визначається наступними факторами безпеки:

A - модуль попередньої підстановки в запити даних; **B** - модуль перевірки системи на віруси; **C** - модуль перевірки входу користувача з правами адміністратора; **D** - модуль моніторингу апаратних збоїв; **E** - модуль моніторингу

доступності даних і ресурсів; **F** - модуль некоректності роботи користувачів; **G** - модуль перевірки даних на цілісність (використовуючи хеш);

H - модуль моніторингу оцінки функціональної стабільності користувачів;

K1- цілісність даних; **K2** - доступність даних; **K3** - конфіденційність даних;

K4 - узгодженість даних; **K5** - посилальна цінність; **K6** - зовнішній вплив;

K7 - відмови апаратного забезпечення; **K8** - відмови програмного забезпечення;

K9 - вплив дій користувачів; **K10** - вплив дій адміністраторів; **K11**- захищеність даних; **K12** - енергетичні відмови

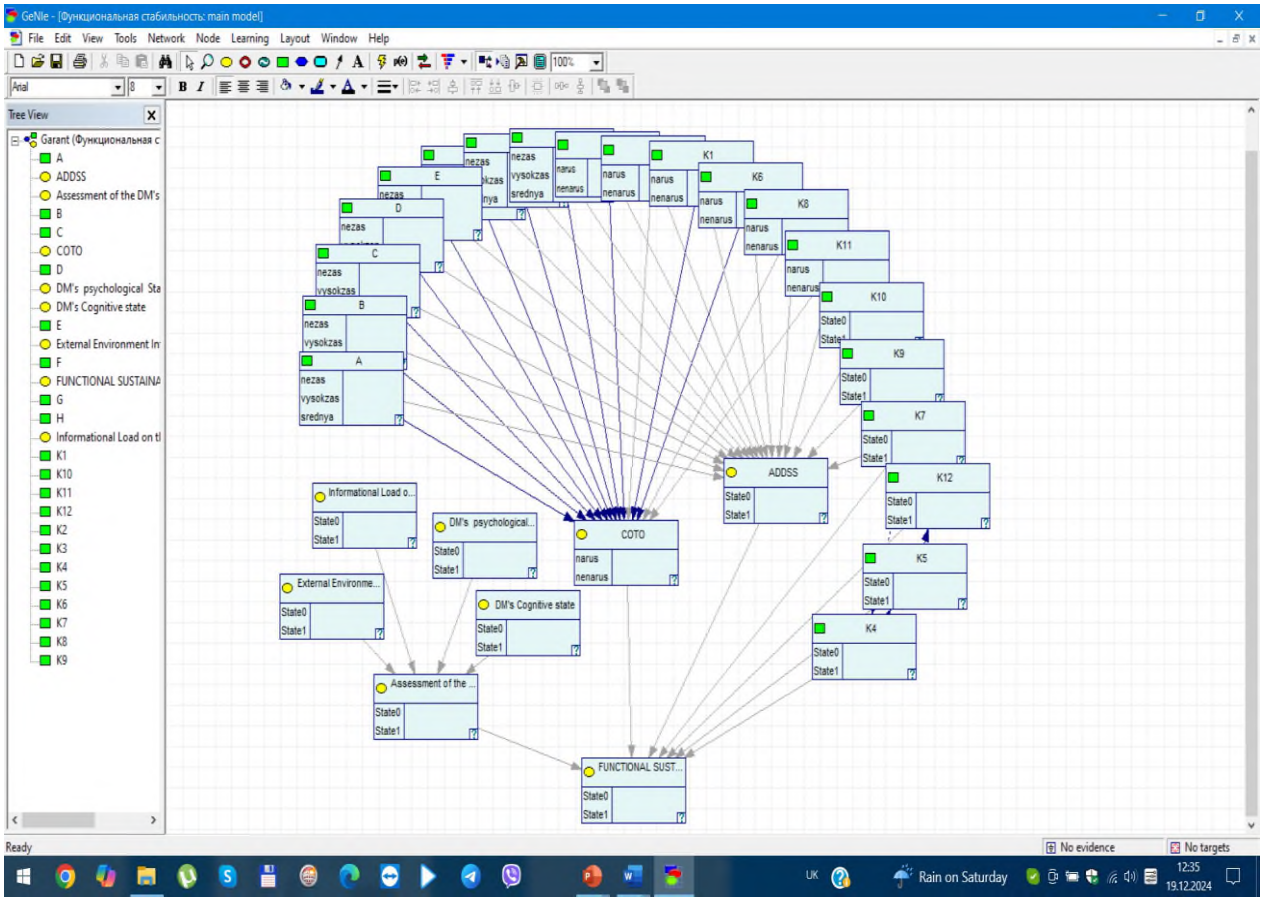


Рисунок 3.5 - Повна модель графа оцінки стану комплексної інформаційної безпеки АРБД.

Для погодженості думок експертів визначення умовних ймовірностей можливих станів вершин БМД застосовані методи експертних оцінок.

Експертизу проводили експерти, які мають досвід з інформаційної безпеки АРБД, і по скільки необхідно визначити тільки ранги факторів безпеки, то

погодженість їх оцінок доцільно визначати за допомогою множинного коефіцієнта конкордації K_0 запропонованого М. Кендаллом і Б. Смітом [27-28].

У якості експертів залучені спеціалісти де експертам (m) пропонувалося привласнити ранг (n) факторам інформаційної та кібернетичної безпеки.

Погодженість думок експертів перевіряється за допомогою F- критерія Фішера [26]. Де через (Xij) позначено ранг j -го виду інформації ($j = \underline{1,n}$) у ранжировкі i -го експерта ($i = \underline{1,n}$). Для оцінки підготовленості експертів дотримуємось умови:

$$\sum_{j=1}^{n} X_{ij} = 0{,}5n(n+1) \tag{3.10}$$

де: $\sum_{j=1}^{n} X_{ij}$- сума рангів у ранжировці j -го експерта.

Погодженість експертів при ранжировці груп інформації оцінювалася коефіцієнтом конкордації (згоди):

$$K_0 = \frac{12S}{m^2(n^2-n)-m\sum_{i-1}^{m} T_i} \tag{3.11}$$

де: $S = \sum_{j-1}^{n} di^2$ - сума квадратів відхилень сум рангів, отриманих усіма групами інформації, від середньо – арифметичного сум рангів

$$d_j = X_j - 0{,}5m(n+1) \tag{3.12}$$

де: d - відхилення суми рангів j-*го* виду від середнього значення сум рангів по всім видам;

$$T_j = \sum_{\mu=1}^{n}({t_{\mu i}}^3 - t_{\mu i}) \tag{3.13}$$

де: $T_{\mu i}$-число повторень μ -го рангу в ранжировці і-*го* експерта.

При $К_0$ = 1 думка експертів вважається узгодженою повністю. При К*о <1*,

згідно з рекомендаціями для перевірки значимості погодженості визначаються значення статистики X^1 і X^2:

$$X_{\text{набл}}^{(1)} = K_0 m(n-1) \tag{3.14}$$

$$X_{\text{набл}}^{(2)} = \frac{(m-1)X^{(1)}}{m(n-1)-X^{(1)}} \tag{3.15}$$

Після чого необхідно визначити числа ступенів свободи (υ1) і (υ2) розподілу, для чого обчислюються значення величин;

$$\upsilon_1 = n-1\,,$$

$$\upsilon_2 = \frac{L^2}{(m-1)\sum_{j=1}^{n} V_j^2} - (m-1) \tag{3.16}$$

де: $L = (m-1)\sum_{j=1}^{n} V_j$

$$V_j = \frac{1}{(m-1)\sum_{i=1}^{m}(X_{ij}-X_j^2)} \tag{3.17}$$

$$X_j = \frac{1}{m}\sum_{i=1}^{m} X_{ij}, \quad j = \underline{1,n}$$

По таблиці F – розподілу Фішера порівнюємо критичне значення $F_{кр.}$ при рівні значимості α =0.05 і числах ступеню свободи υ1 і υ2. Порівнюючи отримане значення *X*набл зі значеням $F_{кр.}$ робимо висновок, що думки експертів можна вважати погодженими.

Метод експертних оцінок – це методологія, що використовується для збору та аналізу думок кваліфікованих фахівців з метою оцінки різноманітних явищ, процесів, проектів чи рішень. У даному випадку було взято до уваги оцінки десяти експертів, що оцінили фактори впливу Інформаційної та кібернетичної безпеки АРБД. Оцінки експертів наведено нижче (табл. 3.1 – 3.3).

Таблиця 3.1 – Фактори інформаційнох безпеки.

Вершина	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**
Стан	**Імовірність захищеності**							
Висока	0,95-1	0,9 -1	0,85-1	0,95-1	0,9-1	0,8-1	0,9-1	0,95-1
Середня	0,4-0,95	0,4-0,9	0,4- 0,85	0,45- 0,9	0,4- 0,9	0,4- 0,8	0,4- 0,9	0,4-0,95
Низька	0 - 0,4	0 - 0,4	0 - 0,4	0 - 0,45	0 - 0,4	0 - 0,4	0 - 0,4	0 - 0,4

Таблиця 3.2 - Фактори кібернетичної безпеки

Вершин	**К1**	**К2**	**К3**	**К4**	**К5**	**К6**	**К7**	**К8**	**К9**	**К10**	**К11**	**К12**
Стан	**Імовірність захищеності**											
Висока	0,85-1	0,9--	0,85-1	0,8-1	0,95-	0,9-1	0,9-1	0,9-1	0,7-1	0,85-	0,9-1	0,9-1
Середня	0,15-0,8	0,1-0,	0,15-0,	0,2-0,	0,1-0,	0,1-0,	0,1-0,	0,1-0,	0,3-0	0,1-0,	0,1-0	0,1-0
Низька	0-0,15	0-0,1	0-0,15	0-0,2	0-0,0	0-0,1	0-0,1	0-0,1	0-0,3	0-0,1	0-0,1	0-0,1

Таблиця 3.3 - Фактори емоційно-когнітивного стану ОПР.

Батько	Informational Load on the DM		External Environment Influence the DM		Інші причини
Стан	negative	positive	negative	positive	
unstable	0,67	0,0	0,85	0,0	0,01
stable	0,33	1,0	0,15	1,0	0,99
батько	DM's Cognitive state		DM's psychological State		інші причини
стан	negative	positive	negative	positive	
unstable	0,62	0,0	0,73	0,0	0,01
stable	0,38	1,0	0,27	1,0	0,99

Використовуючи результати оцінок наведених в таблицях 3.1-3.3 та обчислення ймовірностей за формулами (3.4-3.9) доцільно прорахувати ефективність БМД за допомогою спеціалізованого програмного пакета GeNle Academic 4.1. На рисунку 3.3 наведений приклад результатів оцінки факторів впливу.

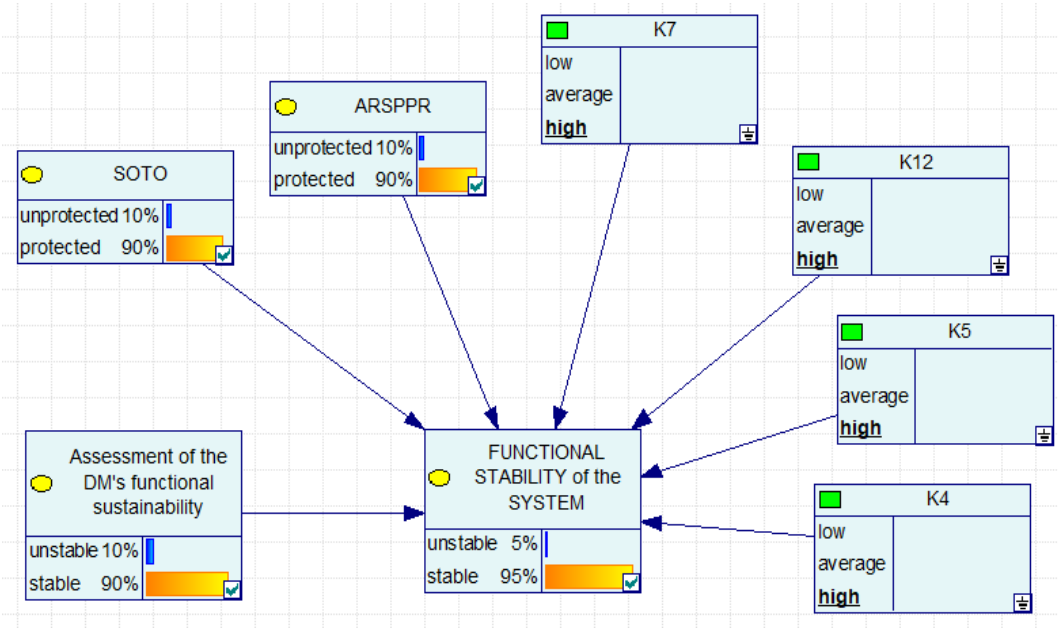


Рисунок 3.6 - Результат оцінки Імовірності комплексної інформаційної безпеки АРБД при високій захищеності вузлів К4,К5, К12.

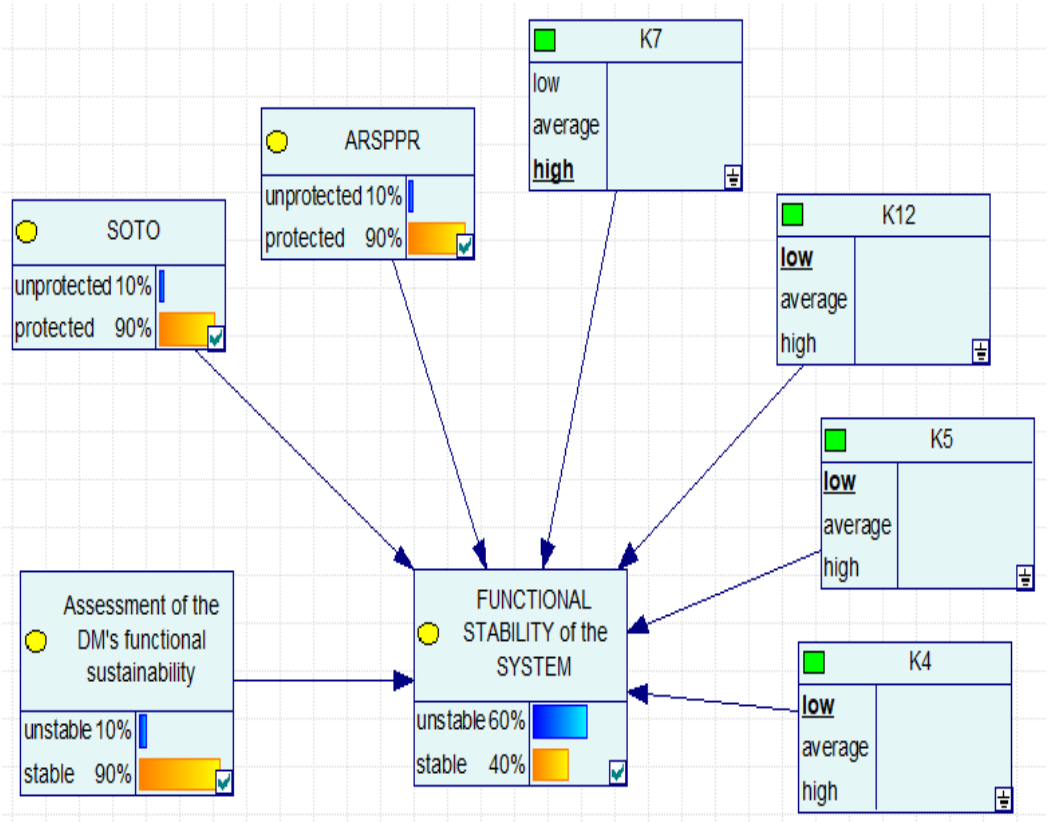


Рисунок 3.7 – Результат оцінки Імовірності комплексної інформаційної безпеки АРБД при низькій захищеності вузлів К4,К5, К12.

Висновки до третього розділу: У розділі проведена розробка моделей і алгоритмів побудови комплексної інформаційної безпеки розподіленої адаптивної БД. Розроблена інформаційна та інформаційно - логічна моделі розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки в складі СППР.

Наведена повна структура інформаційної моделі АРБД, яка містить у собі набори модулів, субмодулів та інших ділянок програмних рішень різних завдань. Для взаємодії з ОПР під час критичних станів системи, СППР має інтегрований засіб АРБД.

В даному розділі розроблена математична модель оцінки стану комплексної інформаційної безпеки СППР з розподіленою адаптивною БД з використанням математичного апарата Байесовської мережі довіри. Для визначення життєздатності побудованої моделі використаний метод експертних оцінок та побудована і досліджена Байєсівська мережа довіри, де стан комплексної інформаційної безпеки розподіленої адаптивної БД визначається відповідними факторами інформаційної та кібернетичної безпеки.

Проведено ряд експериментів з оцінки інформаційної безпеки та захищеності адаптивної розподіленої БД, результати досліджень яких показали значну перевагу запропонованих моделей і алгоритмів в порівняні з існуючими.

Результати оцінки Імовірності комплексної інформаційної безпеки АРБД розраховувались та отримані за допомогою спеціалізованого програмного пакета GeNle Academic.

4 ПРОГРАМНО-ІНСТРУМЕНТАЛЬНІ ЗАСОБИ РОЗРОБКИ РОЗПОДІЛЕНОЇ БД З ЗАБЕЗПЕЧЕННЯМ КОМПЛЕКСНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1 Розробка узагальненої структури програмної частини роботи з АРБД.

Узагальнена структура програмної частини для реалізації роботи з інтерфейсом ОПР і базою даних наведена на рисунку 4.1. Дана структура розділена на три окремі блоки: «Блок роботи з інтерфейсом», «Блок роботи з базою даних і прийняття рішень» та «Блок роботи з пошуком в WEB і формуванням знань» [32]. Кожна система має свої вбудовані модулі.

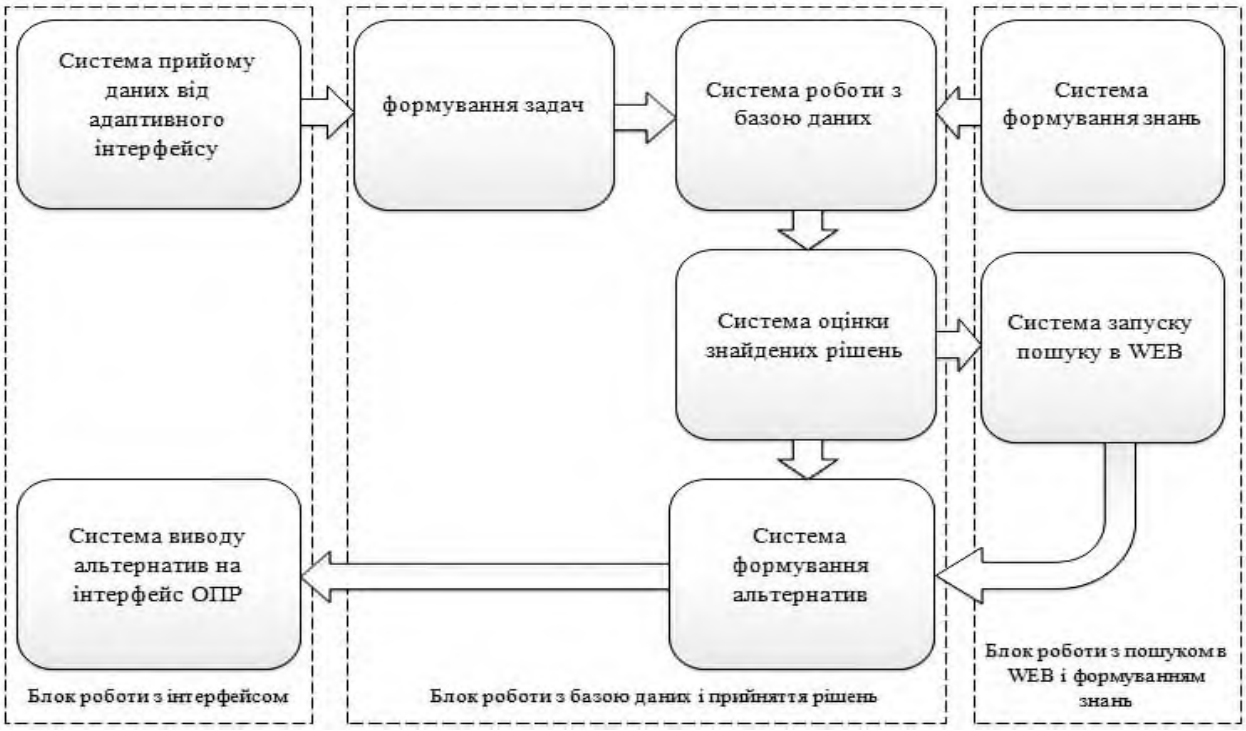


Рисунок 4.1 - Узагальнена структура програмної частини роботи з АРБД.

Блок роботи з інтерфейсом - забезпечує взаємний зв'язок з інтерфейсом, передачу і прийом даних [33]. Складається з 2-х систем таких як, «Система прийому даних від адаптивного інтерфейсу» і «Система виведення альтернатив на інтерфейс ОПР». Ці системи мають модулі захисту з’єднання та перевірки прав доступу до АРБД.

Блок роботи з базою даних і прийняття рішень - призначений для перетворення вхідних параметрів прийнятих від «Інтерфейсу ОПР» в критерії пошуку по АРБД. Надає можливість вибірки з АРБД рішень і оцінку їх достовірності, а також формування альтернатив виходячи з рішень, вибраних з АРБД.

Найдені рішення оброблюються «системою оцінки знайдених рішень», та в разі успішного оцінювання, рішення поступають до «системи формування альтернатив». Якщо рішення вибрані з АРБД не задовольняють критерії оцінювання, то дані технологічного процесу відправляються до «пошукової системи в WEB». Провернені рішення з пошукової системи потрапляють до системи формування альтернатив.

Система формування альтернатив на основі прийнятих «множини результатів психологічних і розумових тестів ОПР» та «множини даних зовнішніх факторів впливу на ОПР» вибирає з АРБЗ допоміжні частки та перетворює рішення в альтернативи. Після перетворення альтернативи повертаються до «блоку роботи з інтерфейсом».

Блок роботи з пошуком в WEB і формуванням знань - даний блок виконує задачу зв’язку між «блоком роботи з базою даних» та «системою пошуку в WEB». Формалізацією запиту і передачі його системі пошуку. Запуском «системи пошуку в WEB», передачею значень та прийомом результатів пошуку.

В даний блок також входить система формування знань на базі сценарного підходу. Вона використовується для представлення доступу експертам до АРБД та БЗ. Завдяки даній системі експертам, які мають права доступу, представляються всі операції роботи з АРБД, такі як: зчитування, запис, редагування та видалення записів.

Узагальнена структура АРБД.

Структура АРБД для адаптивної СППР показана на рисунку 4.2., де головними таблицями являються: «технологічний процес», «психологічна і когнітивна складова» та «фактори впливу зовнішнього середовища».

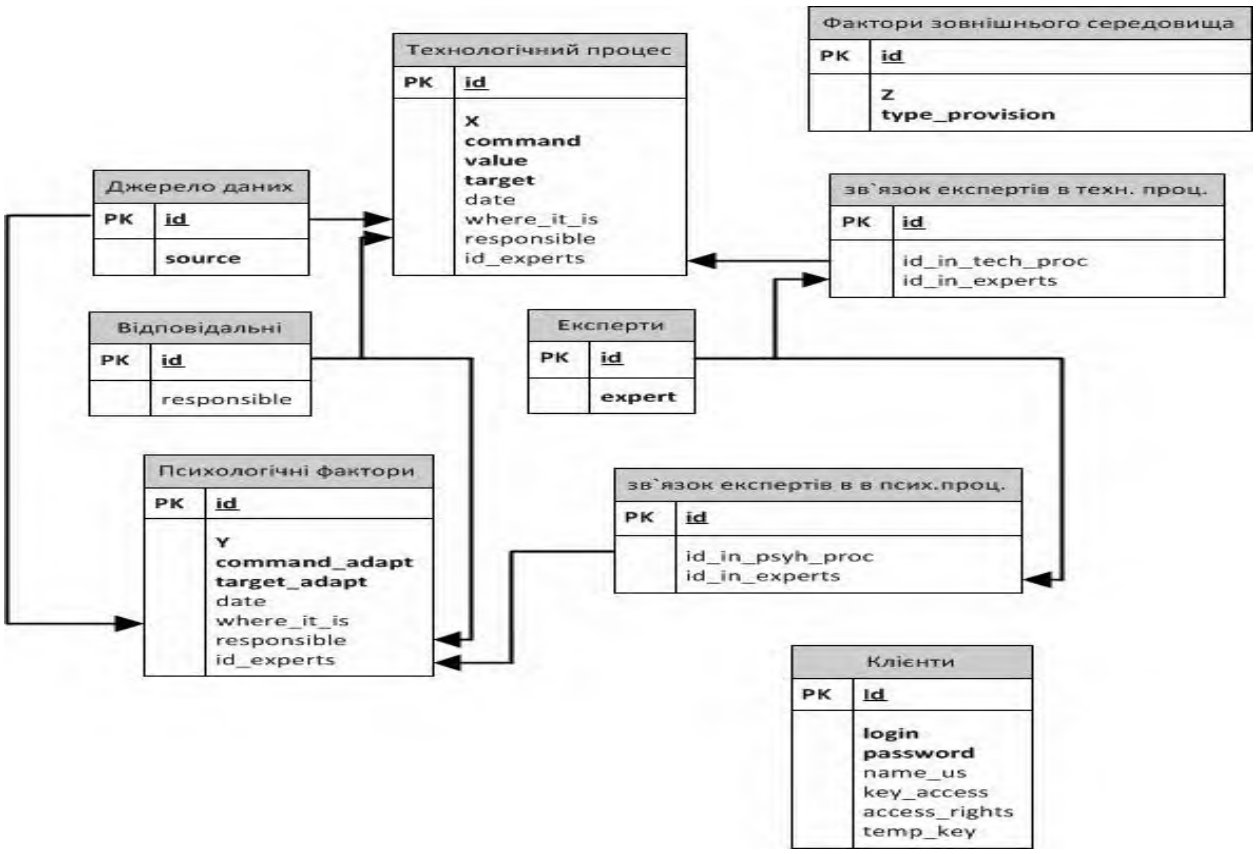


Рисунок 4.2 - Узагальнена структура АРБД.

4.2 Розробка алгоритмів роботи комплексної Інформаційної та кібернетичної безпеки АРБД.

Для повноцінного функціонування комплексної інформаційної безпеки (ІБ) необхідно розробити алгоритми функціонування віх модулів призначених для обчислення інформаційної безпеки адаптивної розподіленої БД (рис.3.1). Надалі приведено повний опис розробки алгоримів модулів.

- Модуль моніторингу входу користувача з правами Адміністратора - Алгоритм даного модуля представлено на рис. 4.3. По завершенню успішної авторизації в сесії записуються ключі для аутентифікації і спеціальні дані з дозволами і правами доступу. Метод роботи модуля для перевірки входу користувача з правами адміністратора здійснює пошук активних користувачів, потім вибирає інформацію з сесій і аналізує, які права дозволені користувачеві. Всі права пов'язані з адмініструванням системи, будуть проаналізовані та враховані для розрахунку ймовірності, це показує ступінь входів користувачів або клієнтів з правами адміністраторів.

- Модуль аналізу системи на віруси, призначений для аналізу та усунення шкідливих програм. Алгоритм даного модуля представлено на рис. 4.4. Для аналізу системи на віруси, проводиться перевірка (сканування) і за результатами сканування розраховуючи кількість заражених файлів, обчислюється ймовірність поточного стану системи по впливу вірусів на працездатність програмного забезпечення.
-

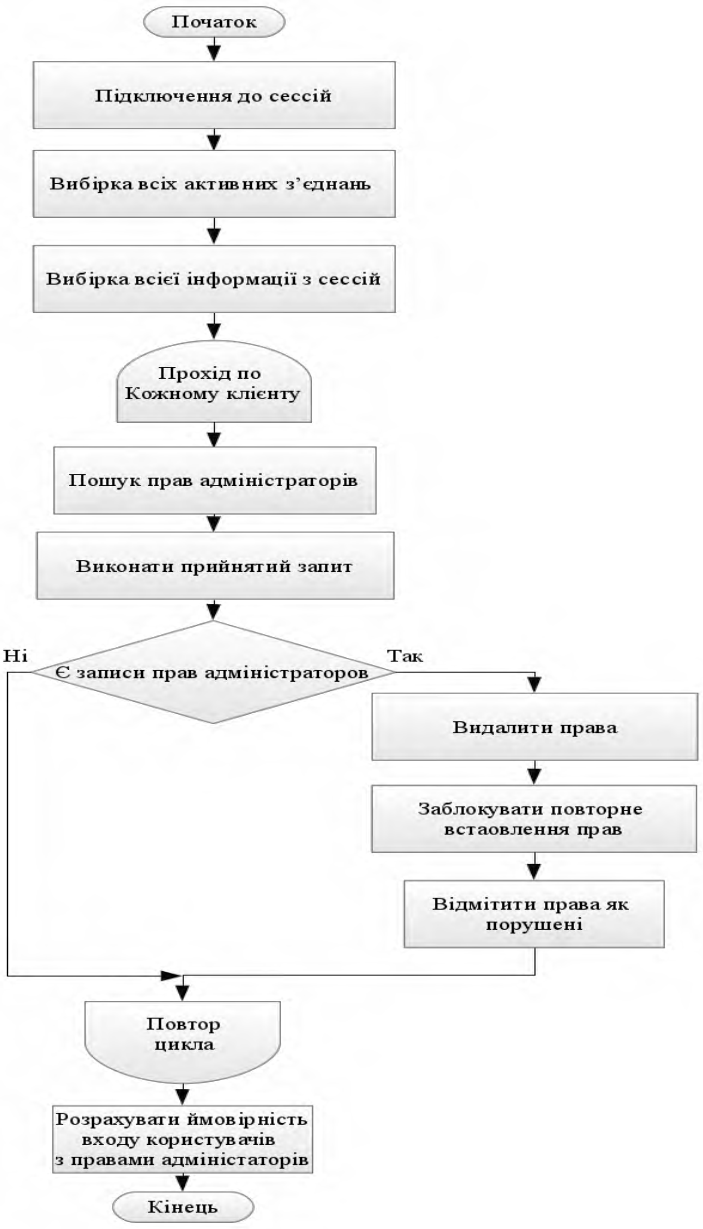


Рисунок 4.3 - Модуль моніторингу входу користувачаз правами адміністатора.

Рисунок 4.4 - Модуль аналізу системи на віруси.

- Модуль попередньої підстановки в запити даних та перевірка на SQL-ін'єкції. Цей модуль приймає дані, потім проводить вибірку запитів, куди будуть підставлятися дані. Проводить процес підстановки даних в запит. Після цього підключається до спеціальної тестової таблиці БД і виконує запити. Процес оцінки виконується на основі результатів. Над результатами проводиться аналіз. Проаналізувавши, система розраховує кількість SQL - ін'єкцій і переводить в імовірнісний формат, який і показує, наскільки система схильна до SQL - ін'єкцій. Алгоритм модуля приведено на рисунку 4.5.

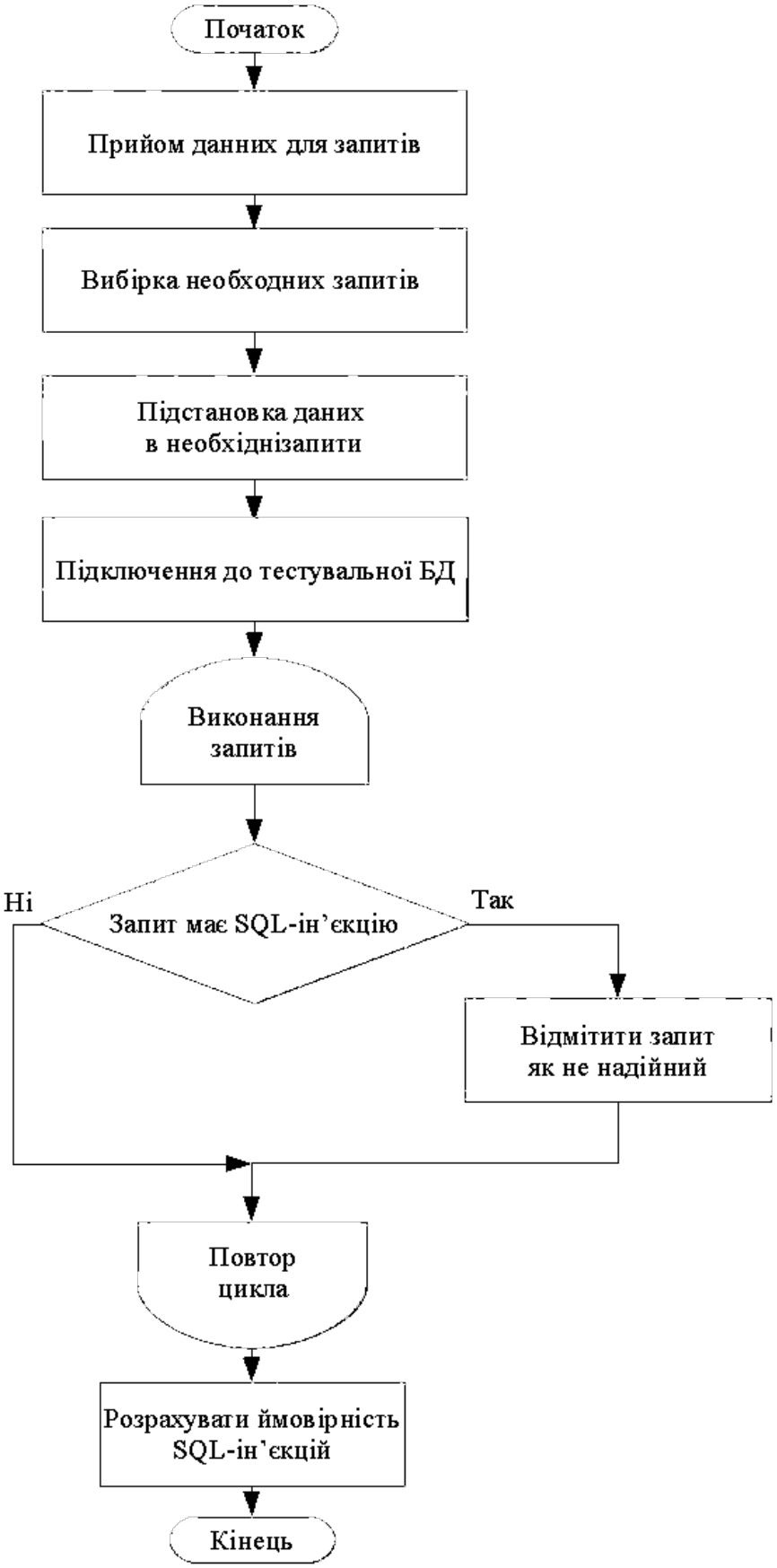


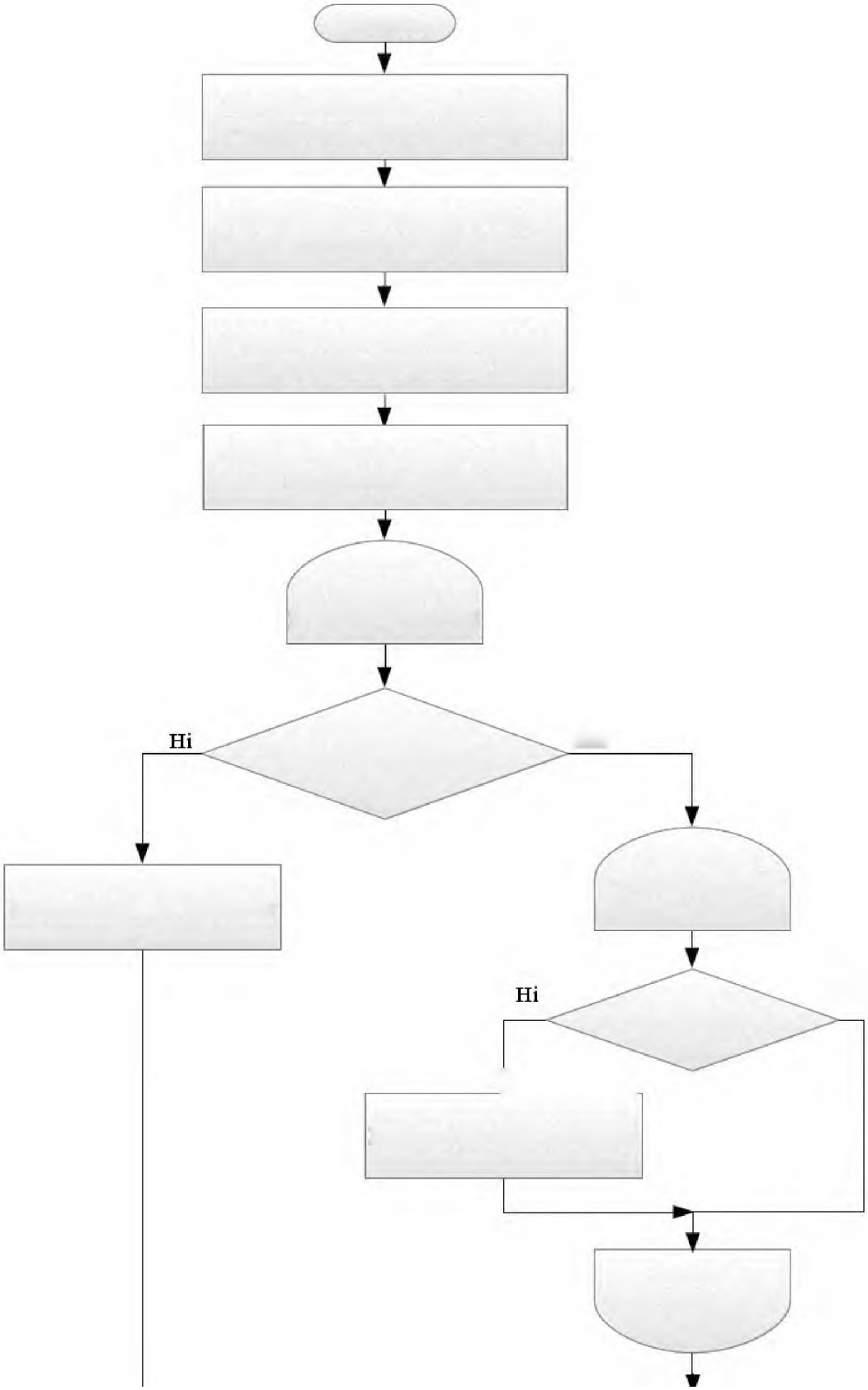
Рисунок 4.5 - Модуль попередньої підстановки даних та перевірка на SQL-ін'єкції

- Модуль моніторингу апаратних збоїв. Алгоритм модуля приведено на рисунку 4.6. Модуль працює за принципом сканування переліку віддалених робочих станцій, БД, програмних пакетів, а також усіх необхідних комп'ютерів, які входять до складу СОТО. У спеціальній таблиці зберігається інформація зі списком необхідних вузлів, БД і т.п. Модуль моніторингу апаратних збоїв вибирає список з БД і в циклічному режимі проводить опитування кожного з пристроїв. Потім відбувається вибірка зі спеціальної БД списку необхідних БД і також по черзі проводить підключення до БД. У разі успішної перевірки заданого вузла або БД цей вузол відзначається як перевірений. Ті вузли, з якими модуль не зміг встановити зв'язок, відзначаються як неперевірений. Співвідношенням загального числа вузлів і БД до кількості успішно перевірених вузлів є ймовірність рівня апаратних збоїв не тільки АРСППР а й СОТО.

- Модуль моніторингу доступності даних і ресурсів виконує попередню вибірку даних для аналізу їх доступності. Алгоритм модуля приведено на рисунку 4.7. Принцип роботи модуля заснований на перевірці доступності даних. Під поняттям дані мається на увазі список таблиць БД, а також список програмних пакетів. Принцип роботи модуля схожий на принцип роботи модуля моніторингу апаратних збоїв, відмітною особливістю є сканована інформація. Модуль підключається до спеціальної таблиці в БД в якій зберігається список таблиць з іменами БД і список назв програмних пакетів. Після вибірки запускається виконання поетапної перевірки даних. Для таблиць це - визначення назви БД і підключення до неї. Спроба вибрати всі дані із заданої таблиці і відзначити про успішне виконання, якщо запит на вибірку повернув дані, тобто не порожній результат або відзначити про неуспішне завершення перевірки доступності даних, якщо результат запиту виявився порожнім. Порожній результат може описувати одну з двох причин:

1. Таблиці не існує;

2. З якихось причин дані, що повинні зберігатися в таблиці пропали або хтось видалив.


Hi
Hi

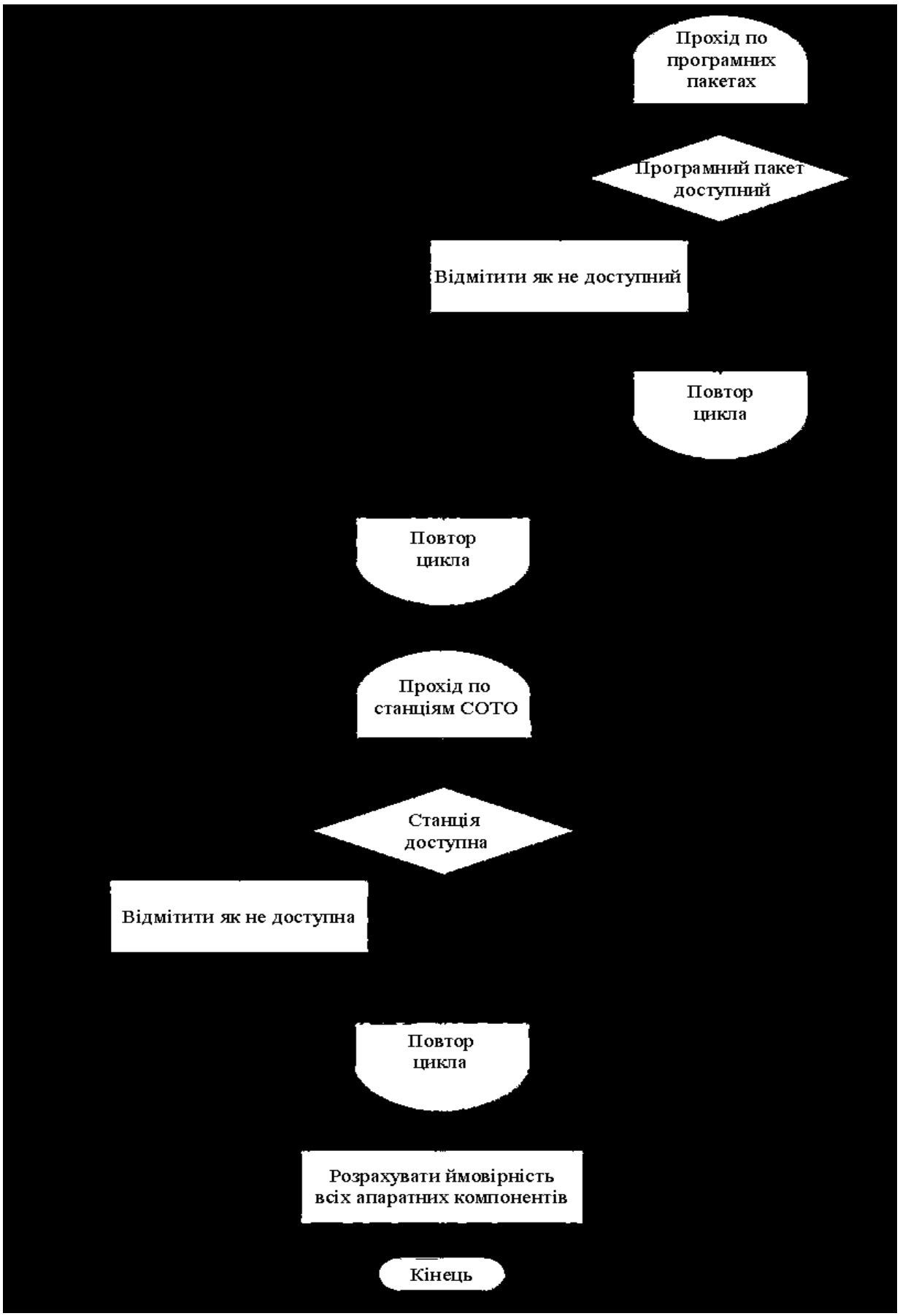
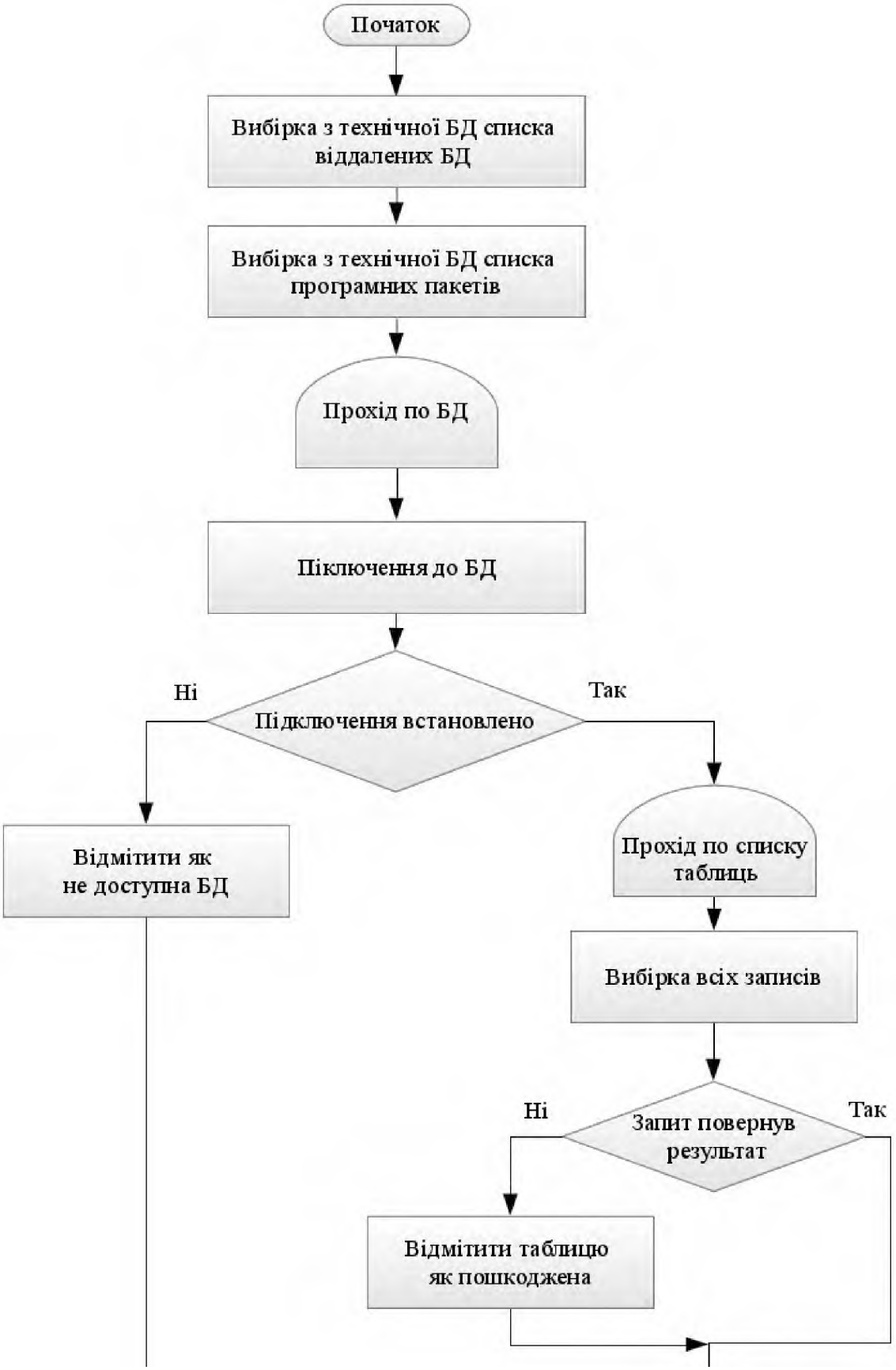


Рисунок 4.43 — Модуль моніторингу апаратних збоїв


Початок
Вибірка з технічної БД списка віддалених БД
Вибірка з технічної БД списка програмних пакетів
Прохід по БД
Піключення до БД
Підключення встановлено
Ні
Так
Відмітити як не доступна БД
Прохід по списку таблиць
Вибірка всіх записів
Запит повернув результат
Ні
Так
Відмітити таблицю як пошкоджена

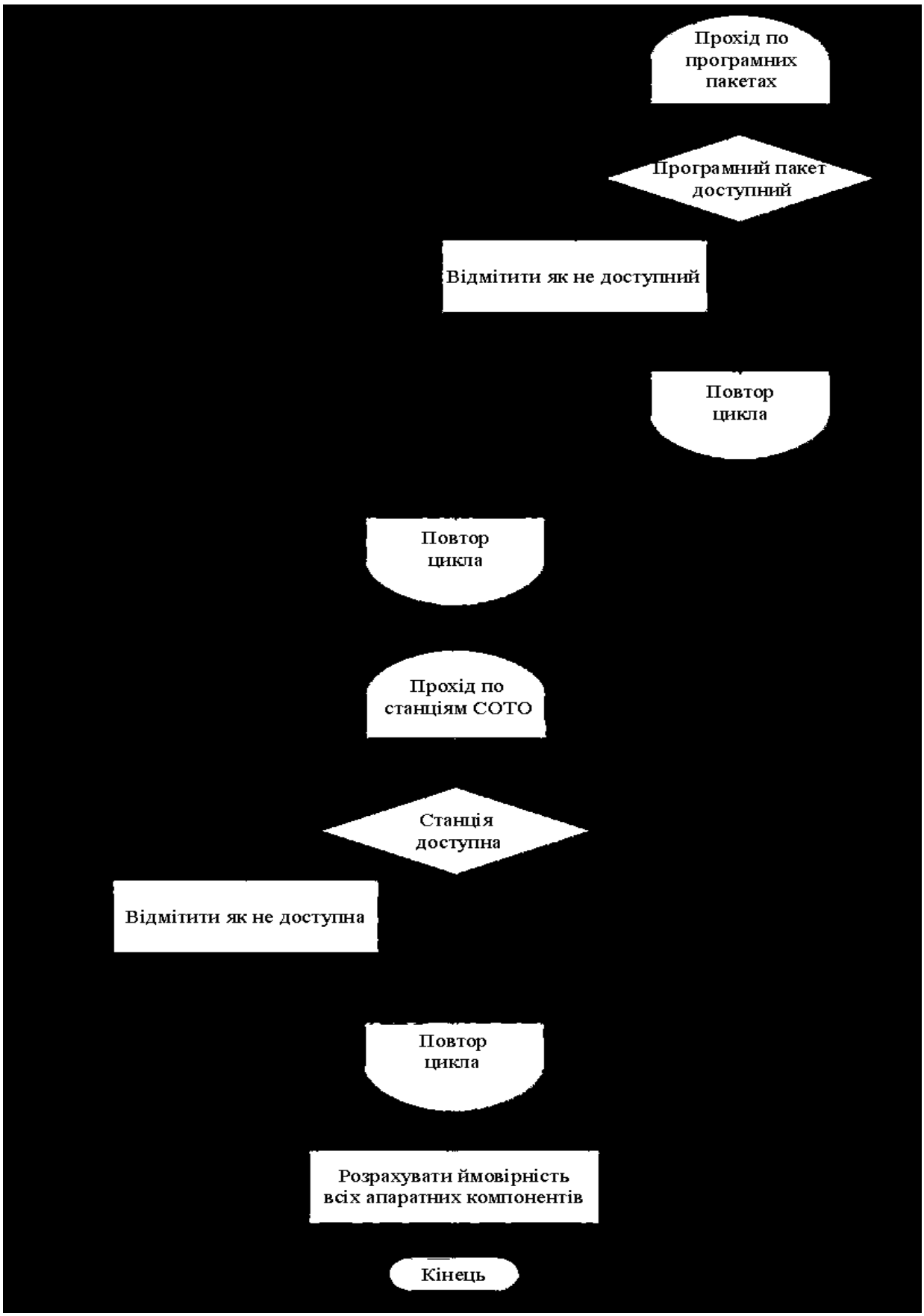


Рисунок 4.8 — Модуль моніторингу доступності даних та ресурсів

Для програмних пакетів це - прохід по всіх іменах програмних пакетів (файлів) і проведення операції зчитування даних з файлу. Найчастіше програми написані на PHP, зберігаються як ісходник, і будь-який пакет повинен мати в собі хоча - б одну строку коду. Для початку програмні пакети шукаються спеціальною функцією, а потім проводиться перевірка пакетів. Перевірка пакетів здійснюється функцією зчитування інформації з файлу, для цього в PHP є функції fopen() & fread() або file_get_contents(). Де в дужках вказується файл з абсолютним або відносним адресом. Ці функції повертають текст (програмний код) прочитаний з файлу у вигляді масиву, де кожен рядок має свій індекс. Перевірка на порожнечу масиву можна призвести функцією count() або sizeof(). Результати перевірки проходять математичне обчислення, завдяки якому результатом є ймовірність, яка показує ймовірність доступності даних і ресурсів.

- Модуль некоректної роботи користувача. Алгоритм програми приведено на рисунку 4.45. Програмне забезпечення, спеціально розроблене постійно супроводжує користувача і аналізує всі дії користувача. У разі коли, користувач навмисно вводить спеціальну адресу, або редагує існуючий, або багаторазово намагається пройти в захищену зону, або впроваджує SQL - ін'єкції, програма записує всі поведінки в спеціальну резервну БД, в якій зберігається інформація про метод злому, час, імені користувача, і ще всяка службова інформація. Модуль некоректності дій користувачів аналізує цю БД, тільки не повністю. Точка початку аналізу, цей час останнього запуску даного модуля, це необхідно для того що б, не враховувати попередніх дій користувачів. Після сканування БД система розраховує кількість некоректних дій з урахуванням типів дій, для визначення сили впливу на всю систему, потім обчислює ймовірність впливу на систему внаслідок некоректних дій користувачів або адміністраторів.

Рисунок 4.9 - Модуль некоректної роботи користувача

- Модуль перевірки даних на цілісність (рисунок 4.46) (використовуючи хеш) всім відомий факт про те що дані, збережені в БД, та й просто інформація, яка зберігається в електронній обчислювальній машині, має великий недолік це проблема цілісності даних. Модуль перевірки даних на цілісність проводить підключення до резервної БД і вибирає весь список назв баз даних, їх таблиць, а також усіх хеш-функцій, які притаманні таблицями. Далі відбувається циклічне підключення до БД-х, потім вибірка таблиць, потім вибірка з таблиць записів. Записи проходять через функцію обчислення хеш-образу і результати виконання

хеш-функції порівнюються із заздалегідь вибраними з резервної БД. У разі збігу хешів, ставиться відмітка про успішну перевірку поля. Далі всі процедури повторюються з наступним записом, потім з наступною таблицею, і з наступною БД. Розрахунок ймовірності обчислюється шляхом співвідношення кількості хешів, які необхідно перевірити на кількість хешів, які успішно були перевірені. Результатом є ймовірність що надає рівень пошкодження інформації в базах даних.

- Модуль перевірки інформації на присутність підміни даних. Алгоритм модуля приведено на рисунку 4.47. У програмній частині, де виконуються запити на вставку даних, реалізований механізм запису дати і часу виконання запиту в спеціальне поле таблиці, а також запис ідентифікатора поля і дату з часом в спеціальну системну таблицю. У разі, коли зловмисник виконає SQL - ін'єкцію запиту, яка буде виконуватися в іншому методі об'єкта, де немає реалізації на вставку дати в спеціальну таблицю, дані не будуть занесені в неї, не дивлячись на те, що зловмисник замінив дані в основній таблиці. На основі такої різниці дат можна визначити, де була змінена інформація. Для відстеження підміни, модуль виконує прохід за списком дат і ідентифікаторів в спеціальній БД, потім відбувається підключення до баз даних, потім виробляється вибірка таблиць з баз даних, і по черзі виконується порівнювання дат та полів з датами, які зберігаються в спеціальній БД. У разі, коли дати не рівні, можна припускати, що інформація в полі, була підмінена. За результатами проведення перевірки, відбувається обчислення ймовірності, наскільки інформація піддалася підміні даних.

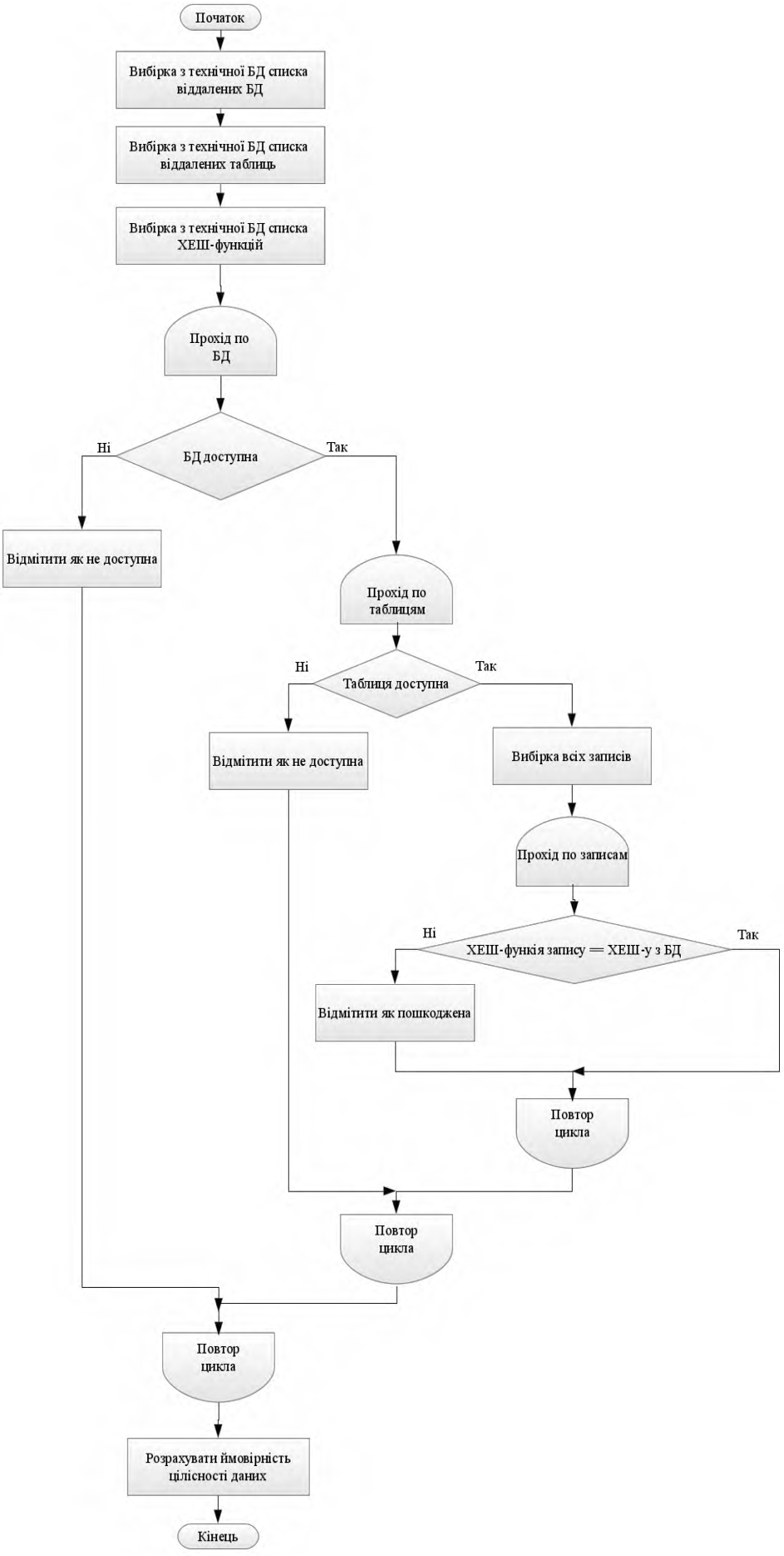


Рисунок 4.10 - Модуль перевірки даних на цілісність (використовуючи ХЕШ)

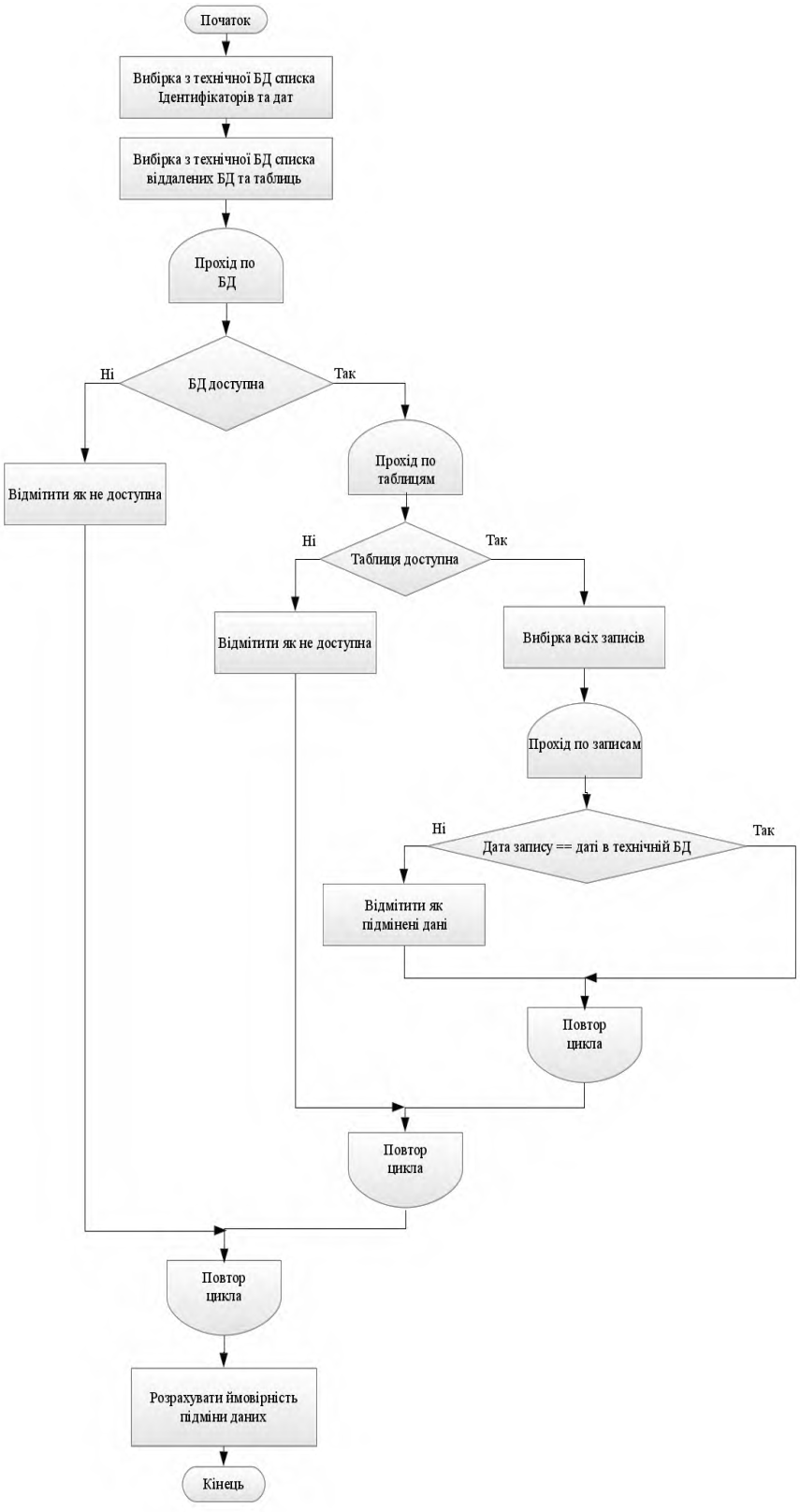


Рисунок 4.11 - Модуль перевірки інформації на присутність підміни даних

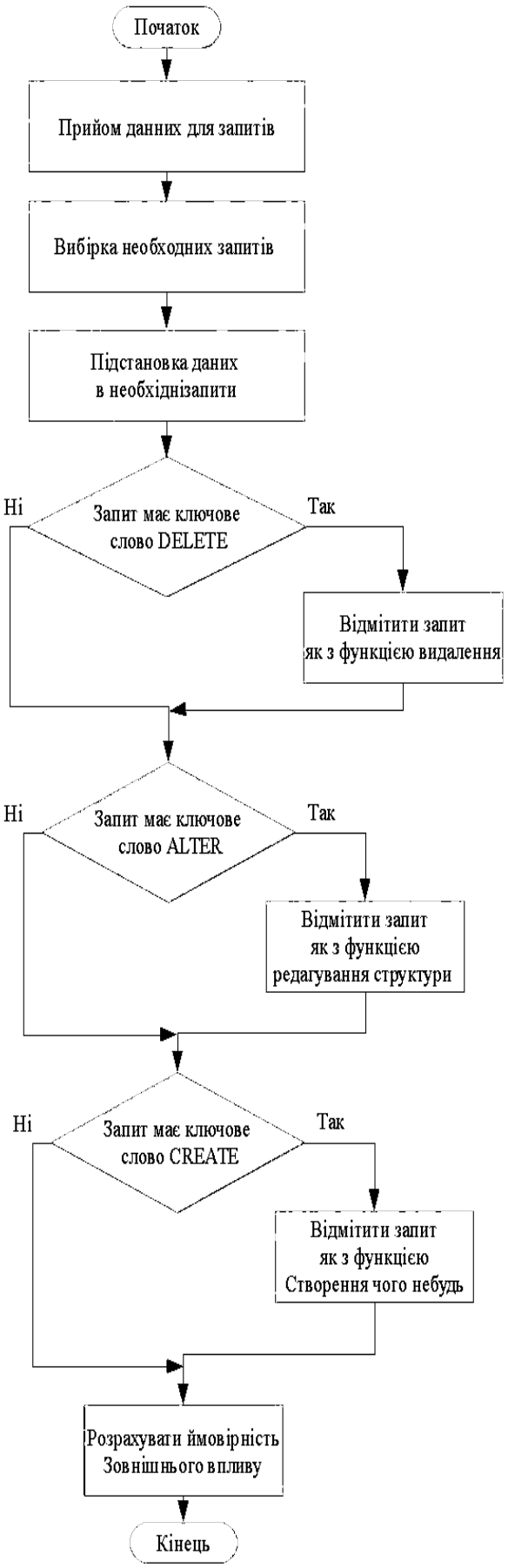


Рисунок 4.12 - Модуль перевірки на зовнішній вплив

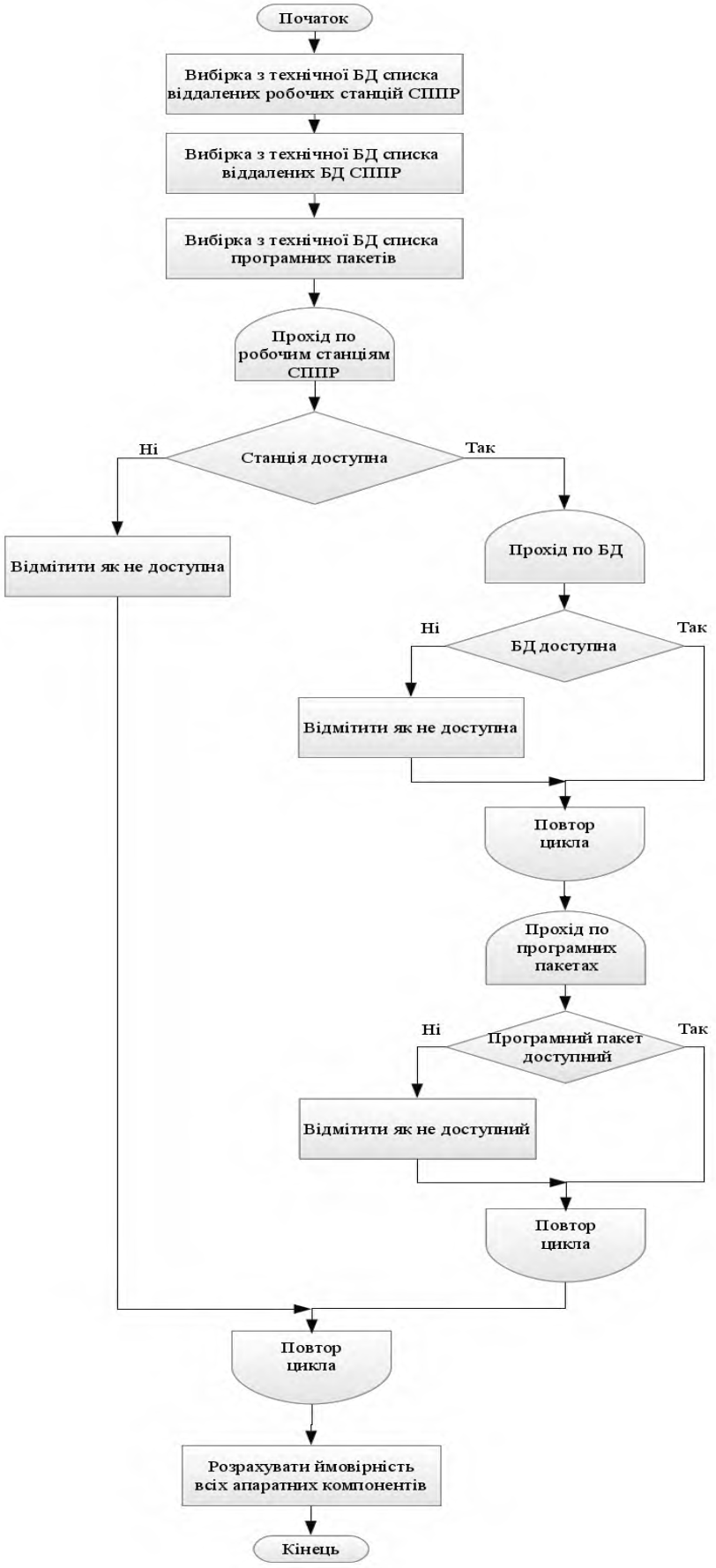


Рисунок 4.13 - Модуль перевірки відмов апаратного забезпечення

Рисунок 4.14 - Модуль перевірки відмов програмного забезпечення

Висновки до четвертого розділу: У даному розділі проаналізовані програмно-інструментальні засоби розробки розподіленої БД з забезпеченням комплексної інформаційної безпеки. Розроблена узагальнена структура програмної частини роботи з АРБД.

Для реалізації повноцінного функціонування комплексної інформаційної безпеки розроблені алгоритми функціонування відповідних модулів призначених для забезпечення та оцінки інформаційної безпеки адаптивної розподіленої АРБД.

Наведено повний опис розробки та функціонування алгоритмів відповідних модулів забезпеченням комплексної інформаційної безпеки АРБД та розроблений код програмного забезпечення реалізації цих алгоритмів.

ВИСНОВОК

У даній роботі запропоновані основні положення побудови розподілених Баз даних, основними особливостями якої є використання якісних і кількісних ознак бази, що визначаються різними технологіями їх розробки. Розглянуті моделі та алгоритми побудови розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки. Використання розподіленої БД призначено для розділення даних на окремих рівнях. Кожен рівень структурований на конкретну область використання. Захист доступу реалізовується обмеженням прав доступу, а також використання розподілу даних на окремих рівнях, завдяки цьому фізично неможливо отримати доступ з одного рівня до іншого.

Для забезпечення довгострокової та безвідмовної роботи АРБД в складі СППР розроблено комплекс заходів та програмного забезпечення до складу якої входить дві групи заходів захисту.

Визначені основні особливості побудови та застосування розподіленої адаптивної БД з забезпеченням комплексної інформаційної безпеки в СППР.

Проведений аналіз та основні вимоги структурної організації розподілених адаптивних БД з забезпеченням комплексної інформаційної безпеки.

Розроблена інформаційна модель формування запитів користувачів та структура адаптивної розподіленої БД.

Розроблена математична модель оцінки комплексної інформаційної безпеки та алгоритмів функціонування розподіленої БД при формуванні запитів, .з використанням теорії ймовірності Байесовської мережі довіри.

Проведено ряд експериментів з оцінки інформаційної безпеки та захищеності адаптивної розподіленої БД, результати досліджень яких показали значну перевагу запропонованих моделей і алгоритмів в порівняні з існуючими.

ПЕРЕЛІК ПОСИЛАНЬ

1. Доктрина інформаційної безпеки України від 25 лютого 2017 року №47/2017

2. Закон «Про критичну інфраструктуру» від 16.11.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/1882-20

3. Закон України Про національну безпеку України Форма доступу - https://zakon.rada.gov.ua/laws/show/2469-VIII

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" Указ Президента України; Стратегія від 26.08.2021 Форма доступу - https://www.president.gov.ua/documents/4472021-40013

5. Закон України Про основні засади забезпечення КБ Форма доступу - https://zakon.rada.gov.ua/laws/show/2163-19

6. Закон України «Про інформацію» Редакція від 16.07.2020 Форма доступу - https://zakon.rada.gov.ua/laws/show/2657-12

7. Закон України «Про захист інформації в інформаційно телекомунікаційних системах» Редакція від 04.07.2020 Форма доступу - https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

8. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» Редакція від 10.02.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF

9. Закон України «Про захист персональних даних» Редакція від 15.12.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/2297-17 10. Закон України

10. «Про державну таємницю» Редакція від 24.11.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/3855-12

11. Thor Olavsrud. 4 information security threats that will dominate 2017. CIO (December 29, 2016) [Online tool]. – Available at : https:// cio.com/article/

3153706/security/4-information-security-threats-thatwill-dominate-2017.html.

12. Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions / L. Bagherzadeh, H. Shahinzadeh, H. Shayeghi,

13. A. Dejamkhooy, R. Bayindir, M. Iranpour // 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), Keonjhar, Odisha, July 29–31, 2020, Keonjhar, Odisha, India. P. 1–8.

14. Тарасенко Ю.С., Соляннiков В.Г., Калюжний О.Е. Концептуально гносеологічні аспекти інформаційної безпеки (захищеності) з позицій соціальної інженерії, DOI: УДК 621.396.96 ISSN 2521-6643 Системи та технології № 2 (60) 2020 с.39-50

15. Тарасенко Ю.С., Соляннiков В.Г., Бруй І.І. Кібербезпека: інформаційні аспекти захисту від технологій впливу, Міжнародна науковопрактична інтернет- конференція «Інноваційні рішення в економіці, бізнесі, суспільних комунікаціях та міжнародних відносинах» (16 квітня 2021, Дніпро). – Дніпро: Університет митної справи та фінансів, 2021. с.424-426

16. Kaspersky Security Network. Развитие информационных угроз во втором квартале 2021 года. Отчеты о вредоносном ПО. Мобильная статистика. Целевые атаки. 12 авг 2021. https://securelist

17. Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions / L. Bagherzadeh, H. Shahinzadeh, H. Shayeghi,

18. A. Dejamkhooy, R. Bayindir, M. Iranpour // 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), Keonjhar, Odisha, July 29–31, 2020, Keonjhar, Odisha, India. P. 1–8.

19. Кайт Томас, Кун Дарл. Oracle для профессионалов: архитектура и методики программирования, 3-е изд.: Пер. с англ. - М.: 000 "ИД. Вильямс", 2016. - 960 с

20. Andrew S. Tanenbaum, Maarten van Steen, 2016. Distributed Systems: Principles and Paradigms 2nd Edition, pp.427-438

21. Andrew S. Tanenbaum, Maarten van Steen, 2017. Distributed Systems 3rd Edition, pp.324-328

22. Особливості проектування розподіленої бази даних [Електронний ресурс] – Режим доступу: https://studopedia.su/19_167104_osobennosti Proektirovaniya raspredelennoy bazi dannih.html

23. Яковлев Ю.С., 2017. О концепции построения и выбора распределенных баз данных информационно-поисковых систем [Электронный ресурс]– Режим:http://dspace.nbuv.gov.ua/bitstream/handle/123456789/727/6-

24. Yakovlev.pdf Distributed Database Architecture [Electronic Resource] – Mode of access:https://docs.oracle.com/html/E25494_01/ds_concepts001.htm

25. Проектування для розподілених баз даних [Електронний ресурс] – Режим доступу: http://bourabai.kz/dbt/servers/12.html.

26. Астахов И.Ф., Потапов А.С., Чулюков В.А., Стариков В.Н. Практикум по информационным системам. Oracale/ 2-изд., К., Юниор, 2004. -180 с.

27. Р. Гринвальд, Р. Стаковьяк. Oracle llg. Основы, 4-е издание. СПб.: Символ-Плюс, 2009.

28. Грег Риккарди. Системы баз данных. Теория и практика использования в Internet и среде Java. Вильямс, 2001.

29. Алапати Сэм Р. Oracle Database 11g: руководство администратора баз данных. : Пер. с англ. -М. : ООО “И.Д. Вильямс”, 2010. — 1440 с. : ил.

30. Oracle для профессионалов. Пер. с англ./ТомКайт- СПб.:ООО ДиаСофтЮП», 2003. - 672 с.

31. http://www.dissercat.com/content/modeli-i-algoritmy-sistemy-podderzhki-prinyatiya-reshenii-na-osnove-mnogomernykh-khranilishc

32. http://tekhnosfera.com/sistema-podderzhki-prinyatiya-resheniy-predpriyatiya-na-osnove-neyrosetevyh-tehnologiy

33. http://www.dissercat.com/content/modelirovanie-informatsionnoi-sistemy-upravleniya-predpriyatiem-na-osnove-intellektualnogo-a

34. http://tekhnosfera.com/intellektualnaya-sistema-podderzhki-prinyatiya-resheniy-na-osnove-ontologii

35. http://ref.rushkolnik.ru/v1552/

36. http://www.habarov.spb.ru/new_es/exp_sys/es06/es6.htm

37. http://ru.wikipedia.org/wiki/%D0%A1%D1%81%D1%8B%D0%BB%D0%BE%D1%87%D0%BD%D0%B0%D1%8F_%D1%86%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C

38. http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BD%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85

39. http://weldingshop.3dn.ru/publ/operacionnye_sistemy/bezopasnost_os/konfidencialnost_celostnost_i_dostupnost_dannykh/12-1-0-24

40. http://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8

41. http://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B1%D0%B0%D0%B7%D1%8B_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85

42. http://gendocs.ru/v24465/%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8_%D0%B2_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D1%85_%D0%B1%D0%B0%D0%B7%D0%B0%D1%85_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85

43. http://goo.gl/sswqDK

44. http://goo.gl/KXa8XX

45. http://goo.gl/3OGHaC

46. http://www.php.net/manual/ru/intro.pdo.php

47. http://vslovar.org.ru/comp/58.html

48. http://www.osp.ru/lan/2009/02/7155782/

49. http://goo.gl/hMhuhd

50. http://goo.gl/67nGzA

51. http://goo.gl/2mS2aI

52. http://goo.gl/GCQvJC

53. http://goo.gl/3kC9w1

54. http://goo.gl/egNdZy

55. http://goo.gl/QdCCGF

56. http://alife.narod.ru/lectures/bayes2003/Lecture_BayesNets.pdf

57. http://genie.sis.pitt.edu/

58. http://cito-web.yspu.org/link1/metod/theory/node10.html

59. http://cyberleninka.ru/article/n/klassifikatsiya-ugroz-v-sistemah-upravleniya-bazami-dannyh

60. http://rudocs.exdat.com/docs/index-424674.html?page=24

61. http://alife.narod.ru/lectures/bayes2003/Lecture_BayesNets.pdf

62. http://genie.sis.pitt.edu/

63. http://cito-web.yspu.org/link1/metod/theory/node10.html

64. http://emerecu.ukma.kiev.ua/books/InfSys/1/1-1-3.htm

ДОДАТОК А

КОД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

```
<?php
    function generateTempKey($id){

        $secret_code = 'kss_nnu';
        $time = time();

        $temp_key = md5($secret_code.$id.$time);

        return $temp_key;
    }

?>
<?php
    include ('functions.php');
    session_start();
    $user_key_access = $_GET['user_key_access'];

    $link = mysql_connect('localhost', 'root', '1111');
    mysql_select_db('db_dyplon');

    $query = mysql_query('SELECT * FROM `users`.`key_access`');

    while($res = mysql_fetch_array($query)){

        if($res['key_access'] == $user_key_access) $right = 1;
```

```
}

        if($right){

                $login = $_GET['login'];
                $password = $_GET['password'];

                $query = mysql_query('SELECT `id` FROM `users` WHERE
`login` = '$login' AND `password` = '$password");

                if($res = mysql_fetch_array($query)){
                        $_SESSION['temp_key'] = generateTempKey($res['id']);
                }
                else $error = 'Помилка авторизації';

        }
?>
<?php

        $R = $_GET['r'];

        $Z = $R / $R1;

        $Y = $R1 / $R2;

        $X = $R2;

?>
<?php
```

```
$temp_key = $_GET['temp_key'];

	if($temp_key == $_SESSION['temp_key']){
		$res = 'звязок встановлено';
	}
	else $res = 'помилка встановлення звязку';

?>

<?php
	include_once "defines.php";

	class conDisconToDB{
		/*
		*	properties
		*/
		public $DBH;

		/*
		*	methods
		*/
		function connectToDB (){
			try {
				$this->DBH = new PDO
('mysql:host='.HOST.';dbname='.NAME_DB, USER, PASSW_DB);
				return $this->DBH;
			}
			catch (PDOException $e){
				echo $e->getMessage();
```

```
                }
}
                        function closeConnectToDB(){
                $this->DBH = null;
            }
        }
?>
<?php
    include_once 'classConDisconToDB.php';

    class pageNavigator{

        private $con;
        private $count_row;
        private $DBH;
        private $num;
        private $page;
        private $STH;
        private $table;
        private $total;

        function __construct(){
            $this->con = new conDisconToDB();
        }

        function __get($propertyName){
            if( property_exists(__CLASS__, $propertyName)){
                return $this->$propertyName;
            }
            else return '0';
```

```
}

        function __set($propertyName, $value){
            if( property_exists(__CLASS__, $propertyName)){
                $this->$propertyName = $value;
            }
        }

        function countTotal(){
            $this->DBH = $this->con->connectToDB();
            $this->STH = $this->DBH->prepare('SELECT COUNT(*)
                                                AS count
                                                 FROM '.$this-
>table);
            $this->STH->execute();
            $this->STH->setFetchMode(PDO::FETCH_ASSOC);
            $this->count_row = $this->STH->fetch();
            $this->count_row = $this->count_row['count'];
            $this->total = intval(($this->count_row - 1) / $this->num) +
1;
                                    return $this->total;
        }

        function startNavi(){
            $this->countTotal();
            $this->total = intval($this->total);
            if($this->page > $this->total){
                $this->page = $this->total;
            }
            $start = $this->page * $this->num - $this->num;
```

```
return $start;
                }
        }
?>
<?php
        define ('HOST', 'localhost', true);
        define ('USER', 'root', true);
        define ('PASSW_DB', '1111', true);
        define ('NAME_DB', 'blog', true);
        define ('COUNT_NAVI', '10', true);



        date_default_timezone_set('Europe/Kiev');

?>
<?php
        include_once 'classConDisconToDB.php';
        include_once 'defines.php';

        class photo {
                /*
                *       properties
                */
                private $DBH;
                private $STH;
                private $res_array;
                private $num;
                private $res_categories;
                private $id_article;
                private $id_cat;
```

```
private $obj_con;
        private $start;
        private $dir_name = "img/authors/";



        /*
        *       methods
        */
        function __construct(){
                $this->obj_con = new conDisconToDB();
        }

        function __set($propertyName, $value){
                if( property_exists(__CLASS__, $propertyName)){
                        $this->$propertyName = $value;
                }
        }

        function fetchAllPhoto(){
                $this->res_array = scandir($this->dir_name);
                $this->res_array = array_diff($this->res_array, array('.',
'..'));
                                return $this->res_array;
        }

        function fetchResToArray(){
                $this->STH->setFetchMode(PDO::FETCH_ASSOC);
                while ($row = $this->STH->fetch()){
                        $this->res_array[] = $row;
                }
```

```
return $this->res_array;
                }



        }
?>
<?php
        class navi {

                private $addr_name;
                private $nextpage;
                private $page;
                private $page2left;
                private $page1left;
                private $page1right;
                private $page2right;
                private $prevpage;
                private $total;

                function __set($propertyName, $value){
                        if( property_exists(__CLASS__, $propertyName)){
                                $this->$propertyName = $value;
                        }
                }

                function createLinks(){
                        if ($this->page != 1) $this->prevpage = '<a href='.$this-
>addr_name.'/1/><<</a><a href='.$this->addr_name.'?/'. ($this->page - 1)
.'/><</a> ';
```

```
if ($this->page != $this->total) $this->nextpage =' <a href= '.$this-
>addr_name.'/'. ($this->page + 1) .'/>></a><a href='.$this->addr_name.'/'
.$this->total. '/>>></a>';
                        if($this->page - 2 > 0) $this->page2left = ' <a
href='.$this->addr_name.'/'. ($this->page - 2) .'/>'. ($this->page - 2) .'</a> | ';
                        if($this->page - 1 > 0) $this->page1left = ' <a
href='.$this->addr_name.'/'. ($this->page - 1) .'/>'. ($this->page - 1) .'</a> | ';
                        if($this->page + 2 <= $this->total) $this->page2right = ' |
<a href='.$this->addr_name.'/'. ($this->page + 2) .'/>'. ($this->page + 2)
.'</a>';
                        if($this->page + 1 <= $this->total) $this->page1right = ' |
<a href='.$this->addr_name.'/'. ($this->page + 1) .'/>'. ($this->page + 1)
.'</a>';

                        $result_navi = $this->prevpage.$this->page2left.$this-
>page1left.'<b>'.$this->page.'</b>'.$this->page1right.$this-
>page2right.$this->nextpage;
                        return $result_navi;
                }
        }
?>
<?php

        include_once 'classConDisconToDB.php';
        include_once 'classPageNavigator.php';

        class author{
                                private $author;
                private $DBH;
                private $num;
```

```
private $obj_con;
        private $res_array;
        private $start;
        private $STH;
        private $table;

        //////////////
        function __construct(){
            $this->obj_con = new conDisconToDB();
        }

        /*function __get($propertyName){

            if( property_exists(__CLASS__, $propertyName)){
                return $this->$propertyName;
            }
            else return '0';
        }*/

        function __set($propertyName, $value){
            if( property_exists(__CLASS__, $propertyName)){
                $this->$propertyName = $value;
            }
        }

        function fetchAll(){
            $this->DBH = $this->obj_con->connectToDB();
            $this->STH = $this->DBH->prepare('SELECT *

    FROM '.$this->table.'
```

```
                                                                LIMIT
'.$this->start.', '.$this->num);
                        $this->STH->execute();
                        $this->obj_con->closeConnectToDB();

                        return $this->fetchResArray();
                }
                function showAboutAuthor(){
                        $this->DBH = $this->obj_con->connectToDB();
                        $this->STH = $this->DBH->prepare('SELECT *
                                                        FROM `autors`
                                                          WHERE
`autors`.`id` = '.$this->author);
                        $this->STH->execute();
                        $this->obj_con->closeConnectToDB();

                        return $this->fetchResArray();
                }
                function fetchResArray(){
                        $this->STH->setFetchMode(PDO::FETCH_ASSOC);
                        while ($row = $this->STH->fetch()){
                                $this->res_array[] = $row;
                        }

                        return $this->res_array;
                }
        }
?>
```