**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**
**ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**
**КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розробка методики підвищення захищеності великих даних банківської системи на основі хмарних технологій»

на здобуття освітнього ступеня магістра
зі спеціальності 121 Інженерія програмного забезпечення
*(код, найменування спеціальності)*
освітньо-професійної програми «Інженерія програмного забезпечення»
*(назва)*

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*

_____ Марія ЮРЧЕНКО
*(підпис)*

Виконала: здобувачка вищої освіти групи ПДМ-62
Марія ЮРЧЕНКО

Керівник: Олена НЕГОДЕНКО
*к.т.н., доцент*

Рецензент: _____
*науковий ступінь, вчене звання* *Ім'я, ПРІЗВИЩЕ*

**Київ 2024**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут інформаційних технологій**

Кафедра Інженерії програмного забезпечення

Ступінь вищої освіти Магістр

Спеціальність 121 Інженерія програмного забезпечення

Освітньо-професійна програма «Інженерія програмного забезпечення»

**ЗАТВЕРДЖУЮ**
Завідувач кафедри
Інженерії програмного забезпечення
_____ Ірина ЗАМРІЙ
«_____» _____ 2023 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Юрченко Марії Юріївні

1. Тема кваліфікаційної роботи: «Розробка методики підвищення захищеності великих даних банківської системи на основі хмарних технологій»

керівник кваліфікаційної роботи Олена НЕГОДЕНКО к.т.н., доцент,

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023 р. №145.

2. Строк подання кваліфікаційної роботи «29» грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, модель хмарної піраміди, технології рівня Saas.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Проаналізувати застосування моделі хмарної піраміди.
2. Дослідити шляхи забезпечення високого рівня захищеності даних.
3. Розробити спосіб підвищення ступіню захищеності великих даних на основі впровадження хмарної піраміди.

5. Перелік графічного матеріалу: *презентація*

1. Порівняльний аналіз існуючих моделей захищеності даних в банківський сфері.
2. Основні принципи методу Saas.
3. Математична модель хмарної піраміди та методу Saas.
4. Оцінка критичних параметрів обмежень застосування методу SaaS для забезпечення безпеки великих даних.

6. Дата видачі завдання «19» жовтня 2023 р.

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Аналіз наявної науково-технічної літератури | 19.10-05.11.23 | |
| 2 | Вивчення матеріалів для аналізу застосування моделі хмарної піраміди | 06.11-12.11.23 | |
| 3 | Дослідження шляхів забезпечення високого рівня захищеності даних | 13.11-19.11.23 | |
| 4 | Аналіз рівня інформаційного ступіню захищеності великих даних в банку | 20.11-26.11.23 | |
| 5 | Впровадження способу підвищення ступіню захищеності великих даних на основі впровадження хмарної піраміди | 27.11-03.12.23 | |
| 6 | Розробка обов`язкових матеріалів | 04.12-10.12.23 | |
| 7 | Оформлення роботи: вступ, висновки, реферат | 11.12-20.12.23 | |
| 8 | Розробка демонстраційних матеріалів | 21.12-29.12.23 | |

Здобувачка вищої освіти _____ Марія ЮРЧЕНКО
*(підпис)*

Керівник
кваліфікаційної роботи _____ Олена НЕГОДЕНКО
*(підпис)*

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 85 стор., 6 табл., 5 рис., 23 джерел.

*Мета роботи* – підвищення ступіню захищеності великих даних банківської системи за рахунок застосування моделі хмарної піраміди та способу SaaS.

*Об'єкт дослідження* – захист інформаційного ступеню захищеності великих даних в банківській діяльності.

*Короткий зміст роботи*: У роботі проведено аналіз застосування моделі хмарної піраміди та методу SaaS для оцінки рівня інформаційної безпеки даних в банку. Проведено оцінку критичних параметрів, що стримують розвиток моделі хмарної піраміди для забезпечення інформаційної безпеки великих даних в банку. Розроблено методику підвищення захищеності великих даних на основі впровадження моделі хмарної піраміди та методу SaaS, яка дозволяє реалізувати інноваційні підходи до захисту конфіденційної інформації та оптимізації роботи з даними клієнтів. Проаналізовано результативність застосування моделі хмарної піраміди та методу SaaS для забезпечення високого рівня захищеності великих даних.

КЛЮЧОВІ СЛОВА: ВЕЛИКІ ДАНІ (BIG DATA), ІНФОРМАЦІЙНА БЕЗПЕКА, ХМАРНІ ОБЧИСЛЕННЯ, МОДЕЛЬ ХМАРНОЇ ПІРАМІДИ, ТЕХНОЛОГІЇ РІВНЯ «ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЯК ПОСЛУГА» (SAAS).

## ABSTRACT

Text part of the master's qualification work: 85 pages, 5 pictures, 6 tables, 23 sources.

The purpose of the work is to increase the degree of security of big data of the banking system due to the use of the cloud pyramid model and the SaaS method.

Object of research – protection of the information security level of big data in banking.

Subject of research – cloud technologies to increase the level of protection of big data in banking.

Summary of the work: The study of analysis of the application of the cloud pyramid model and the SaaS method was carried out to assess the level of information security of data in the bank. An assessment of the critical parameters restraining the development of the cloud pyramid model to ensure the information security of big data in the bank was carried out. A methodology for increasing the security of big data has been developed based on the implementation of the cloud pyramid model and the SaaS method, which allows implementing innovative approaches to protecting confidential information and optimizing work with customer data. The effectiveness of using the cloud pyramid model and the SaaS method to ensure a high level of big data security is analyzed.



KEYWORDS: BIG DATA, INFORMATION SECURITY, CLOUD COMPUTING, CLOUD PYRAMID MODEL, SOFTWARE AS A SERVICE (SAAS) TECHNOLOGIES.

**ЗМІСТ**

# ВСТУП

В даний час, на тлі світу, що швидко змінюється, етап розвитку банківської системи протікає в умовах жорсткої конкуренції і кризових явищ на фінансових ринках. Одним з основних чинників успішного розвитку банківської діяльності є впровадження та реалізація нововведень, які є основою стабільності, конкурентоспроможності та сталого економічного зростання банків. Саме з цієї причини стало актуальним питання вивчення великих даних у банківській індустрії.

Великі дані (Big Data) – напрямок, пов'язаний з обробкою та зберіганням великого обсягу інформації, з яким дуже важко працювати за допомогою звичайних програмних пристроїв та неможливо проаналізувати за допомогою людської праці.

На сьогоднішній день великі дані (Big Data) є рушієм розвитку інформаційних технологій та найшвидшою сферою [3, с. 188], оскільки кількість інформації постійно зростає, тому актуальність теми дуже велика.

Завданням дослідницької роботи є визначення практичної значущості застосування технологій великих даних та розгляд перспективи поширення даних технологій у банківській сфері.

Оскільки банківський сектор є одним із найбільш клієнтоорієнтованих, то можна сказати, що дана сфера найбільше зацікавлена у застосуванні даної технології, оскільки банки щодня отримують величезний обсяг інформації, і в більшості випадків ці отримані дані хаотичні і неструктуровані, і саме тому , банки з великим бажанням прагнуть ефективно використовувати Великі дані (Big Data), щоб мінімізувати ризики та оперативно боротися з шахрайством.

В сучасних банках існують загальні вимоги щодо захисту інформації, а саме:

- прогнозування та оперативне виявлення з наслідком усунення інформаційних загроз захищеності персоналу та ресурсам банку;
- інтеграція інформаційних засобів аналіз причин і умов, які потенційно або явно наносять різного роду збиток банку, що призводить до порушення його приватного функціонування;

- класифікація конфіденційної інформації до категорій обмеженого доступу (банківської та комерційної таємниць, платіжних та особистих даних клієнтів і співробітників банківських організацій) та оцінка критеріїв їх уразливості;
- забезпечення інформаційних засобів оперативного реагування на ідентифіковані загрози захищеності на локальному або глобальному рівнях і контроль проявів негативних тенденцій у функціональній діяльності банку;
- ефективне та своєчасне блокування інформаційних загроз персоналу;
- створення умов для мінімізації ризиків нанесеного збитку при проведенні неправомерних дій та ослаблення негативного впливу внаслідок порушення інформаційного ступіню захищеності на виконання операційних і стратегічних завдань банку.

В даний час інформаційні загрози в банках (і не тільки) виявляються у наступних формах:

- розміщення різної конфіденційної фінансової інформації про клієнтів або інфраструктуру банку;
- витоки секретної інформації за допомогою використання технічних засобів забезпечення діяльності співробітників банку;
- несанкціонований доступ до конфіденційної інформації та інших ресурсів банку, які охороняються законом, зі сторони конкурентів і зловмисників.

Основними джерелами загроз інформаційній безпеці (ІБ) є:

- несприятливі події природного, техногенного та соціального характеру;
- терористи та кримінальні елементи;
- залежність від постачальників/провайдерів/партнерів/клієнтів;
- збої, відмови, пошкодження програмних та технічних засобів;
- працівники, які реалізують загрози ІБ з використанням легально наданих їм прав та повноважень;

- зовнішні порушники ІБ;
- невідповідність вимогам наглядових та регулюючих органів, чинному законодавству.

Реалізація несанкціонованого доступу до інформаційних ресурсів на практиці, згідно з наявним досвідом сучасних банківських компаній, часто проводиться шляхом організації зловмисниками наступних дій:

- хакерського доступу, копіювання та зміни важливої банківської інформації;
- перехоплення інформаційних потоків та пакетів, що рухаються в системах зв'язку та обчислювальної техніки за допомогою апаратно-технічних засобів знімання інформації.

Захист інформаційних ресурсів банку повинен передбачати:

- обгрунтованість будь-якого доступу ресурсів, тобто. кожен співробітник чи користувач має відповідну власну форму допуску до роботи з інформацією, реалізовану певному рівні конфіденційності;
- персональну відповідальність, яка виявляється у тому, що співробітник чи користувач несе відповідальність за збереження даних, інформації та за свої дії в ІБ;
- надійність зберігання даних, тобто. інтеграції умов, що виключають можливі способи несанкціонованого доступу до інформації;
- контроль та попередження передачі критичної конфіденційної інформації щодо існуючих незахищених ліній передачі даних;
- цілісність інформаційного програмного середовища, що забезпечується фізичною безпекою засобів інформатизації, оновлення програмного операційного середовища з усуненням можливих потенційних місць злому.

Таким чином, необхідно зазначити, що стратегія інформаційного ступіню захищеності банків дуже відрізняється від аналогічних стратегій інших компаній та організацій. Це обумовлено, перш за все, специфічним характером загроз, а також публічною діяльністю банків, які змушені робити доступ до рахунків досить

легким для зручності для клієнтів.

Звичайна компанія будує свою інформаційну безпеку, виходячи лише з вузького кола потенційних загроз - головним чином захист інформації від конкурентних організацій та комерційних структур. Така інформація цікава лише вузькому колу зацікавлених осіб та організацій і рідко буває ліквідна, тобто перетворюється на грошову форму.

Інформаційна безпека банку (на відміну більшості існуючих компаній) має забезпечувати максимально можливу надійність роботи ІБ, зокрема у разі позаштатних ситуацій, т.к. банк несе всю відповідальність власним коштом, а й кошти своїх клієнтів.

Головними складовими структури інформаційної системи банку є:

- Інформаційне забезпечення. Являє собою сукупність всієї інформації, що зберігається в банку (системи різних фінансових показників, спосіби кодування інформації та документів, бази даних і бази знань).
- Функціональне забезпечення. Необхідно на формування змістовної спрямованості ІС, реалізується у вигляді низки операцій та функцій.
- Технологічне забезпечення виявляється у вигляді сукупності проектних рішень. Необхідно визначення технології створення технологічних умов задля забезпечення коректного виконання банківських операцій у автоматичному режимі. Даний тип забезпечення поєднує інформаційне та функціональне. Базовим елементом виступає зовнішня подія, у разі реакції ініціюється виконання низки технологічних операцій, певним чином взаємопов'язаних.
- Програмне забезпечення. Полягає в інтеграції операційних систем із розгорнутими системами управління базами даних та модулями реалізації програмних інтерфейсів.
- Апаратні засоби. Як правило, це засоби обчислювальної техніки, обладнання локальних та глобальних обчислювальних мереж, засоби зв'язку, платіжні термінали та банкомати.

Для автоматизації процесів моніторингу та управління подіями інформаційного ступіню захищеності (ІБ) банків та інших фінансових організацій нині керівництво провідних відділів ІБ сучасних компаній часто приймає рішення про впровадження спеціалізованих систем, спрямованих на забезпечення оперативного моніторингу подій, їх подальшу обробку, аналіз та виявлення інцидентів з ранжуванням пріоритетів та ризиків.

Процедура моніторингу ІБ банків проводитиметься шляхом реалізації наступних етапів:

- ідентифікація дій та операцій, що підлягають реєстрації;
- визначення змісту даних про дії та операції, що підлягають реєстрації, визначити терміни їх зберігання;
- організація резервування обсягу пам'яті до виконання запису даних;
- забезпечення оперативної реакції на збої при реєстрації дій та операцій, таких як програмні та апаратні помилки;
- формування генерації часових міток для виконання реєструючих дій із синхронізації системного часу на використовуваних технічних засобах моніторингу ІБ.

На практиці до таких систем автоматизації моніторингу та управління подіями (МУП) висуваються наступні вимоги:

- забезпечення аналізу різних інцидентів та подій ІБ у режимі онлайн;
- автоматизація всіх процесів, спрямованих на виявлення причин виникнення критичних ситуацій, інцидентів та ризиків;
- оптимізація виробничих операцій, що виконуються фахівцями із забезпечення моніторингу стану ІБ на підприємстві чи організації;
- мінімізація різних фінансових та тимчасових витрат з отримання, зберігання, структуризації та класифікації, аналізу та оцінки виявлених інцидентів;
- оптимізація існуючих рутинних операційних завдань, які мають на меті забезпечення оцінки ефективності вживаних заходів з ІБ.

Сучасні системи МУП ІБ типу SIEM (Security Information and Event

Management) у результаті повинні забезпечувати комплексний підхід до вирішення основних функціональних завдань, найбільш пріоритетними з яких є:

- автоматизований збір та структурування відповідної інформації;
- оперативний аналіз небажаних зовнішніх і внутрішніх факторів, що впливають;
- контроль подій, інформація про які надходить від інтегрованих засобів захисту.

МУПС ІБ типу SIEM, зокрема, допомагає вирішити такі пріоритетні для банківської сфери завдання:

- координація всього обсягу подій ІБ;
- забезпечення візуалізації процесів, що відбуваються, та оцінки стабільності ситуації ІБ в цілому в рамках функціонування інформаційної системи;
- оцінка поточного рівня захищеності шляхом розрахунку показників ефективності (KPI);
- оперативне і точне виявлення інцидентів, що з'явилися в ІБ;
- забезпечення отримання достовірних даних для ідентифікації, аналізу та оцінки відповідних фінансових та матеріальних ризиків;
- підтримка прийняття керуючих рішень, спрямованих на підвищення рівня захищеності функціонування всієї інформаційної інфраструктури банку;
- забезпечення дотримання та виконання відповідних законодавчих вимог та актів у сфері виконання моніторингу подій ІБ.

В сучасних умовах банки генерують великий обсяг критично важливих даних, таких як особиста інформація, комерційні дані та багато інших. Згодом обсяг створених цифрових даних поглинає можливості зберігання даних банків. Саме по цій причині створити необхідну інфраструктуру, таку як перевірка систем зберігання даних великої ємності. Величезна кількість додатків, що використовуються в хмарі, можуть бути використані для збереження великих даних, і одночасно можуть розглядатися як сукупність наборів даних, які є

складними, що затруднює збір, зберігання, аналіз та візуалізацію інформації внаслідок використання застарілих систем. Щоб керівництво банку могло ефективно керувати центрами обробки даних та хмарними системами, оператори повинні спрямувати свої зусилля на створення програм та додатків для збереження великих даних. Все вищезазначене визначає **актуальність обраної тематики.**

**Аналіз останніх досліджень і публікацій.** Питання застосування хмарних технологій в банку розглядалися різними дослідниками. Б. С. Тріпаті, Р. Гупта підкреслювали, що розвиток і впровадження нових інформаційно-комунікаційних технологій вимагає застосування системного підходу та проведення наукових теоретико-правових досліджень з метою забезпечення ефективного правового регулювання суспільних відносин, що виникають в процесі впровадження інформаційних технологій в банківській діяльності [4, с. 762; 19, с. 173].

Л. Ванг, С. С. Чен відзначали, що хмарна інфраструктура – це сукупність динамічно розподілених та налаштованих хмарних ресурсів, які можуть бути оперативно надані користувачу хмарних послуг, а потім вивільнені засобами глобальної та локальної мереж передачі даних [20, с. 184].

С. Янгуй визначав, що суттєвий вплив на більшість сегментів галузі індустрії інформаційних технологій пов`язаний із тенденцією переходу до хмарних обчислень для контролю даних в процесі реалізації банківських послуг. Навіть наявність значної уваги до обраної проблематики не призвела до розробки єдиної відмовостійкої хмарної моделі, що забезпечила б високий рівень надійності даних клієнтів банку. Завдяки такій моделі можливо формування передумов, які б дозволили виконувати подальші дослідження [21, с. 254].

**Мета і завдання дослідження.** Метою дослідження є підвищення ступіню захищеності великих даних банківської системи за рахунок застосування моделі хмарної піраміди та способу SaaS. Для реалізації вказаної мети необхідно реалізувати ряд завдань:

- розглянути сутність поняття, роль та функції застосування системи інформаційного ступіню захищеності, яка б зберігала Великі дані (Big Data) в банку;

- провести аналіз застосування моделі хмарної піраміди та способу SaaS з метиою оцінки рівня інформаційного ступіню захищеності даних в банку;
- організувати сприяння технічним регламентам і стандартизації банківської інформаційної системи, створити та вдосконалити впровадження відповідних механізмів моніторингу, формування умов захищеності інформаційних систем;
- посилити технічне обслуговування інформаційних систем і управління повсякденними операціями, а також забезпечити створення та вдосконалення документації операційних процесів і стандартизації для забезпечення цілісності та доступності інформації;
- створити централізований центр моніторингу шляхом збирання та подальшого керування всією інформацію, щоб у будь-який час контролювати роботу всієї банківської мережі, системи та умови роботи, щоб виявити проблеми, а потім контролювати процес їх вирішення;
- забезпечити комплексне використання високотехнологічних засобів у банку;
- посилити потенціал запобігання ризикам і контролю для боротьби з фінансовими злочинами в мережі, щоб забезпечити безпечну та безперебійну роботу мережевої системи в банку;
- зміцнити інфраструктуру банківського центру та резервного центру обробки даних, а також забезпечити доступність систем резервного копіювання, що дозволяє зменшити або взагалі уникнути ризиків втрати великих даних;
- підвищити обізнаність керівництва та персоналу щодо формування системи інформаційного ступіню захищеності.

**Об`єкт і предмет дослідження. Об`єктом дослідження** є захист інформаційного ступіню захищеності великих даних в процесі банківської діяльності.

**Предметом дослідження** є хмарні технології, які дозволяють підвищити рівень захисту великих даних в банківській діяльності.

**Спосіби дослідження.** Для написання роботи використано аналіз даних, порівняльний і системний спосіб, та математичне моделювання.

**Наукова новизна одержаних результатів.** Вперше розроблено спосібику підвищення ступіню захищеності великих даних в банку на основі впровадження моделі хмарної піраміди та способу SaaS та визначено економічну ефективність їх застосування.

**Практичне значення одержаних результатів.** Результати дослідження можуть бути застосовані у практиці діяльності банків, а також для застосування моделі хмарної піраміди та способу SaaS з метою підвищення рівня захисту великих даних.

# 1 ДОСЛІДЖЕННЯ ШЛЯХІВ ЗАБЕЗПЕЧЕННЯ ВИСОКОГО РІВНЯ ЗАХИЩЕНОСТІ ВЕЛИКИХ ДАНИХ В БАНКУ

## 1.1 Сутність поняття, роль та функції застосування системи інформаційного захисту великих даних в банку

Наразі не існує єдиного визначення великих даних. Цей термін використовується для опису величезних масивів даних [7, с. 21]. Він використовується для позначення великих та/або складних масивів даних і відповідних технологій їх зберігання та обробки. Ці масиви даних можуть мати як структуровану форму (зовнішні та внутрішні бази даних), так і неструктуровану (інформція в соціальних мережах, газетах та журналах тощо). Фінансові установи щодня створюють мільярди байтів даних в результаті проведення щоденних транзакцій, відображення в журналах облікових записів користувачів, здійснення оновлення даних, реалізації модифікацій облікових записів.

Великі дані (Big Data) – це значний обсяг інформаційних активів, які вимагають застосування економічно ефективних інноваційних форм обробки інформації. Такі активи забезпечують покращене розуміння, прийняття рішень та автоматизацію процесів обробки. Визначення великих даних передбачає наявність трьох основних критеріїв: обсягу, швидкості та різноманітності, причому:

– обсяг означає використання даних з різних джерел;

– швидкість означає співвідношення довжини шляху отримання, збору та аналізу даних на одиницю часу;

– різноманітність стосується різних типів використовуваних даних, як структурованих, так і неструктурованих.

Існують різні типи великих даних, серед яких виокремлюють:

– інформацію з соціальних мереж, блогів та публікацій в Інтернеті;

– дані про діяльність в Інтернеті, включаючи пошукові запити користувачів і дані про відвідані сайти;

– інформацію з традиційних бізнес-процесів (інформацію про транзакції, замовлення, платежі, реєстрацію клієнтів, банківські операції тощо);

– дані громадських організацій (адміністративні дані, включаючи митні, податкові, медичні дані тощо);

– інформацію з мобільних та інших пристроїв (геолокаційні дані, обсяг трафіку, дані систем розумного дому, камер відеоспостереження, датчиків, трекерів та інших приладів).

Великі дані (Big Data) разом із технологіями їх обробки створюють ряд важливих переваг для фінансових організацій, такі як:

– висока швидкість обробки величезних обсягів інформації є однією з найважливіших переваг технологій великих даних, що дозволяє покращити різні аспекти діяльності фінансових установ;

– суттєво поліпшується якість управління ризиками здатності аналізувати істотні обсяги даних, включаючи неструктуровані зовнішні дані, які раніше не враховувалися;

– клієнти отримують більш якісні фінансові послуги.

Таким чином, технології захисту великих даних дозволяють значно відвищити рівень інформаційного ступіню захищеності даних клієнтів [1, с. 37]. З точки зору фінансової стабільності, використання великих даних може зменшити небезпеку втрати даних за рахунок покращення якості управління ризиками та формування довгострокових взаємовідносин з клієнтами банку.

Застосування великих даних призводить до виникнення ряду ризиків, які впливають на процедуру обробки інформації [2, с. 1690]. Слід зазначити, що «використання зовнішніх даних, пов`язаних з розпізнаванням тексту та аналізом зв`язків шляхом обробки неструктурованої інформації у ЗМІ, соціальних мережах та інших джерелах, потребує застосування нових автоматизованих підходів до управління якістю даних. Це дозволить виявити спотворення фактів або виявлення дезінформації. Щоб підвищити рівень повноти та якості великих зовнішніх даних, вкрай важливо використовувати незалежні джерел. Цей крок передбачає формування потреби в нових знаннях і вдосконаленні наявних знань про хмарні

сервіси, покращуючи існуючі знання, використовуючи нові знання, створені для роботи з бездротовими мережами, забезпечуючи зв`язок між хмарами та периферійними пристроями за допомогою штучного інтелекту.

Ще одна проблема полягає в наявності модельного ризику під час побудови моделей на основі великих даних: використання помилкових вхідних даних або припущень, застосування моделі з неналежною метою або помилки в розробці самої моделі. У зв`язку з цим важливим є питання кваліфікації співробітників, які аналізують Великі дані (Big Data). На рівні оператора мають розглядатися виключно початкові дані [23, с. 183].

Недостатнє розуміння функціонування різних форм аналітики великих даних може призвести до матеріалізації відповідного ризику. Топ-менеджмент банку також повинен мати достатні знання, щоб розуміти результати моделювання щодо виконання завдань, для вирішення яких використовуються ці моделі. Матеріалізація модельного ризику може призвести до таких несприятливих наслідків, як системно некоректна оцінка ризику під час використання великих даних в процесі управління ризиками. Внаслідок цього в процесі проведення кредитного скорингу платоспроможність клієнта може бути оцінена неправильно, і такі помилки можуть регулярно повторюватися, що призведе до накопичення кредитних ризиків у банківському секторі, які негативно вплинуть на показники ефективності діяльності банку.

Під час використання великих даних для клієнтів банків існують ризики, які пов`язані із захистом персональних даних. В першу чергу ризики пов’язані зі збором даних щодо клієнтів банків. З одного боку, це допомагає підвищити якість фінансових послуг, оскільки вони стануть персоналізованими. З іншого боку, зростають ризики неналежного використання персональних даних, що в свою чергу викликає необхідність їх захисту. Наприклад, до категорії конфіденційних відносяться фінансові дані та дані щодо здоров`я фізичних осіб.

Зловживання доступом до даних призводить до втрати довіри клієнтів [22, с. 345]. У той же час люди часто поширюють власну конфіденційну інформацію, в тому числі в соціальних мережах, не розуміючи в повній мірі важливість цієї

інформації та наслідків, які можуть виникнути внаслідок несакціонованого використання персональних даних.

Великі дані (Big Data) надають змогу більш точно оцінити потреби кожного окремого споживача, а також дозволяють фінансовим установам оцінити готовність кожного клієнтів сплатити певну ціну за послугу, що потенційно може призвести до цінової дискримінації. Така ситуація призводить до зменшення споживчого надлишку, особливо якщо клієнт потребує своєчасної послуги і не проаналізував ціни на ринку заздалегідь, або не має схильності до такого аналізу.

На основі аналізу IP-адрес пристроїв, які покупці використовують для доступу до Інтернету, і даних про геолокацію, постачальники фінансових послуг можуть відстежити, в якому районі живе покупець, і запропонувати більш сприятливу ціну. Одним із наслідків відсутності прозорості чи інтерпретованості способів обробки великих даних є можливі прояви нецінової дискримінації.

Іноді дискримінація вважається ненавмисною [3, с. 211]. Оскільки різні групи людей мають присутні їм особливості поведінки, слід зазначити, що в даному випадку причина полягає у використанні моделей штучного інтелекту, заснованих переважно на використанні нейронних мереж. Однак, Великі дані (Big Data) можна аналізувати не тільки за допомогою таких способів, але й шляхом використання звичайних статистичних (економетричних) способів. Хоча в цьому випадку модельний ризик також присутній, моделі є набагато прозорішими та зручнішими для інтерпретації, оскільки вони демонструють усі фактори, що впливають на результати досліджень.

Моделі нейронних мереж вважаються найбільш перспективним способом роботи з великими даними з точки зору швидкості та повноти результатів, в тому числі в Інтернеті, в соціальних мережах, в процесі онлайн-покупок, а модель недостатньо високої якості може надати результат, що вказує на нижчий рівень кредитоспроможності позичальника, ніж є в реальності, в результаті недооцінки особливостей поведінки різних груп населення. Таким чином, моделі великих даних можуть бути неточними та упередженими щодо різних груп позичальників.

Нецінова дискримінація може бути навмисною з боку фінансової установи, через непрозорість способів роботи з великими даними. Ще одним викликом є збільшення кількості ризиків для фінансових установ, які відстають у впровадженні технологій великих даних.

Великі дані (Big Data) успішно використовуються низкою фінансових установ для моніторингу та запобігання матеріалізації операційних ризиків, включаючи кіберризики та ризики протидії відмиванню коштів та фінансуванню тероризму.

Ю. Ерік вважав, що інформаційна безпека дозволяє підтримати безпечні умови життєдіяльності [3, с. 212]. М. С. Делгоша, Ю. Ван сформулювали визначення інформаційного ступіню захищеності як сукупності відносин, що регулюють обробку інформації [5, с. 2500]. На думку М. Хасана під інформаційної безпекою слід розуміти поєднання трьох елементів: захист інформації, захист і контроль інформаційного простору, забезпечення належного рівня інформаційної достатності [7, с. 21]. Незважаючи на наявність значної уваги до обраної проблематики, не було створено єдиної надійної системи захищеності даних клієнтів банку, що створює передумови для продовження проведення досліджень з обраної проблематики.

Система інформаційного ступіню захищеності великих даних банку формується шляхом застосування сукупності заходів забезпечення захисту таємності, цілісності, зручності використання, контрольованості та незаперечності інформації. Ця система містить інформаційне середовище, інформаційну мережу, механізм роботи інформаційного додатку та інші компоненти.

Механізм реалізації інформаційного ступіню захищеності великих даних в банку передбачає шифрування ключового поля з подальшим його переміщенням в сховище полів. Це забезпечить дійсність зміни даних та дозволить уникнути неліцензійних змін даних. Для керування повноваженнями формуються відповідні рівні із визначеннями повноважень для користувачів [12, с. 3]. Коли процес подання заявки на обробку даних запущено, слід використати спосіб підпису для ідентифікації оператора та відповідно до дозволів контролювати його права.

Відповідно до питань забезпечення захищеності мережі банки використовують маршрутизатори та брандмауери для створення відносно потужної технології захищеності мережі.

Побудова інформаційного ступіню захищеності банку є поєднанням процесів планування, управління технічною системою, та являє собою безперервний процес динамічного розвитку захисту великих банківських даних. Ці два аспекти є взаємозалежними.

Системи комп'ютерної мережі в банку повинні використовувати передові технології мережевої захищеності. Відповідні технічні засоби включають контроль доступу, шифрування та захист цілісності даних, ідентифікацію та автентифікацію, застосування мережевої антивірусної технології, брандмауерів, здійснення резервного копіювання та відновлення даних, а також проведення контролю над відстеженням даних клієнтів банку.

У прикладних системах відбуваються авторизовані операції або створюється таблиця визначення транзакцій, встановлюються багаторівневі дозволи, які надаються операторам різного рівня. Після того, як сервер перевірить особу користувача, буде визначено права користувача у вигляді інформації щодо контролю повноважень. Оператор на всіх рівнях системи може працювати лише в межах своїх професійних обов'язків. Для шифрування даних застосовується наскрізне шифрування [9, с. 151].

У той час як для Інтернет-банкінгу пакети даних під час онлайн-передачі базуються на структурі даних транзакції та MAC-компонентах коду автентифікації повідомлення хеш-алгоритму, отримувач отримує перевірку MAC-адреси і може виявити випадкову або навмисну помилку передачі даних, модифіковану для захисту цілісності та конфіденційності передачі даних.

Автентифікація джерела даних є засобом ідентифікації інформації та здійснюється за допомогою технології цифрового підпису. В той самий час завдяки використанню технології цифрового підпису можна досягти захисту від відмови від автентифікації. Мережева антивірусна технологія дозволяє виявляти і видаляти комп'ютерні віруси. Це дозволяє запобігти проникненню вірусу в комп`ютерну

систему банку та спричинити знищення великих даних. Антивірусна технологія повинна поєднувати всі ці технології разом, щоб сформувати багаторівневу систему захисту.

У мережі банку та інших мережах брандмауер створює перешкоди для запобігання незаконному доступу до інформації, а також може захистити банківську мережу від несанкціонованої передачі інформації. Моніторинг виявлення великих даних стосується процесу надання доступу до системи за допомогою різноманітних технічних засобів для моніторингу поведінки, отримання доступу та виявлення даних, щоб забезпечити безпеку процесу доступу суб`єкта до даних.

Журнали аудиту застосовуються для відстеження системи дій користувачів і додатків, щоб покращити можливість перевірки системи інформаційного ступіню захищеності великих даних в банку. Записи зберігаються у файлі журналу та пов`язаній базі даних. Резервне копіювання та відновлення є заходами захищеності, які забезпечуються функціонуванням технічних засобів, що максимально захищають техніку від кібератак.

Стандартизацію системи управління інформаційною безпекою банку розподіляють на макро- та мікрорівень [4, с. 763]. Макрорівень головним чином стосується наукової розробки політик захищеності, він зменшує зони ризику за допомогою застосування стандартизованої інформаційної системи. Мікрорівень полягає в розумному плануванні на стадії розробки системи, попередньо зменшивши або усунувши вразливість системи за допомогою застосування сучасних інформаційних технологій.

Система інформаційного ступіню захищеності великих даних в банку реалізує наступні функції:

– сприяння технічним регламентам і стандартизації банківської інформаційної системи, створення та вдосконалення відповідних механізмів моніторингу, формування умов захищеності інформаційних систем, оскільки остаточним рішенням, на яке можна покластися, є правовий захист даних;

– поліпшення технічного обслуговування інформаційних систем і управління повсякденними операціями, а також забезпечення поступового створення та вдосконалення документації операційних процесів і стандартизації для забезпечення цілісності та доступності інформації;

– створення централізованого центру моніторингу, який буде збирати всю інформацію та керувати нею, щоб у будь-який час контролювати функціонування всієї банківської мережі, системи та умови роботи, щоб виявити проблеми, а потім контролювати процес їх вирішення;

– забезпечення комплексного використання різноманітних високотехнологічних засобів у банку;

– посилення стійкості потенціалу запобігання ризикам і контролю для боротьби з фінансовими злочинами мережі для забезпечення безпечної та безперебійної роботи мережевої системи в банку;

– зміцнення інфраструктури банківського центру та резервного центру обробки даних, а також забезпечення доступності систем резервного копіювання, щоб зменшити та уникнути ризиків втрати великих даних;

– підвищення обізнаності керівництва та персоналу щодо формування системи інформаційного ступіню захищеності.

Отже, в управлінні банком система інформаційного ступіню захищеності великих даних повинна суворо контролюватися. Система інформаційного ступіню захищеності великих даних в банку повинна застосовуватися для вирішення існуючих проблем інформаційного ступіню захищеності та постійно вдосконалювати систему захищеності мережі в банку за допомогою залучення нових технологій.

## 1.2 Аналіз застосування моделі хмарної піраміди та способу SaaS для оцінки рівня інформаційного захисту даних в банку

Ресурси управління банківськими даними використовуються для розробки рішень, які забезпечують доступність даних, міграцію, реплікацію та інтеграцію. Виконавча система управління використовується для виконання завдань шляхом максимального використання наявних обчислювальних ресурсів. Крім того, він використовується для відстеження ходу виконання завдання та обробки результатів обчислень. З іншого боку, хмарні обчислення часто використовуються для надання ресурсів через хмару. Хмарне програмне забезпечення – це спосіб надання різних фракцій залежно від типу наданого хмарного сервісу, який використовується для підтримки поточних знань про доступні обчислювальні ресурси та створення та керування віртуальними технологіями у відповідь на запити користувачів.

Застосування хмарних технологій у банках розглядали різні дослідники. Б. С. Тріпаті, Р. Гупта підкреслювали, що розробка та впровадження нових інформаційно-комунікаційних технологій має відбуватися систематично [4, с. 762; 19, стор. 173].

Л. Ван, С. С. Чен відмічали, що хмарна інфраструктура дозволяє об’єднувати хмарні ресурси, що надаються користувачеві [20, с. 184]. С. Янгі визначив, що значний вплив на більшість сегментів індустрії інформаційних технологій пов’язаної із застосуванням хмарних технологій [21, с. 254]. Проте наявність значної уваги до вибраного питання не призвела до розробки єдиної надійної хмарної моделі, яка б забезпечувала високий рівень достовірності даних клієнтів банку, що створює передумови для продовження досліджень у майбутньому.

Хмарне програмне забезпечення може допомогти з впровадженням, конфігурацією та розгортанням додатків, а також забезпечити ціноутворення, облік та адміністрування для клієнтів банку. Ефективне використання обчислювальних послуг передбачає прийоми та правила, які визначають, де мають створюватися віртуальні технології, а також коли їх слід запускати та зупиняти на основі уподобань користувача.

Хмарний контроль є простим у використанні, оскільки він вбудовується у систему адміністрування [10, с. 17]. Технологія хмарних обчислень є високоефективним ресурсом, доступним для величезної кількості користувачів і широко використовується в усьому світі, включаючи абстрактні межі, масштабованість і неоднозначність розташування, які є наслідком природи справжньої хмари. Хмара містить численні інформаційні технології, а технологічний розвиток призводить до зростання та розвитку хмари.

Хмарні обчислення – це технологія, яка забезпечує всеохоплюючу, просту мережеву роботу за вимогою користувачів системи. Це збільшує доступ до загальної кількості конфігурацій обчислювальних ресурсів, таких як сервери, додатки, мережі та служби, прискорюючи процес ініціалізації та зменшуючи робоче навантаження постачальників послуг під час залучення нових клієнтів.

Хмарні обчислення дозволяють поєднати традиційні та новітні обчислювальні спосіби [5, с. 2500]. Мета розподіленого обчислення полягає в тому, щоб розділити обчислення на керовані частини, після чого кілька різних користувачів комп`ютерів призначаються для аналізу та збору всіх результатів. Паралельні обчислення вирішують проблеми, які потребують високої обчислювальної ефективності. Вони об`єднують значні ресурси для обчислення та оцінки результатів виконання певного завдання.

Модель хмарної піраміди – це бізнес-модель, у якій послуги надаються від імені клієнтів на апаратному забезпеченні, яким клієнти не володіють і не керують ним. IT- та бізнес-ресурси в хмарних обчисленнях слід динамічно надавати відповідно до потреб користувачів і робочого навантаження системи. Такі ресурси включають сервери, сховище, мережу, програми та процеси. Хмарні обчислення дозволяють кінцевому користувачеві запускати програмні додатки та отримувати доступ до даних у будь-якому місці та з будь-якого комп`ютера. Користувачеві не потрібно будь-коли встановлювати, оновлювати та усувати технічні проблеми програмного забезпечення фізично на локальному робочому столі чи сервері.

Стек хмарних технологій складається із трьох частин, кожна з яких представляє окрему категорію сервісів. На верхньому рівні розташовується SaaS -

по суті, це хмарні програми, доступ до яких надається через веб-інтерфейс. За ним слідує PaaS-платформа для самостійної розробки та розгортання додатків.

На третьому рівні розташувався IaaS - сервери, сховища, мережі, обчислювальна інфраструктура, яку клієнт отримує у користування для запуску своїх рішень.

Модель хмарної піраміди реалізується на трьох рівнях: нижній рівень «Інфраструктура як послуга» (IaaS), середній рівень «Платформа як послуга» (PaaS), верхній рівень «Програмне забезпечення як послуга» (SaaS), див. табл. 1.1.

Таблиця 1.1

Порівняння хмарної піраміди

| Характеристика | IaaS (Infrastructure as a Service) | PaaS (Platform as a Service) | SaaS (Software as a Service) |
|---|---|---|---|
| Рівень Контролю | Високий | Середній | Низький |
| Основний Фокус | Інфраструктура | Розробка додатків | Готовий продукт |
| Управління Операційною Системою | Користувач | Платформа | Постачальник послуг |
| Управління Додатками | Користувач | Користувач | Постачальник послуг |
| Масштабованість | Висока | Висока | Стандартизована |
| Час Впровадження | Середній | Низький | Низький |
| Витрати | Високі | Середні | Низькі |
| Захищеність Даних | Залежить від Користувача | Залежить від Користувача | Обов'язок Постачальника |
| Доступ та Оновлення | Вимагає наявності ПО; користувач відповідає за оновлення | Надаються засоби для розробки та деплойменту; користувач відповідає за розробку | Доступ лише через Інтернет; автоматичні оновлення та немає необхідності в ручних втручаннях користувача |
| Легкість Використання | Вимагає інсталяції та конфігурації; може знадобитися управління операційною системою | Спрощений процес розробки; вимагає налаштування та деплойменту додатку | Простий доступ через браузер; немає необхідності встановлення; |

Продовження таблиці 1.1

Порівняння хмарної піраміди

| Характеристика | IaaS (Infrastructure as a Service) | PaaS (Platform as a Service) | SaaS (Software as a Service) |
|---|---|---|---|
| Відповідальність за Інфраструктуру | Користувач | Постачальник послуг | Постачальник послуг |
| Відповідальність за Оновлення | Користувач | Користувач | Постачальник послуг |
| Відповідальність за Захищеність Даних | Користувач | Користувач | Постачальник послуг |
| Відп. за Центр Обробки Даних | Користувач | Користувач | Постачальник послуг |
| Автоматизація Організації | Висока | Середня | Висока |

Кожен рівень має свій функціонал. Архітектура рівня функціонує таким чином, що вищий рівень може бути сформований на основі послуг нижчого рівня. Сервісна модель — це хмарний продукт, де споживач платить за все, що він використовує. Однією з переваг цих моделей обслуговування є те, що початкові витрати зазвичай нижчі. Завдяки цьому забезпечується більш високий рівень масштабованості. Кожен рівень служби забезпечує абстракцію та автоматизацію встановлення, керування сервером, розгортання програмного забезпечення, безпеки та інших операцій. Сервісні моделі дозволяють споживачам хмарних обчислень більше зосередитися на своєму основному бізнесі, а не на хмарній інфраструктурі. Середовище розробки дозволяє розширити можливості користувачів [6, с. 270]. Окрім послуг інфраструктури, було створено середовище розробки, яке пропонує можливості розробки та розгортання додатків.

Можливості хмарних обчислень використовуються для надання користувачам обчислювальних ресурсів і послуг, що складаються з мереж, доставки вмісту, зберігання, резервного копіювання та відновлення, а також обробки даних. Вони також допомагають користувачам у впровадженні та експлуатації власного програмного забезпечення.

При виборі IaaS, ви отримаєте сервери, мережеві ресурси та сховища в якості послуги, що підключається. Виходить, що компанія набуває обчислювальних ресурсів у постачальника, уникаючи необхідності закуповувати власне залізо та підтримувати його. При цьому сервіс може бути наданий на кшталт публічної хмари, приватної хмари або комбінованого підходу.

Поняття IaaS включає такі особливості:

- Ресурси – це послуга. Клієнт має можливість у будь-який час збільшувати та зменшувати обсяги споживаних ресурсів.
- З фізичними ресурсами можуть працювати декілька користувачів завдяки можливостям віртуалізації
- Гнучкі моделі оплати (наприклад, варіант pay as you go, коли компанія платить тільки за потужності, що споживаються)

Враховуючи все сказане вище, можна визначити, коли слід використовувати IaaS-рішення. Звертатися до IaaS варто в тому випадку, компанія іноді потребує підвищення потужностей при сплесках навантаження - тобто є потреба в оперативному масштабуванні інфраструктури.

Ще один варіант — компанія є стартапом, який не має коштів на придбання власного «заліза» та його підтримку, або ж організація хоче запустити експериментальний напрямок бізнесу та закуповувати обладнання для цього не завжди буває доцільно (проект може не злетіти).

Однак, незважаючи на гнучкість і масштабованість IaaS, технологія має певні обмеження. У зв'язку із цим є ситуації, коли використовувати її не рекомендується. Наприклад, компанія є гравцем регульованої галузі, правила якої не дозволяють зберігати дані на серверах, що не належать компанії.

Існує думка, що нібито не варто використовувати хмарні рішення для бізнес-критичних додатків. Проте зазначимо, що це негаразд. Критичний бізнес-додаток може бути розгорнутий на продуктивному сервері з 16 ядрами та терабайтами пам'яті, в якому передбачено дублювання ряду компонентів (у тому числі і на вищих рівнях).

Платформа як послуга, або PaaS, спрощує розгортання додатків та управління

ними, при цьому приховуючи в собі роботу з серверами, балансування навантаження, DNS та ін. Тому відпадає необхідність наймати інженерів для обслуговування інфраструктури. Це дозволяє розробникам приділяти більше уваги розробці та проблемам розгортання.

Тут слід зазначити, оскільки PaaS є другим рівнем піраміди хмарних послуг, то він будується на основі IaaS, проте ще більше зменшує час з моменту генерації ідеї до її втілення. Це досягається за рахунок більшої автоматизації процесів та абстракції від заліза.

Щоб абстрагувати концепцію роботи з серверами, було зроблено таке:

- Реалізована система складання, що компілює та зберігає код;
- Впроваджено базу даних управління додатками, що слідкує за версіями та метаданими;
- Запущено планувальник завдань, що обробляє велику групу серверів і запускає додаток на декількох машинах як на одній;
- Балансувальник навантаження керує інтернет-трафіком;
- Роботу DNS автоматизовано;
- Реалізовано форму контейнеризації (FreeBSD Jail, Solaris Zones, Linux Containers), що запобігає втручанню однієї програми в роботу іншого.

Перший та останній пункти – це ті елементи, які сприяли зростанню популярності Docker. Технологія Linux Container давно була частиною ядра ОС Linux, але автоматизувати їх використання зважилися лише великі компанії або PaaS-провайдери.

Компанії використовують архітектури та мікросервіси, орієнтовані на роботу з програмним забезпеченням, тому що вони пропонують можливості автоматичного розгортання та тестування коду, а також масштабування залежно від навантаження. Цей функціонал реалізує PaaS.

На жаль, такий підхід має одну серйозну ваду. Ви передаєте частину контролю своєрідному чорному ящику і потрапляєте у залежність від нього. Проте в іншому випадку компанії постійно винаходять велосипед або починають використовувати повільні інструменти.

У випадку SaaS споживач набуває можливості користуватися програмами постачальника, що виконуються у хмарі. Програми доступні з різних клієнтських пристроїв, наприклад, через браузер.

Програмне забезпечення як послуга (SaaS) — останній рівень хмарних обчислень, який найчастіше доповнює PaaS, як видно із схеми на початку статті. Це повнофункціональна програма для користувача, яка виконує певні функції, наприклад роботу із зображеннями або звуком. Найбільш популярною формою оплати у цьому сегменті залишається передплата.

У випадку SaaS в зону відповідальності хмарного провайдера передаються питання налаштування програм, моніторингу та резервного копіювання. Тому така модель роботи не потребує наявності в команді організації технічного фахівця – все робить провайдер.

На рівні «Інфраструктура як послуга» (IaaS) користувачі не мають права керувати хмарною інфраструктурою. Вони можуть лише керувати операційними системами та розгортати програми. На цьому рівні користувачі мають обмежені права на керування міжмережевими екранами хостів. До особливостей застосування рівня «Інфраструктура як послуга» (IaaS) належать наступні характеристики: використовується для підключення кількох різних користувачів обладнання; має можливості динамічного масштабування, вартість яких залежить від вибору інфраструктури; складається з ресурсів, які є часто доступними для використання.

Рівень «Інфраструктура як послуга» (IaaS) може застосовуватися до таких типів організацій: організації, які розвиваються, але не знають, які програми їм підходять; розвиток цих організацій є непередбачуваним, і вони ще не готові використати певну інфраструктуру; малі підприємства, яким не потрібно витрачати багато грошей і часу на обладнання та програмне забезпечення; компанії, які використовують Microsoft Azure, Amazon Web Services (AWS), IBM Smart Cloud, Cisco Metapod, Verizon, GoGrid і Google Compute Engine (GCE).

На рівні «Платформа як послуга» (PaaS) полегшується розгортання хмарної інфраструктури за допомогою програм, розроблених мовами та інструментами

програмування постачальників хмарних обчислень. Користувачі не мають права керувати серверами, програмами, даними, мережами або сховищами. Однак, користувачі можуть контролювати додатки, розміщені на хостах середовищ додатків.

Середовище розміщення додатків забезпечує швидке та прозоре виконання додатків і має низку компонентів, зокрема надання веб-служб, служб баз даних, платформ розробки та віртуальних робочих столів. Рівень «Платформа як послуга» (PaaS) характеризується такими особливостями: багато користувачів використовують одне середовище розробки для інтегрованих баз даних і веб-сервісів; різні категорії послуг з розробки та впровадження додатків використовуються для сприяння розробці, розгортанню, розгортанню та тестуванню додатків в інтегрованому середовищі; підписка та виставлення рахунків, керовані інструментами хмарних обчислень; технологія віртуалізації дозволяє користувачам отримувати доступ до корисних для них ресурсів, і це динамічно збільшує або зменшує їх важливість.

Рівень платформи як послуги (PaaS) може бути застосований до таких типів організацій: підприємства, які прагнуть диверсифікувати свої капіталовкладення, оскільки очікується економія коштів, пов’язаних з обчислювальною інфраструктурою, розробкою та впровадженням програм; компанії, які використовують Oracle Public Cloud, Microsoft Windows Azure, Google App Engine і Appends; розробники, які співпрацюють над спільним програмним продуктом; організацій, які розробляють програмне забезпечення за допомогою гнучких методів, оскільки при цьому можна зменшити кількість проблем, пов’язаних із швидкою розробкою та ітерацією програм.

Користувачам хмарних обчислень дозволено керувати хмарною інфраструктурою, що не дозволяє клієнтам хмарних сервісів авторизувати хмарну інфраструктуру та адмініструвати окремі програми. Користувачі можуть не мати достатнього доступу для налаштування програм. Планування ресурсів підприємства, управління взаємовідносинами з клієнтами в соціальних мережах, керування даними та безпека, керування електронною поштою та офісним

програмним забезпеченням – усе це включено до рівня програмного забезпечення як послуги (SaaS). Рівень «Програмне забезпечення як послуга» (SaaS) може застосовуватися до таких типів послуг: програми, які потребують доступу до Інтернету та мобільного зв'язку, включаючи програмне забезпечення для керування продажами та систему CRM; здійснення співпраці для реалізації короткострокових проектів, оскільки через визначення моделі оплати за користування швидко налаштувати та закрити середовище співпраці буде незручно; програми, на які спостерігається явне зростання та падіння попиту.

Рівень «Програмне забезпечення як послуга» (SaaS) може застосовуватися до компаній, які тільки починають роботу. Цьому рівню пристуні наступні риси: користувачам додатків не потрібно турбуватися про проблеми з апаратним і програмним забезпеченням, наприклад виправлення та оновлення; управління програмами базується на центральному сайті; сервер програмного забезпечення розміщено віддалено, а доступ до нього здійснюється через веб-браузер в Інтернеті [20, с. 106].

Рівень «Програмне забезпечення як послуга» (SaaS) дозволяє забезпечити високий рівень інформаційного ступіню захищеності даних в банку за рахунок наступних засобів: реалізації угоди про рівень обслуговування, адже перед використанням обчислювальних хмарних служб користувач повинен підписати угоду про рівень обслуговування; досягнення ефективності і результативності запровадження алгоритмів хмарних обчислень, які слугують допоміжним компонентом захисту системи інформаційного ступіню захищеності; забезпечення ефективної пропускної здатності мережі, адже продуктивність хмарних обчислень часто знижується через недостатню пропускну здатність, що призводить до неможливості запропонувати необхідні ресурси в будь-який момент; забезпечення відмовостійкості, адже хмарні обчислення повинні забезпечувати ресурси та резервне копіювання переліку наданих послуг; здійснення відновлення даних, адже хмарні обчислення можуть відновлювати будь-які дані, які були втрачені, пошкоджені або зіпсовані, що забезпечує ефективне функціонування; забезпечення обчислювальної потужності, масштабованості, резервування, які сприятливо

впливають на продуктивність хмарних обчислень.

Отже, додатки рівня «Програмне забезпечення як послуга» (SaaS) застосовують сервер SaaS-провайдера, а користувачі отримують до них доступ через інтернет-браузер. Користувач не купує SaaS-додаток, а орендує його – періодично сплачує за його використання деяку суму. Таким чином, досягається економічний ефект, який вважається одним з головних переваг технологій рівня «Програмне забезпечення як послуги» (SaaS). SaaS провайдер піклується про працездатність додатків, здійснює технічну підтримку користувачів, самостійно встановлює оновлення. Отже, користувач менше думає про технічну сторону питання інформаційного ступіню захищеності, а зосереджується на своїх бізнес-цілях і може бути впевненим, що надана інформація банку буде гарантовано збережена.

Що стосується питання захищеності великих даних, то постачальник технологій рівня «Програмне забезпечення як послуга» (SaaS) бере на себе всі обов`язки щодо організації центру обробки даних, розробки та оновлення програмного забезпечення, контролю роботи операційної системи, управління додатками та системою, управління мережею, серверами, сховищем.

Використання технологій рівня «Програмне забезпечення як послуга» (SaaS) має конкретні переваги для користувачів, а саме: доступ залежить лише від стабільного Інтернет-з`єднання, функціонування технологій відбувається незалежно від того, де знаходиться користувач і який пристрій застосовується, користувачеві не потрібно робити жодних оновлень, це робиться автоматично, користувачеві не потрібно встановлювати програмне забезпечення, йому необхідно тільки зареєструватися.

Всі ці переваги роблять застосування технологій рівня «Програмне забезпечення як послуга» (SaaS) дуже гнучким та привабливим рішенням. Провайдери SaaS забезпечують високий рівень захищеності даних. Провайдери SaaS для підвищення рівня захищеності своїх користувачів застосовують розширене шифрування даних.

Регулярне тестування та перевірки безпеки необхідні для забезпечення

захисту даних від зовнішніх і внутрішніх загроз. RBAC, або контроль доступу на основі ролей, керує входом співробітників і користувачів, щоб обмежити доступ до конфіденційної інформації.

Інфраструктура SaaS регулярно виконує резервне копіювання та відновлення даних, щоб забезпечити безперебійну роботу служби захисту даних. Провайдери SaaS використовують безпечні методи кодування, щоб обмежити кількість вразливостей, які з’являються в системі на цьому етапі. Завдяки постійному моніторингу додатків SaaS можна виявити підозрілу активність у режимі реального часу.

Приватні хмари та VPN можуть забезпечити безпеку та конфіденційність даних, оскільки вони будуть доступні для меншої кількості систем. VPN сьогодні широко використовуються для анонімного доступу до послуг і шифрування трафіку, щоб обмін даними між користувачем і постачальником SaaS залишався безпечним. Навчання співробітників і клієнтів є найкращою практикою для заходів кібербезпеки. Такі програми навчання та підвищення обізнаності можуть допомогти краще виявляти фішингові електронні листи, атаки соціальної інженерії та інші потенційні загрози. Крім того, вони також зможуть допомогти розробити кращий план реагування. Використання двофакторної або багатофакторної автентифікації може допомогти додати рівень до входу користувача, щоб гарантувати, що жоден зловмисник не спробує отримати доступ до його особистих даних.

# 2 ОЦІНКА РІВНЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ ВЕЛИКИХ ДАНИХ В БАНКУ

## 2.1 Побудова моделі хмарної піраміди за рахунок застосування способу SaaS для оцінки забезпечення інформаційного захисту великих даних в банку

У процесі обслуговування клієнтів банку збирається значна кількість даних про клієнтів, які необхідно ефективно зберігати, а для цього вже немає жодних можливостей. Ось чому хмарна піраміда та метод SaaS можуть бути використані для реалізації цих функцій, використовуючи програмне забезпечення, яке розгортається через Інтернет, або працює за брандмауером у локальній мережі чи персональному комп'ютері. З точки зору постачальників програмного забезпечення, SaaS — це програмне забезпечення, яке ліцензує програму клієнту як послугу на вимогу через підписку. Також використовується розрахункова модель і багатокористувацькі функції. Програма SaaS може використовуватися кількома користувачами одночасно, але вони не впливають один на одного.

Додаток SaaS має одночасно вирішувати кілька питань, а саме масштабованість, розділення та узгодженість бази даних, відмовостійкість, безпеку та справедливість, паралельну обробку, ізоляцію, продуктивність та доступність. З точки зору кінцевого користувача, SaaS надає доступ до можливостей, які не надаються іншим споживачам □23, с. 190□.

BIB (банківське посередництво) призводить до великого навантаження на дані та середню обробку транзакцій і висуває високі вимоги до системи безпеки. Найважливішим показником є продуктивність системи, яка вимірює використання системи та кількість транзакцій за секунду. Еталонні показники продуктивності повинні включати два основні компоненти: робоче навантаження, яке включає роботу, яку система виконуватиме під час еталонного тесту, і набір показників продуктивності, що характеризує продуктивність системи під час еталонного тесту. Основна ідея полягає в моделюванні архітектури, бази даних і бізнес-транзакцій

BIB для створення реальних моделей BIB. Ці моделі дозволяють запропонувати відповідний еталон BIB разом із кваліфікованими показниками. Застосовується класифікація методів тестування продуктивності HPFT, яка поділяє методи на наступні три класи: методи, засновані на тестуванні продуктивності, такі як послідовні дані OLTP TPC; методи, засновані на інструментах тестування робочого навантаження, таких як HP LoadRunner і Spirent Avalanche; методи, засновані на архітектурі та аналізі робочого навантаження / робочого процесу [10, с. 22].

Також застосовуються дослідження контрольних показників та вимірювань застосованої методики для оцінки якості та продуктивності системи HPFT, такі як TPC-C і TPC-E. Тест TPC-C моделює обчислювальне середовище для введення замовлень, коли група користувачів виконує транзакції з простою базою даних TPC-C, а тест TPC-E моделює брокерську компанію разом із клієнтами, які генерують транзакції, що пов’язані з угодами, рахунками, запитами тощо. Хоча існує багато тестів OLTP, все ще не вистачає тестів, які грунтуються на фактичних транзакціях і використовують високопродуктивні архітектури.

Модель BIB застосовує модулі обробки ключів BIB business. Використовується архітектура на основі SaaS, SaaS-BIB-DM (модель бази даних), SaaS-BIB-DF (модель потоків даних) і опис транзакцій. Тестування включає дії, які підтверджують аспекти системи. Різноманітні проблеми виникають на кожному рівні тестування SaaS, і типове тестування SOA (сервісно-орієнтованої архітектури) складається з тестування композиції, інтеграції та виконання функціонального тестування. Проте, найбільш фундаментальними факторами є архітектура та моделі.

Абревіатура MTA була утворена на основі Multi-Tenant Architecture, і є ключовою функцією SOA (сервісно-орієнтованої архітектури). MTA надає можливість контролювати впровадження хмарних технологій.

Абревіатура SaaS-BIB-DM утворена на основі моделі бізнес-бази даних банківського посередника на основі програмного забезпечення як послуги, яка сформована на рівні 4 архітектури BIB на основі SaaS. Застосовується SaaS гібридна схема розподілу бази даних для підвищення продуктивності бази даних і

тестування. База даних BIB поділяється на чотири категорії, включаючи Partner Tables (опис таблиць сторонніх компаній), Customer Tables (опис особистих рахунків та інформаційних таблиць), Bank Tables (опис банківських каналів, рахунків, контрактів та інших інформаційних таблиць) і таблиці розмірів (опис технічної допомоги).

Застосовуються три типи даних у моделі SaaS-BIB-DM, а саме метадані, фактичні дані та зведений індекс. Застосовано гібридну схему поділу для моделі SaaS-BIB-DM, яка розподіляє таблицю на рядки та горизонтальні сховища ключ-значень.

Показники моделі хмарної піраміди та способу SaaS для забезпечення інформаційного ступіню захищеності великих даних банку розраховано за формулами (2.1)-(2.7):

$$S - \text{множина суб`єктів; } O - \text{множина об`єктів, така що } S \subset O \quad (2.1)$$

$$R = \{r, w\} - \text{множина прав доступу, } r - \text{на читання, } w - \text{на запис} \quad (2.2)$$

$$S - \text{множина суб`єктів; } O - \text{множина об`єктів, така що } S \subset O \quad (2.3)$$

$$L = \{U, SU, S, TS\} - \text{множина рівнів конфіденційності інформації,} \quad (2.4)$$

де U – некласифікований;

SU – класифікований;

S – секретний;

TS – найвищий рівень секретності.

$$\Lambda = (L, \leq, \odot, \otimes) - \text{решітка рівня конфіденційності,} \quad (2.5)$$

де $\leq$ – оператор, що визначає часткове нестроге співвідношення порядку до рівнів конфіденційності;

$\odot$ – оператор найменшої верхньої межі;

$\otimes$ – оператор найменшої нижньої межі.

$$V - \text{множина станів системи, сукупність упорядкованих пар } (F, M), \quad (2.6)$$

де $F : S \cup O \rightarrow L$ – функція рівнів конфіденційності, що ставить у відповідність кожному об`єкту і суб`єкту в системі певного рівня конфіденційності;

M – матриця поточних прав доступу.

$$\Sigma = (\mathrm{vo}, \mathrm{R}, \mathrm{T}), \tag{2.7}$$

де $v$o − початковий стан системи;

$R$ − множина прав доступу до об`єктів;

$T$ − функція переходу, що переміщує систему з одного стану в наступний при виконанні запитів.

Із формул (2.1)-(2.7) можна зробити висновок, що математична модель набуває форму піраміди, в якій найпростіший параметр розташовано зверху, а функція стану системи – знизу. Складність системи зростає зверху-вниз. SaaS-BIB-WF (робочий процес) складається із семи кроків, і якщо етап трансформації не вдається, робочий процес розпочнеться заново з кроку 1. Робочий процес розпочинається з виклику клієнта сторонньої компанії або клієнта власного банку, якому потрібен BIB (банківський посередницький бізнес) через касу банку або Інтернет-сервіси. Після того, як банк отримає вимоги обробки агентських транзакцій, банк здійснить пошук відповідних послуг і застосує форму SaaS-BIB-WF на вимогу. Якщо судження про успіх не виконано, відбувається повернення до кроку 1. Потім в процесі реалізації кроку 4 здійснюватиметься їх обробка за допомогою рівня 3 архітектури SaaS-BIB. Потім проводиться реальний пошук і виконання робочого процесу, а також одночасний запис результатів тестування та створення результатів і звітів застосовуються для подальшого аналізу. Оцінку рівнів захищеності великих даних хмарної піраміди в банку розраховано за формулами (2.8)-(2.9):

– стан системи ($F$, $M$) називається безпечним за читанням, якщо для кожного суб`єкта, який здійснює в цьому стані доступ за читанням до об`єкта, рівень захищеності суб`єкта домінує над рівнем захищеності об`єкта, адже

$$\forall \mathrm{s} \in \mathrm{S}, \forall \mathrm{o} \in \mathrm{O}, \mathrm{r} \in \mathrm{M}\,[\mathrm{s}, \mathrm{o}] \rightarrow \mathrm{F}\,(\mathrm{o}) \leq \mathrm{F}\,(\mathrm{s}) \tag{2.8}$$

– стан системи $(F, M)$ називається безпечним по запису у випадку, якщо для кожного суб`єкта, який здійснює в цьому стані доступ по запису до об`єкта, рівень захищеності об`єкта домінує над рівнем захищеності суб`єкта, адже:

$$\forall s\, S, \forall o \in O,\ w \in M\,[s, o] \rightarrow F\,(s) \leq F\,(o) \qquad (2.9)$$

– стан $(F, M)$ називається безпечним, якщо він є безпечним за читанням та по запису.

Із формул (2.8)-(2.9) можна зробити висновок, що для оцінки рівня захищеності всієї системи слід оцінити безпечність функціонування кожного рівня утвореної хмарної піраміди. Програма SaaS є альтернативою на основі послуг для надання автономного програмного забезпечення користувача [1, с. 35]. Помітивши зростання цифрової трансформації, дистанційно доступні програмні послуги стають трендом. Як результат, послуги розробки додатків SaaS є зручним рішенням. Часто SaaS-додатки є послугами на основі підписки на вимогу, де користувачам не потрібно встановлювати їх локально.

Користувач зможе отримати доступ до програми SaaS з кількох пристроїв за допомогою свого Інтернет-браузера. Крім того, власник продукту SaaS не є зобов`язаним відповідати за обслуговування хмарної інфраструктури. Сховищами даних керують сторонні постачальники послуг хмарних обчислень, такі як AWS і Azure. Розробка додатків SaaS може призвести до створення надійного та масштабованого продукту.

Служби розробки SaaS здійснює розробку та дизайн додатків SaaS, узгоджує проблеми архітектури з кількома клієнтами, а також забезпечує інтеграцію сторонніх API, надає консультації щодо програм SaaS, а також технічну підтримку та технічне обслуговування. Слід підкреслити, що початкові кроки слідування процесу обігу даних проходять шляхом аналізу ідей користувачів і створення робочого процесу для банківського планування. Одним із критичних етапів є анотація, яка потребує глибокого вивчення, планування та затвердження ідеї програми.

Додаток дозволяє продемонструвати користувачеві можливості хмарних ресурсів [11, с. 173]. Веб-мобільний додаток зосереджується на дизайні інтерфейсу

користувача (UI) та дизайні взаємодії з користувачем (UX). Крім того, щоб робочий процес користувача залишався доступним і прибутковим, експерт з інтерфейсу користувача / UX повинен розробити інтерфейс з урахуванням простоти та розуміння для користувача.

Бекенд SaaS є невід`ємною частиною розробки. Дотримуючись оцінки інтерфейсу, розробка бекенда відіграє життєво важливу роль для демонстрації бажаного результату. Інженери серверного програмного забезпечення зосередяться на впровадженні дизайну, додадуться функції управління хмарою, а також буде проведена інтеграція API за потреби та буде підготовлено сценарії до розгортання.

На цьому етапі розробка та хмарна інфраструктура є паралельним етапом процесу розробки додатків SaaS, який пілотується розробниками архітектурних рішень та програмних забезпечень. Цей етап безпосередньо впливає на оцінку вартості, оскільки є більш складним та трудомістким. Коли програмне забезпечення буде готове, воно буде розгорнуто на хмарній платформі, наприклад, AWS, Azure, IBM Watson, Google Cloud або на інших подібних платформах. На цьому етапі залучається експертна команда інженерів DevOps для введення в дію хмарного сховища. Крім того, інженери зможуть допомогти підтримати та масштабувати хмарну інфраструктуру. Вибір специфікацій інфраструктури та ресурсів відображатиме поточні витрати на розробку додатків SaaS.

Тестування додатків SaaS передбачає надання клієнту бездоганного, безпечного та надійного програмного забезпечення. Інженер DevOps контролює та підтримує функції для оновлення хмарного сервера. Вдосконалення стає найважливішим фактором. Оптимізація кожного фактора SaaS за допомогою оновлень і додавання різних функцій може допомогти покращити рівень масштабованості та доступності для користувача.

На ринку SaaS додатки SaaS поділяються на категорії. Додатки SaaS мають дві різні моделі рішень: горизонтальну SaaS і вертикальну SaaS. Горизонтальна модель SaaS – добре структурована програма, яка використовує хмарні сервіси. Вертикальна модель SaaS являє собою створення програми SaaS для певної галузі. Слід підкреслити, що SaaS-BIB-TM (модель транзакцій) є абревіатурою від моделі

банківських посередницьких бізнес-транзакцій на основі програмного забезпечення як послуги, яка є сформованою на рівні 3 архітектури BIB на основі SaaS. Рівень послуг і композиції складається з різних транзакцій BIB. Передумовою банківського обслуговування є підписання угоди з клієнтом [22, с. 351].

Транзакційні категорії угод є основою для кожної транзакції пошуку, торгівлі чи відстеження. Категорія «Торгівля» містить дві ключові транзакції обробки, такі як «Комісійна плата» та «Оплатна транзакція». Категорія «Пошук» має три різні види обробки пошуку на основі різних цілей.

Перш за все, порівняльний тест BIB на основі SaaS застосовуватиме наступні чотири показники, такі як:

– tpsBank (транзакції за секунду банківського бізнесу);
– PCN (паралельна кількість активних користувачів);
– TRT (час відгуку обробки транзакцій);
– RU (використання ресурсів, пам`яті).

Сценарій – це послідовність дій, пов`язаних дією чотирьох факторів, такими як послідовність, вибір, цикл і паралелізм. Кожна діяльність – призначення даних, обмін подією, виконання дії або виконання підсценарію. Простий сценарій 1 залучає кілька користувачів, які хочуть сплатити рахунки за рахунок залучення банківського посередника. Потім компанія підпише угоду з банком, щоб уповноважити бізнес-систему банку-посередника, яка стягує комісію з користувачів компанії. Користувачі компанії можуть обрати шлях проведення Інтернет-платежів.

Складний або змішаний сценарій 2 полягає в тому, що міжнародна компанія повинна щомісяця сплачувати заробітну плату своїм співробітникам і надсилати премії щорічно. Міжнародна компанія повинна підписати угоду з бізнес-системою банку-посередника, щоб отримати послугу виплати заробітної плати. Відповідно до умов угоди, йому буде призначено дату виплати заробітної плати, і система BIB одночасно оновлюватиме баланс компанії та рахунки її співробітників.

Для забезпечення реалізації взаємодії з клієнтами банку застосовується система управління відносинами з клієнтами (CRM), яка включає в собі набір

інтегрованих рішень, які допомагають використовувати, відстежувати та зберігати інформацію про існуючих та потенційних клієнтів банку. Збираючи цю інформацію в централізованій системі, підрозділи банку зможуть отримати доступ до аналітики будь-якої миті.

Ще нещодавно керівництво банку відстежувало дані про клієнтів за допомогою електронних таблиць, електронної пошти та інших ізольованих CRM-рішень. Відсутність інтеграції та автоматизації не дозволяло співробітникам швидко знаходити актуальну інформацію та обмінюватися нею, що уповільнювало здатність створювати маркетингові кампанії, залучати нових потенційних клієнтів та обслуговувати покупців [2, с. 1690].

CRM автоматично збирає величезну кількість інформації про існуючих та потенційних клієнтів. Ці дані включають адреси електронної пошти, телефонні номери, сайти компаній, публікації в соціальних мережах, історії придбання, а також запити на обслуговування та підтримку. Надалі система інтегрує дані та створює консолідовані профілі, які спільно використовуватимуть відповідні команди. CRM, також, підключається за допомогою інших бізнес-засобів, включаючи онлайн-чати та програми для обміну документацією. Крім того, вона включає вбудовані засоби бізнес-аналітики та штучного інтелекту, які прискорюють виконання адміністративних завдань та надають аналітику існуючих даних. Розглянемо кілька способів ефективно використовувати можливості CRM, до яких належать:

– Відстеження кожної можливої угоди для збільшення обсягів наданих банківських послуг. CRM-рішення допомагають відстежувати дані, пов`язані з потенційними клієнтами, і отримувати аналітику, щоб відділи продажів та маркетингу співпрацювали організовано, розуміли етап залучення кожного потенційного клієнта в процесі продажу та знали, хто регулював кожну окрему угоду.

– Оцінка обсягів наданих послуг, щоб отримувати дані про продуктивність в реальному часі.

– Зосередження на найважливішому за допомогою вбудованої аналітики,

щоб визначати головні пріоритети та максимально ефективно використовувати час та зусилля для забезпечення впровадження конкурентної стратегії розвитку банку.

– Оптимізація робочих процесів за допомогою автоматизації. Автоматизація завдань допоможе прискорити процес обслуговування клієнтів. Таким чином, ці рішення скорочують обсяг операцій, що повторюються, дозволяючи команді співробітників зосередитися на завданнях з великою віддачею.

– Забезпечення розвитку гнучкості роботи банку. Масштабоване інтегроване CRM-рішення, створене на безпечній платформі, допомагає задовольняти постійно мінливі потреби клієнтів банку та ринку.

Застосовується, також, Microsoft 365, що об`єднує в собі Word, Excel, PowerPoint, Outlook, OneNote, зі всіма актуальними оновленнями та доповненнями, а саме Teams, Skype for Business, SharePoint, OneDrive. Завдяки тісній інтеграції додатків, співробітники отримають по 1 ТБ хмарного сховища, загальний доступ до файлів, календарів, зустрічей, зможуть ефективно працювати, і бути на зв`язку в потрібний момент. Щомісяця додатки Office отримують оновлення та розширюють функціональність. Прості інструкції і цілодобова підтримка від Microsoft допоможе швидше розпочати роботу [14, с. 242].

Windows 365 поєднує в собі потужність і безпеку Windows 10 або Windows 11 із універсальністю хмарної доставки для того, щоб забезпечити надійне та знайоме робоче середовище на будь-якому фізичному пристрої. Хмарні ПК є оптимізованими для забезпечення гнучкості бізнесу та користувачів, адже виставляється рахунок за моделлю витрат на кожного користувача за місяць, що спрощує структуру витрат клієнтських обчислювальних середовищ.

Windows 365 забезпечує простоту використання додатку [6, с. 263]. Надається кожному користувачеві комп`ютер із доступом до хмари, на якому застосовується індивідуальна операційна система Windows 10 або Windows 11, забезпечуючи просту в управлінні екосистему. Це дозволяє IT-менеджерам зосередитися на вирішенні проблем бізнес-процесів. Застосування знайомої та потужної обчислювальної екосистеми кінцевого користувача є ефективним рішенням для організацій роботи над задоволенням складних потреб гібридної або

віддаленої роботи в банку.

Процес економічної перевірки ESG є перевіреним способом розуміння, перевірки, кількісної оцінки та моделювання пропозиції економічної цінності продукту або рішення. Цей процес використовує ключові компетенції ESG на ринку для проведення галузевого аналізу, здійснюючи прогнозні дослідження та техніко-економічне підтвердження. Процес економічної перевірки ESG включає реалізацію комунікацій з експертами в галузі та галузевими аналітиками, щоб краще зрозуміти та кількісно визначити, як Windows 365 Cloud PC може вплинути на банки, особливо в порівнянні з іншими системами Desktop as a Service (DaaS) та актуальними рішеннями застосування віртуального робочого столу.

Різні якісні та кількісні результати були використані як основа для поглибленого дослідження економічної моделі, що порівнює очікувані витрати та переваги цих рішень EUC. Хмарні середовища Windows 365 зможуть принести користь керівництву банку, яким доручено надавати обчислювальне середовище кінцевого користувача, яке надає можливість своїм співробітникам і підрядникам досягати визначених бізнес-цілей. Потенційні клієнти обраного банку зможуть очікувати економії та переваг у наступних трьох категоріях, таких як:

– передбачуваність витрат – здатність прогнозувати витрати, які допомагають узгодити технології з досягненням бізнес-цілей;

– гнучкість для користувачів – надання співробітникам і підрядникам рішення EUC за години замість тижнів, що прискорює час оцінки, дозволяючи банкам швидше використовувати тенденції та короткострокові перспективи розвитку можливостей програми;

– покращена система захищеності – захист інтелектуальної та фізичної власності під час швидких змін, що являє собою величезний виклик для організацій. З Windows 365 ESG віднайдено значні покращення в здатності посилити позицію захищеності.

Поєднання виключених витрат і моделі передбачуваних фіксованих витрат, забезпечує фінансову вигоду в кількох випадках банкам, які використовують Windows 365 Cloud PCs, до яких належать:

– зниження витрат – перехід на Windows 365 зменшує або усуває витрати в кількох сферах, включаючи ліцензування VDI, застосування серверних операційних систем, ліцензування віддаленого робочого столу, зберігання, управління, живлення та охолодження, отримання ліцензії, здійснення управління VDI тощо. Докладні відомості про економічні переваги забезпечують застосування моделі з фіксованою ціною – цінною можливістю прогнозування витрат, адже більшість моделей ціноутворення VDI базуються на обсягах споживання; хоча спочатку це може здатися перевагою, менеджери обраного банку часто виявляють, що їхні щомісячні витрати виходять далеко за рамки прогнозів. Застосовується, також, можливість перехресного стягнення плати за послуги, яке передбачає, що організації, які стягують внутрішні або зовнішні бізнес-групи за ліцензії, апаратне забезпечення або служби виявлять, що модель прогнозованої вартості Windows 365 значно полегшує розподіл конкретних витрат детально і передбачувано, особливо в порівнянні з капіталомісткими закупівлями, необхідними для полегшення локального VDI або DaaS.

Для використання програми SaaS комунікаційні служби повинні надавати інтерфейс веб-сервісу та запропонувати зв`язок як послугу (CaaS) [4, с. 763]. Оскільки комунікації є службами з підтримкою стану під час надання інтерфейсів веб-служб комунікаційним службам, то необхідно врахувати кілька факторів. По-перше, послуги зв`язку є двонаправленими. Кінцевими точками зв`язку можуть бути як клієнт, так і сервер. Не лише кінцева точка може ініціювати запити на отримання послуг від постачальника послуг, постачальник послуг, також, може ініціювати запити або надсилати події до кінцевої точки, яка запитує послугу. По-друге, комунікаційні послуги мають асинхронний характер. Коли кінцева точка ініціює запит до постачальника послуг, постачальник послуг може підтвердити запит і надіслати остаточний результат асинхронно після того, як постачальник послуг завершить обробку запиту.

Сповіщення про події є ще однією загальною та важливою функцією в службах зв`язку. Одним із прикладів є послуги телефонії, де клієнт (телефон) отримує події (дзвінок) від сервера без ініціювання запиту. Взаємодії між клієнтом

і сервером відбуваються послідовно, і вони мають значення лише в контексті сеансу. Ці фактори необхідно врахувати під час надання інтерфейсу веб-сервісу для комунікаційних служб. Існуючих інтеграційних рішень SaaS, які в основному обслуговують інтеграцію даних, може бути недостатньо для обробки комунікаційних послуг.

Незважаючи на те, що платформи SaaS надають веб-сервіси як механізм інтеграції, пряма інтеграція між програмою SaaS і локальними програмами відбувається рідко з наступних причин. Через широкий спектр існуючих стандартів веб-сервісів різні постачальники підтримують різний набір стандартів. Навіть для одного стандарту веб-служб постачальники можуть підтримувати різні версії, а також спеціальні розширення. WS-I Basic Profile надає деякі рекомендації щодо сумісності веб-сервісів, але проблема є далекою від вирішення. Щоб вирішити проблему взаємодії, інтеграція зазвичай здійснюється через адаптер.

Наприклад, служби зв`язку, визначені мовою опису веб-служб (WSDL) для CSTA Phase III (ECMA-348), використовують WS-Eventing і WS-BaseNotification для сповіщення про події, де платформа SaaS все ще користується власними, часто значно спрощеними службами організації подій. Крім того, комунікаційні послуги включають кілька операцій, що виконуються в певному порядку.

У цьому випадку перевага віддається адаптеру служби, щоб увімкнути композицію та оркестровку служби. Це зменшує кількість взаємодій між SaaS і корпоративними додатками, роблячи додатки SaaS більш зосередженими на бізнес-логіці, а не на деталях зв`язку [20, с. 180].

Наприклад, у службі конференції, щоб розпочати конференцію, клієнтській програмі потрібно спочатку увійти на сервер конференції, отримати ідентифікатор сеансу, а потім він може викликати операцію для запуску конференції з конкретним ідентифікатором сеансу. Якщо клієнтська програма бажає відстежувати статус конференції та її учасників, необхідно підписатися на сповіщення про події від служби конференції, щоб отримувати цікаві події. У цьому випадку сервісний адаптер виконає всі детальні операції для з`єднання підписки на подію та доставки подій між мостом конференції та власним інтерфейсом подій абонента. Це дозволяє

службі обгортати деталі зіставлення повідомлень і маршалінгу, відкриваючи високорівневі служби додаткам SaaS для виклику меню.

Послуги зв`язку, як правило, знаходяться в корпоративних мережах і захищені NAT/брандмауерам. Програми SaaS, з іншого боку, розміщуються в хмарі. Щоб увімкнути інтеграцію, банку потрібно дозволити програмам SaaS отримувати доступ до своїх локальних служб через корпоративні NAT / брандмауери. Корпоративний брандмауер/NAT впливає на інтеграцію SaaS із локальними програмами у двох аспектах. По-перше, розташування (або URL-адреса) локальної програми буде дійсним лише в корпоративній мережі, і її не можна маршрутизувати у відкритому доступі. По-друге, брандмауер налаштовується так, щоб дозволяти лише вихідний трафік, блокуючи весь вхідний трафік до банку. Отже, коли додатки SaaS надсилають запити веб-сервісу до локальної програми, брандмауер відхиляє ці запити.

Щоб зробити локальні програми доступними, типовий підхід вимагає або змінити конфігурацію брандмауера для проходження трафіку додатків SaaS від певного хоста, або розгорнути зворотний проксі-сервер у DMZ для маршрутизації трафіку до внутрішніх програм. Оскільки корпоративна архітектура захищеності може бути дуже складною, процес схвалення цих змін займає багато часу. Це перешкоджатиме розгортанню та прийняттю SaaS. На додаток до потенційних ризиків безпеці, які виникають у конфігурації брандмауера для кожної служби, стає дедалі складніше підтримувати модель надання послуг SaaS, адже SaaS сервіси можна додавати або видаляти на вимогу клієнтів.

Віртуальна приватна мережа (VPN) є ще однією галузевою практикою роботи на рівні корпоративних доменів [9, с. 152]. Однак, це – неможливе рішення для SaaS, оскільки SaaS є платформою з декількома клієнтами, де кілька клієнтів спільно використовують ту саму мережеву інфраструктуру, той самий комп`ютер і навіть той самий запущений екземпляр програми. Завдяки VPN локальні служби залишаються відкритими для всіх додатків, що працюють на платформі SaaS включно з програмами від ненавмисних орендарів.

Одним з альтернативних підходів, який використовується в багатьох

рішеннях інтеграції SaaS, є зміна шаблону інтеграції, щоб уникнути прямого доступу до локальних даних або послуг із програм SaaS. Локальні програми передають дані до програм SaaS через регулярні проміжки часу або щоразу, коли дані змінюються. Оскільки в цьому випадку всі повідомлення веб-служб ініціюються зсередини брандмауера, вони будуть дозволені брандмауером / NAT. Цей підхід не підходить для комунікаційних послуг, оскільки програми SaaS очікують отримання послуг майже в режимі реального часу. Крім того, він не масштабується, оскільки надсилання даних може бути інтенсивним з точки зору обчислень і мережі, коли дані часто змінюються, особливо якщо передаються масові дані.

## 2.2 Оцінка критичних параметрів, що стримують розвиток моделі хмарної піраміди для забезпечення захисту великих даних в банку

Застосування моделі хмарної піраміди та способу SaaS обмежуються впливом критичних параметрів, які є загрозами, що заважають користувачам якнайповніше довіряти персональну інформацію банкам, послугами яких користуються [3, с. 211].

Поява цих загроз може призвести до пошкодження або незаконного доступу до конфіденційних даних користувача. Основні загрози безпеці банківської інформації включають зловживання та нечесне використання хмарних обчислень зловмисниками, уразливості спільних технологій, втрату/витік даних, крадіжку рахунків, послуг і трафіку, а також застосування ризику невідомого профілю. Ці загрози пов’язані з комп’ютерними та мережевими вторгненнями чи атаками. Деякі інші загрози включають втрату фізичного контролю над даними, відсутність стандартів безпеки, регулювання на місцевому, національному та міжнародному рівнях, а також недостатній час безвідмовної роботи для критично важливих програм.

Постачальники хмарних послуг вирішують ці загрози за допомогою добре розроблених і перевірених заходів безпеки та процесів і вважають за краще

гарантувати безпеку через контракти з постачальниками онлайн-послуг, а не за допомогою внутрішнього контролю. Вразливість – це «слабке місце в системі безпеки». Іншими словами, вразливість відноситься до програмного, апаратного або процедурного недоліку, який може дозволити зловмиснику увійти в комп'ютер або мережу та отримати несанкціонований доступ до ресурсів у середовищі. Вразливість характеризує відсутність або слабкість захисту, якою можна скористатися. У випадку корпоративних хмарних обчислень вразливі місця включають підслуховування, злом, зловмисні атаки та збої. У хмарних обчисленнях будь-кому легко точно визначити фізичне розташування цільових даних, щоб використати відмову в обслуговуванні для атаки на цільові дані.

Оцінка критичних параметрів обмежень використання методу SaaS для забезпечення безпеки великих даних у банківській справі наведена в таблиці 2.1.

Таблиця 2.1

Оцінка критичних параметрів обмежень застосування способу SaaS для забезпечення захищеності великих даних в банківській діяльності

| Назва критичного параметру | Частота проявів | Ваговий критерій, балів із 10 | Сукупна оцінка |
|---|---|---|---|
| Зловживання та нечесне використання хмарних обчислень зловмисникам | 0,01 | 1 | 0,01 |
| Вразливі місця спільних технологій | 0,02 | 2 | 0,04 |
| Втрата / витік даних | 0,03 | 2 | 0,06 |
| Викрадення облікових записів, служб і трафіку | 0,04 | 3 | 0,12 |
| Застосування невідомого ризику профілю | 0,05 | 3 | 0,15 |
| Всього | | | 0,38 |

З таблиці 2.1 можна зробити висновок, що кожен із зазначених вище ризиків має незначний вплив на систему інформаційної безпеки великих даних в цілому, однак збільшення частоти проявів кожного критичного параметра може призвести до репутаційних втрат і ризиків втрата клієнтів до рівня 40%.

Використання хмарних сервісів полягає в максимальному залученні

фізичних серверів, ефективному завантаженні їх технічними засобами. Хмарні обчислення слід запропонувати як «клієнтську технологію» для обмеження впливу перевантажених даними ноутбуків і загроз резервного копіювання. Використання методу SaaS дозволить хмарі стати кращим антивірусним детектором, а провайдери хмарних обчислень зможуть виправити застосування неефективних підходів до питань безпеки великих даних.

Підтримка є ключовою вимогою для хмарних і локальних програм, де і банки, і кінцеві користувачі платять постачальникам хмарних послуг. Отже, очікується, що постачальники хмарних послуг наймуть і навчать персонал служби підтримки, щоб надавати цілодобову підтримку своїм клієнтам. Таким чином, доступність і підтримка позитивно вплинуть на сприйману корисність додатків і сприйману легкість використання додатків SaaS.

Моніторинг додатків SaaS – набір дій DevOps, призначених для запису та аналізу продуктивності додатків SaaS з метою сповіщення про невідповідності та нерегулярні шаблони для своєчасного виявлення аномалій, аналітики, виправлення помилок та запобігання фактичним проблемам [13, с. 137□.

Складність розподілених систем, яка виникає внаслідок побудови архітектури мікросервісів, посилюється складнощами хмарних обчислень і вимагає використання більшої кількості інструментів моніторингу. Варто підкреслити, що моніторинг мережі відрізняється від моніторингу додатків, оскільки він зосереджений на сповіщенні адміністраторів про стан систем, коли користувач не може отримати доступ до певного рішення. Моніторинг додатків, з іншого боку, забезпечує спостереження за кількома параметрами та показниками, які сигналізують про аномалії, навіть коли користувачі можуть отримати доступ до програми SaaS.

Моніторинг продуктивності програми SaaS і керування продуктивністю програми часто використовуються як взаємозамінні. Однак термін «управління» передбачає більш проактивний, стратегічний підхід, тоді як «моніторинг» відноситься до вузького контексту тактичного спостереження. Вибір правильного постачальника SaaS стає дедалі важливішим, оскільки все більше банків прагнуть

передавати свої IT-системи на аутсорсинг. У зв'язку з появою бар'єрів на вході і в процесі функціонування SaaS-додатків, виникає необхідність вирішення існуючих проблем, щоб запропонувати значний спектр якісних послуг нашим клієнтам.

Правильне розуміння конкретних бізнес-потреб є критично важливим перед вибором будь-якого постачальника SaaS, включаючи технічні вимоги та вимоги до послуг, управління даними, безпеку даних і керування послугами, включаючи уточнення мінімальних і конкретних бізнес-вимог, щоб можна було порівняти їх із тим, що пропонує постачальник.

Вибір або порівняльний аналіз постачальника послуг стане легшим, якщо чітко вдасться визначити мінімальні та конкретні банківські вимоги [8, с. 108]. Хоча сертифікація та відповідність можуть бути не такими важливими для обраного банку, адже вони можуть бути вирішальними факторами для обраного банку, який має відповідати галузевим стандартам. Розуміння того, як постачальник планує впроваджувати інновації та розвиватися, допомагає визначити, чи відповідатиме це довгостроковим цілям розвитку діяльності банку.

Місцезнаходження даних відіграє ключову роль у складанні плану класифікації даних. Постачальники SaaS, які пропонують контроль над юрисдикцією, обробкою та керуванням даними, є кращими за постачальників, які цього не роблять. Можливість захисту даних під час передавання за допомогою шифрування або шифрування лише конфіденційних даних мінімізує ймовірність несанкціонованого доступу. Угода про рівень обслуговування має чітко визначати процеси порушення даних і втрати даних, а також повинна узгоджуватися з нормативними зобов`язаннями банківської діяльності й передбачати дотримання вимог і управління ризиками. Кодекс практики для постачальників хмарних послуг є чудовою відправною точкою для визначення процесів і політик керування даними та побудови системи захищеності у банківській діяльності. Діяльність користувачів і доступ до них мають бути перевірені через усі можливі маршрути, а ролі захищеності мають бути чітко визначені в Угоді про рівень обслуговування.

Для того, щоб обмежити вплив дії критичних параметрів функціонування програми SaaS, необхідно інтегрувати корпоративні комунікаційні служби з

програмами SaaS [21, с. 254]. По-перше, потрібно застосувати механізм, щоб виставляти послуги зв`язку як веб-послуги (як у CaaS). По-друге, потрібно побудувати структуру для перекладу та композиції служби надання банківських послуг. По-третє, коли локальні служби знаходяться всередині брандмауера банку, слід дозволити програмам SaaS, які взаємодіють у двосторонніх веб-службах, отримувати доступ до локальних служб без змін конфігурації брандмауера.

Розглянемо інтеграцію платформи SaaS із корпоративними комунікаційними послугами через проміжне програмне забезпечення інтеграції SaaS. Проміжне програмне забезпечення інтеграції SaaS дозволяє програмам SaaS отримувати доступ до комунікацій як послуг через двосторонні веб-сервіси, до елементів якого належать:

– Web Service Enabler – компонент для надання інтерфейсів веб-служб для комунікаційних служб. Для комунікаційних служб, які не мають інтерфейсу веб-служби, Web Service Enabler перетворює виклики веб-служб у належні виклики API і навпаки;

– SaaS Adapter Framework (SAF) – посередник для з`єднання служб SaaS і локальних служб; його основні функції включають відображення / маршалінг повідомлень веб-сервісу, перетворення сервісу та композицію сервісу, причому він забезпечує механізм / фреймворк для розробки та розгортання нових сервісних адаптерів;

– Двосторонній шлюз веб-служб – спеціальний шлюз для додатків SaaS для перетину корпоративних NAT/брандмауерів без зміни конфігурації брандмауера, адже він складається з двох підкомпонентів, тобто агента PASS і сервера PASS.

Користувачі програм SaaS взаємодіють із програмами SaaS через HTTP / HTTPS [7, с. 21]. Користувач може отримати доступ до комунікаційних послуг із програми SaaS, викликавши службу, розгорнуту на SAF. Агент PASS і сервер PASS дозволяють запиту служби SOAP перетинати брандмауер через спеціальний захищений тунель для досягнення SAF, і вони використовують стандартні безпечні процедури доступу до веб-служби. Потім SAF викликає одну або кілька служб

зв`язку від імені програми SaaS і надсилає відповідь назад до програми SaaS.

Компонент Web Service (WS) Enabler розширює механізм односторонньої взаємодії веб-служб запитів/відповідей до парадигми двосторонніх повнодуплексних взаємодій веб-служб для зв`язку. Це дозволяє відобразити та використати повнодуплексні та складні комунікаційні служби як веб-сервіси. Слід зазначити, що веб-служба забезпечує функціонування транспортного нейтрального механізму, використовуючи повідомлення SOAP для налаштування та надання послуг, у яких одна й та сама послуга може передаватися кількома транспортними протоколами HTTP, TCP тощо. Зв`язування веб-служби з HTTP забезпечує інфраструктуру прикладного рівня для розподілених служб через IP.

SaaS Adapter Framework (SAF) – проміжне програмне забезпечення для з`єднання додатків SaaS із серверними службами зв`язку. З точки зору додатків SaaS, SAF є постачальником послуг і завершує виклики веб-служб із додатків SaaS. З точки зору комунікаційних служб, SAF є клієнтом служби, оскільки він перетворює запит на службу від програми SaaS у набір нових запитів до серверних служб.

SAF надає механізм плагіна для обробки кількох служб. Це дозволяє розробникам легко розробляти та розгортати нові спеціальні сервісні адаптери для кожної нової служби. Мова виконання бізнес-процесів (BPEL) є стандартною мовою для моделювання та виконання бізнес-процесів на основі веб-сервісів; критично важлива технологія для SOA, яка забезпечує гнучке включення послуг у бізнес-транзакції, включаючи послуги зв`язку.

Спеціальна реалізація з використанням мов програмування низького рівня є ще одним підходом до перетворення та композиції служби, де взаємодія служби моделюється як виклик API функції, а інформація про стан зберігається як змінна. Обираючи композиційний підхід для комунікаційних послуг, необхідно врахувати декілька факторів, таких як:

– Ефективність. Для послуг зв`язку в режимі реального часу час відповіді має бути коротким, щоб відповідати своєчасному обмеженню, що вимагає ефективності впровадження. Механізм BPEL характеризується більшими обсягами

накладних витрат, а композиція не є такою ефективною, як її користувальницькі реалізації.

– Розширюваність. Служби зв`язку використовують розширені стандарти веб-служб, наприклад, WS-Addressing і WS-Eventing. Тому бажано, щоб підхід до композиції послуг міг підтримувати всі ці стандарти або міг бути розширеним для підтримки необхідних стандартів. Як мова оркестровки сервісів високого рівня, BPEL зосереджується на перебігу бізнес-процесів, а не на підтримці процесів нижчого рівня. Хоча додавання підтримки нового стандарту в BPEL є можливим, цей процес може бути складним і залежати від постачальника послуги. З іншого боку, незважаючи на те, що спеціальна реалізація є специфічною для конкретних програм, користувальницька реалізація яких може бути легкою та легко підтримувати необхідні стандарти за допомогою різних інструментів розробки веб-служб.

Необхідно застосувати підхід, заснований на BPEL, який можна підключити до SAF і створити за допомогою різних служб у SAF. Сервіси на SAF можуть застосувати свої низькорівневі та залежні від додатків модулі, які характеризуються спеціальним впровадженням [23, с. 179]. SAF складається з двох типів сервісних компонентів: специфічних для конкретної програми та спільних для всіх програм і служб. SAF надає загальні компоненти як вбудовані утиліти, що дозволяє розробникам зосередитися на логіці роботи служби.

Комунікаційні служби можуть реалізувати механізм сповіщення про події, щоб надсилати події назад до SAF. Для кожної служби в SAF створюється заглушка, доступ до якої можливий для всіх адаптерів. Кожен адаптер створює власний WSDL-файл служби, який описує доступні операції для програм SaaS. «Адаптер створюється на основі файлу WSDL. Адаптер реалізує композицію служби та логіку перетворення. Він викликає серверні служби через заглушки від імені програм SaaS і координує отримані відповіді відповідно до потоку композиції служби для конкретної служби. Коли завершується, кінцевий результат надсилається назад до програм SaaS. SAF надає набір стандартних стеків веб-служб, включаючи WS-Addressing і WS-Eventing, через загальний модуль WS-

*Support. Ще одним корисним компонентом є підписка на події, яка дозволяє сервісному адаптеру підписуватися на цікаві події від постачальника послуг і керувати підпискою на події (продовжити, зупинити тощо) □12, стор 3□.

Якщо сервісному адаптеру потрібно отримувати сповіщення про події від служби, він реалізує приймач подій і надає цю інформацію джерелу подій у повідомленні про підписку на події. Приймач подій реалізує складний WSDL подій, наданих джерелом подій (у більшості випадків, постачальником послуг). Підписуючись на події зі служби, адаптер служби надає розташування (URL) свого одержувача подій. При отриманні події, пов'язаної з даними програми SaaS, одержувач події повинен оновити відповідні дані в програмі SaaS, щоб відобразити наявні зміни.

Оскільки програма SaaS підтримує статус учасника обробки даних, приймач події відповідає за ініціювання зміни статусу програми, що працює на платформі SaaS або в режимі конференції. Цей процес виконується спільно модулями Event Sink, Event Mapping Rules і SaaS Data Synchronization (SDS). Правила зіставлення подій – список правил, що містять зіставлення між подіями та відповідними даними SaaS. Залежно від різних платформ SaaS, відображенням можуть бути або деякі SQL-запити, або XML-повідомлення, які використовуються для оновлення даних на платформах SaaS.

Після отримання подій від джерела події одержувач події шукає правила зіставлення для цієї події. Якщо правило не знайдено, подія відхиляється. Якщо збіг знайдено, повертається запит або шаблон XML-повідомлення. Потім приймач події заповнює шаблон інформацією, вбудованою в подію, і передає зібране повідомлення модулю синхронізації даних. SDS відповідає за оновлення даних SaaS для всіх служб. Використання модуля SaaS Login дозволяє зменшити суму понесених витрат [5, с. 2512].

SAF взаємодіє з програмами SaaS і серверними службами, а також з компонентами SAF, які взаємодіють один з одним. Коли програма SaaS ініціює запит до SAF для запуску служби конференції, адаптер служби конференції спочатку викличе операцію getSessionId служби конференції, що дозволить

адаптеру служби увійти на сервер конференції, автентифікувати себе та встановити сеанс взаємодії із сервером. Тоді SA викличе операцію підписки, щоб підписатися на події з сервера. Запит на підписку містить місце розташування події. Після цього він викличе іншу операцію для запуску конференції та забезпечить повернення відповіді-підтвердження програмі SaaS. Коли статус учасника змінюється, подія надсилається з сервера на відповідний приймач подій. Він шукає відповідне повідомлення, і якщо збіг знайдеться, повідомлення буде надіслано до SaaS через SDS. Таким чином, втілення вищезазначених вдосконалень здійснення комунікаційних задоволень дозволить підвищити рівень контролю споживача над здійсненими сеансами взаємодії з програмою SaaS.

## 2.3 Оцінка результативності застосування моделі хмарної піраміди та способу SaaS для забезпечення високого рівня захищеності великих даних в банку

В умовах сучасності банки генерують великий обсяг критично важливих даних, такі як особиста інформація, комерційні дані тощо. Згодом обсяг створених цифрових даних поглинає можливості зберігання даних в обраному банку. Саме тому слід створити необхідну інфраструктуру, таку як перевірка систем зберігання даних великої ємності. Величезна кількість додатків, які використовуються в хмарі, можуть бути використані для збереження великих даних, і одночасно можуть розглядатися як сукупність наборів даних, які є складними, що створює труднощі для збору, зберігання, аналізу та візуалізації даних за рахунок використання застарілих систем.

Для того, щоб керівництво банку змогло ефективно керувати великомасштабними центрами обробки даних і хмарними системами, оператори банку повинні спрямувати свої зусилля на освоєння програм та додатків для збереження великих даних. Однією з головних переваг обслуговування в банку є високий рівень конфіденційності та захищеності фінансової інформації своїх клієнтів. Він є відомим своєю здатністю обробляти великі суми коштів, і, як

наслідок, банк бере на себе відповідальність за забезпечення захищеності збереження конфіденційної інформації своїх клієнтів.

Конфіденційність у банку є ключовим аспектом фінансових послуг, оскільки банк дозволяє клієнтам бути впевненими, що їхня фінансова інформація обробляється з максимальною обережністю [14].

Банки працюють відповідно до принципів Кодексу етики та правил надання банківських послуг. Керівництво банку вживає низку заходів безпеки. Ці заходи включають використання захищених серверів, технологій шифрування та заходів фізичної безпеки, таких як моніторинг, системи відеоспостереження та системи контролю доступу. Крім того, існують суворі внутрішні правила та процедури, які гарантують, що співробітники пройшли навчання та усвідомлювали важливість збереження конфіденційності даних клієнтів банку.

Безпека фінансової інформації є дуже важливим напрямком діяльності банку. Керівництво банку застосовує передові заходи безпеки для захисту фінансової інформації клієнтів від крадіжок, шахрайства та кібератак. Заходи безпеки, які використовує керівництво банку, спрямовані на запобігання несанкціонованому доступу до їхніх систем та даних, що може призвести до викрадення конфіденційної фінансової інформації клієнтів банку.

Для забезпечення безпеки фінансової інформації клієнтів банку використовується ряд технологій. До них відносяться брандмауери, системи виявлення вторгнень і антивірусне програмне забезпечення. Також залучені експерти з безпеки, які постійно перевіряють свої системи на наявність будь-яких ознак порушення безпеки. Окрім технологічних заходів, керівництво банку впроваджує заходи фізичної безпеки, які включають використання камер спостереження, захищених точок доступу та залучення персоналу служби безпеки.

Керівництво банку також обмежує доступ до конфіденційної фінансової інформації лише для уповноваженого персоналу. Тому конфіденційність і безпека є двома найважливішими аспектами надання фінансових послуг, адже керівництво банку розуміє важливість захисту конфіденційної фінансової інформації своїх клієнтів. Тому активно впроваджуються передові заходи безпеки для забезпечення

достовірності конфіденційної інформації, яку клієнти надають працівникам банку.

До сфери діяльності системи управління інформаційною безпекою банку належать:

– надання послуг електронних транзакцій юридичним і фізичним клієнтам;

– видача кредитів під заставу;

– надання строкових вкладів;

– надання управлінських послуг для корпоративних клієнтів.

Банки зобов`язуються:

– забезпечити конфіденційність, цілісність і доступність наданих послуг та всю інформацію, яка зберігається у банку;

– підтримувати, керувати та постійно вдосконалювати систему управління інформаційною безпекою;

Цілями застосування системи інформаційного ступіню захищеності в банку є необхідність:

– постійно підвищувати ефективність інформаційного ступіню захищеності системи управління в реалізації Політики інформаційного ступіню захищеності банку та її цілі;

– виокремити ресурси, які є необхідними для належного функціонування інформації в системі управління безпекою;

– забезпечити ефективне управління ризиками та використання відповідних ризиків заходів управління до прийнятного рівня через проведення щорічної оцінки ризиків та реалізації плану управління ризиками;

– задовольняти потреби зацікавлених сторін, виконувати договірні зобов`язання та застосовувати вимоги до захищеності інформації;

– забезпечити підвищення компетентності та обізнаності працівників банку у системі забезпечення інформаційного ступіню захищеності;

– забезпечити основні принципи захищеності наданих послуг і всієї інформації, яка зберігається в банку;

– у разі порушення захищеності інформаційної системи слід оцінити

обсяг завданої шкоди, обмежити її наслідки та вжити необхідних заходів їх усунення, забезпечити заходи щодо організації безперервності діяльності банку;

– необхідно регулярно оновлювати цілі управління інформаційною безпекою банку, регулярно оновлювати технічні засоби, що використовуються для забезпечення інформаційного ступіню захищеності банку;

– проводити регулярні аудити управління інформаційною системою захищеності банку та усунути невідповідності, виявлені під час аудиту [17].

Політика сприяння функціонування системи інформаційного ступіню захищеності банку повинна бути доступною для зацікавлених сторін у доступній формі і залишатися зрозумілою для них. Принципи реалізації цієї політики мають періодично переглядатися, принаймні один раз на рік. Керівництво банку завжди гарантує безпеку коштів клієнтів, проте, самі клієнти банку мають подбати про безпеку збереження своїх заощаджень. Саме тому керівництво банку розробило правила, дотримуючись яких, клієнти не стануть жертвами шахраїв. До них належать наступні правила, такі як:

– уникати онлайн-угод з людьми, які використовують шахрайські прийоми;

– не прохати сторонніх людей допомогти скористатися своєю пластиковою карткою;

– не надавати персональну інформацію по телефону;

– не відповідати на дзвінки із незнайомих номерів;

– не відкривати листи із вірусами і не переходити за наданими посиланнями;

– не записувати свій PIN-код на пластиковій картці: у разі втрати або крадіжки картки сторонні особи можуть легко зняти з неї кошти;

– уважно оглянути банкомат перед використанням;

– бути завжди на зв`язку з банком;

– використовувати надійні паролі та не повідомляти їх нікому;

– оплачуючи онлайн-покупки, слід бути обережними та ніколи не розголошувати особисту інформацію;

– бути уважними, якщо надійшло SMS невідомого походження з проханням відправити отриманий код або дивний набір команд на інший номер;

– ніколи не передавати інформацію про свої картки третім особам, навіть якщо вони звертаються нібито від імені банку;

– забезпечити безпеку зберігання та використання ключів електронного цифрового підпису для бізнесу;

– використовувати додатки з дотриманням техніки захищеності;

– повідомити банк про те, що клієнт збирається використовувати картку за кордоном [16];

– блокувати картку або номер фінансового телефону в разі крадіжки або втрати;

– оновлювати свою операційну систему за допомогою останніх оновлень захищеності та виправлень;

– переглянути налаштування захищеності в Інтернеті;

– уникати використання загальнодоступних комп`ютерів або підключення до мережі, особливо під час перевірки фінансової інформації;

– захистити ноутбук та інші портативні електронні пристрої;

– регулярно очищати кеш браузера;

– створювати резервні копії особистих даних і зберігати їх у безпечному місці;

– не обирати опцію браузера для збереження імені користувача та пароля;

– перевірити автентичність веб-сайту фінансової установи, порівнявши URL-адресу та назву фінансової установи в її цифровому сертифікаті або спостерігаючи за показниками, наданими розширеним сертифікатом перевірки;

– перевіряти, чи адреса веб-сайту фінансової установи змінюється з http:// на https:// і чи з`являється піктограма захищеності, схожа на замок або ключ, коли очікується автентифікація та шифрування;

– перевіряти баланс банківського рахунку та транзакції та повідомляти про будь-які невідповідності;

– розглянути можливість використання технології шифрування для захисту конфіденційних даних;

– не встановлювати програмне забезпечення та не запускати програми невідомого походження;

– вимкнути спільний доступ до файлів і принтерів на своєму комп`ютері, особливо якщо вони мають доступ до Інтернету через кабельні модеми, широкосмугові з`єднання чи подібні налаштування;

– видалити небажані або ланцюгові електронні листи;

– друкувати та зберігати друковані копії торгових документів для подальшого використання [15].

Для забезпечення захищеності пароля та PIN-коду клієнт банку має врахувати, що:

– паролі до веб-сайтів мають містити принаймні 6 цифр або 6 буквено-цифрових символів, жодна цифра чи символ не мають повторюватися більше одного разу;

– паролі веб-сайтів не повинні базуватися на ідентифікаторі користувача, особистому номері телефону, даті народження чи використанні іншої особистої інформації;

– паролі веб-сайтів повинні зберігатися в таємниці та не розголошуватися нікому;

– паролі до сайтів необхідно запам`ятовувати і не слід їх записувати;

– паролі на веб-сайтах слід регулярно змінювати і слід уникати використання одного пароля для різних веб-сайтів, програм або служб, особливо якщо вони стосуються різних організацій;

– не дозволяти нікому зберігати, використовувати чи змінювати маркер захищеності (генератор одноразового електронного PIN-коду);

– нікому не повідомляти PIN-коди, згенеровані маркером захищеності / мобільним маркером;

– не повідомляти код розблокування мобільного маркера;

– розглянути можливість використання технології шифрування для

захисту конфіденційних даних;

– видалити небажані або ланцюгові електронні листи;

– залишатися пильними щодо кіберзлочинців.

Застосування моделі хмарної піраміди та способу SaaS для забезпечення захищеності великих даних в банку пояснюється залученням великої кількості даних клієнтів банку. Це пояснюється тим, що будь-який банк надає наступні послуги, такі як:

– здійснення преказів на картки Visa та Mastercard;

– проведення поповнення мобільного зв`язку будь-яких українських операторів;

– проведення оплати комунальних та інших послуг;

– здійснення управління картками та рахунками, як для фізичної особи, так і для підприємця;

– здійснення відкриття депозитів;

– проведення оформлення кредитів;

– здійснення купівлі квитків на поїзд, літак чи автобус;

– оформлення страховки;

– відправка міжнародних грошових переказів у будь-яку точку світу.

У практиці активно залучається онлайн-банкінг, а тому питання захищеності великих даних залишається ще й досі актуальним [17]. У банку здійснюється шифрування даних, які передаються в банк і приймаються з серверів банку. Сервіс має багаторівневу систему захищеності. Для входу в додаток необхідно ввести пароль від свого облікового запису та підтвердити авторизацію. Після введення пароля для підтвердження авторизації використовуються такі спосіби перевірки, як:

– застосування банківського дзвінка;

– прохання ввести ПІН активної картки цього банку;

– налаштування авторизації за допомогою відбитка пальця або розпізнавання обличчя.

Інформативне повідомлення про наявну вразливість має містити наступні

елементи, такі як:

– ресурс на якому знайдено вразливість;

– тип вразливості;

– вектор атаки;

– ризики від можливої реалізації вразливості;

– кроки відтворення;

– можливі шляхи виправлення бага;

– скрін-шоти / відео екрана, що підтверджують наявність вразливості та демонструючі кроки відтворення.

В якості вразливостей не приймаються наступні елементи інформаційнлї системи, такі як:

– повідомлення від сканерів захищеності та інших автоматичних систем;

– повідомлення про вразливість, засновані на версіях програмного забезпечення / протоколу без вказівки реального застосування;

– повідомлення про відсутність механізму захисту або невідповідності рекомендаціям без вказівки на реально існуючі негативні наслідки.

В додатку керівництво банку веде до розгляду послуг, може одержати дані і документи, що відображають етнічні, політичні, релігійні або ідеологічні характеристики своїх клієнтів. У особливій мірі керівництво банку зможе отримати таку інформацію документів покупців. Іноді мають місце надання неправдивої інформації. Саме тому, щоб протидіяти залучення неправдивої інформації слід реалізувати наступні дії, такі як:

– пошук джерел колекції і місцезнаходження даних, спрямованих на процесування або місцезнаходження;

– отримання додаткових відомостей про умови для отримання доступу до особистих даних, включаючи інформацію, яка є пов`язаною з третіми особами;

– здійснення персоналізованого керування персоналом об`єкта перед персоналізованим процесом [14].

За результатами оцінки впливів критичних параметрів, що стримують розвиток моделі хмарної піраміди для забезпечення інформаційного ступіню

захищеності великих даних в обраному банку показник ймовірності настання випадків втрати конфіденційних даних складає 0,38. Саме тому показник ефективності забезпечення захищеності великих даних складає 1 – 0,38 = 0,62. Очікуваний показник вірогідності проявів ризиків втрати конфіденційних даних під впливом застосування хмарної піраміди та способу SaaS має зменшитися до досягнення показника 0,24, а тому очікуваний показник ефективності забезпечення захищеності великих даних в обраному банку складе 1 – 0,24 = 0,76.

Таким чином, застосування хмарної піраміди та способу SaaS призведе до збільшення показника ефективності забезпечення захищеності великих даних на 0,76 – 0,62 = 0,14, що визначає зростання рівня інформаційного ступіню захищеності в банку на 0,14 / 0,62 * 100 = 22,58%. Отже, чисельно підтверджено, що застосування хмарної піраміди та способу SaaS дозволить обмежити прояв критичних факторів системи інформаційного ступіню захищеності банку та сприятиме клієнтів банку активно користуватися послугами, які надає банк.

Розрахуємо економічну ефективність застосування технологій рівня «Програмне забезпечення як послуга» (SaaS) в банку. Середня ціна оренди додатка SaaS складе 100 доларів на місяць за курсом 36,37 грн. / дол. Таким чином, обсяг річних витрат на оренду додатка SaaS складе 100 * 36,37 * 12 = 43 644 грн. У 2022 році середній обсяг чистого прибутку банків склав 30,25 млрд. грн., а обсяги втрат коштів з рахунків клієнтів склали 2,4 млрд. грн. За умови застосування додатка SaaS вдалося б запобігти списанню грошей з рахунків клієнтів і очікуваний рівень доходів у 2023 році склав би 30,25 + 2,4 = 32,65 млрд. грн., а з урахуванням витрат на оренду додатка SaaS обсяг річний прибутку склав би 32,65 – 0,000043644 = 32 649 956 356 грн.

Таким чином, економічний ефект від впровадження додатка SaaS склав би 32 649 956 356 – 30 250 000 000 ≈ 2,4 млрд. грн., що означає, що запровадження додатка SaaS для забезпечення даних клієнтів банку є економічно вигідним. Застосування хмарної піраміди та хмарних обчислень відіграють ключову роль для великих даних; не лише тому, що вони надають інфраструктуру та інструменти, а й тому, що цей спосіб дозволяє проводити аналіз великих даних. Хмара забезпечує

функціонування ідеальної платформи з величезною обчислювальною потужністю та ємністю для зберігання даних для обробки великих даних із великою різноманітністю, обсягом, правдивістю та швидкістю обміну.

У майбутньому хмарні обчислення та Великі дані (Big Data) стануть важливим внеском у розвиток швидкості та гнучкості надання електронних банківських послуг. Окрім зменшення поточних проблем електронного банкінгу, можна зменшити витрати, пов’язані з використанням ІТ. Було б корисно і ефективно створити основу для розуміння проблем, пов'язаних з цією сферою.

Проблеми конфіденційності даних необхідно вирішити безпосередньо перед тим, як набори даних будуть проаналізовані або доступні в хмарі. Доступність, цілісність і якість даних є найвпливовішими факторами, тоді як фактори трансформації, управління та конфіденційності є більш значущими. Відповідно, краще більше зосередитися на впливових критеріях, які можуть призвести до набагато кращого переходу та скористатися перевагами аналізу великих даних через застосування хмарної піраміди та способу SaaS.

## 2.4 Перспективи підвищення рівня ступіню захищеності великих даних в банку за рахунок застосування моделі хмарної піраміди та способу SaaS

Основною характеристикою архітектури SaaS є мультиоренда, коли один екземпляр програмного забезпечення обслуговує кількох клієнтів або орендарів. Дані кожного орендаря є ізольованими та залишаються невидимими для інших орендарів. Рішення SaaS повинні мати високу масштабованість, щоб задовольняти потреби різних користувачів. Оскільки до системи приєднується більше користувачів, архітектура повинна плавно масштабуватися, щоб задовольнити попит. Подібним чином, коли кількість користувачів зменшується, вона повинна мати можливість зменшувати масштаб охоплення.

Висока доступність є критично важливою особливістю архітектури SaaS, розробленою для забезпечення максимального часу безвідмовної роботи, що часто вимагає резервування, відмовостійкості та ефективних протоколів відновлення

після відмови. Оскільки конфіденційні дані часто зберігаються та керуються в програмах SaaS, надійні заходи захищеності є критично важливими. Архітектура захищеності цих рішень включає шифрування, безпечний контроль доступу, регулярні аудити захищеності та відповідність різним стандартам захищеності даних.

Додатки SaaS є доступними за рахунок застосування мережі інтернет [20, с. 105]. Доступними через Інтернет, що означає, що їх можна використовувати будь-де та на будь-якому пристрої з підключенням до Інтернету. Завдяки веб-інтерфейсу вони є неймовірно гнучкими та зручними для користувачів. Рішення SaaS часто надають API, які дозволяють інтегруватись з іншими програмними системами. Це є надзвичайно важливим, оскільки обраний банк використовує різні програмні засоби, і їх інтеграція може значно підвищити ефективність проведення робочого процесу.

SaaS використовує модель ціноутворення на основі передплати, тобто користувачі платять за доступ до програмного забезпечення, а не купують програмне забезпечення безпосередньо. Така модель ціноутворення робить високоякісне програмне забезпечення доступнішим для розвитку бізнесу. Однією з ключових переваг архітектури SaaS для користувачів є автоматичне додавання оновлень і нових функцій, без необхідності встановлення чи завантаження користувача.

Архітектура SaaS спрямована на забезпечення надійної якості обслуговування та безпеки, що дозволяє легко розширювати за потреби, бути доступною з будь-якого місця та постійно оновлюватися. Такий підхід надає значні переваги користувачам, особливо банку, оскільки пропонує економічно ефективні, адаптовані та прості в обслуговуванні програмні рішення.

В останні роки SaaS стає все більш популярним. Він використовує хмарні технології, що дозволяє користувачам отримувати доступ до програмних додатків і послуг на вимогу, не встановлюючи та не обслуговуючи їх на власних серверах. Цей підхід має багато переваг, включаючи нижчі витрати, більшу гнучкість і покращену масштабованість. Оскільки вибраний банк використовує додаток SaaS

для своїх потреб у програмному забезпеченні, вкрай важливо враховувати потенційні ризики кібербезпеки.

Кіберзлочинність стала проблемою для багатьох сфер, зокрема банківської. Оскільки людині потрібен лише доступ до Інтернету, за який стягується невелика плата, щоб вчинити кримінальну дію, щоб завдати величезної шкоди, більшість злочинних дій в онлайн-просторі підтримується середовищем поза групою, надаючи програмні ресурси, необхідні для здійснювати свою діяльність в оптимальних умовах. , щоб отримати пряму чи непряму вигоду, як фінансову, так і конкурентну. Наприклад, злочинна діяльність полягає в недоступності цільових систем зберігання даних користувача, діяльності, яка вимагає як апаратного простору, так і найсучасніших процесорів для досягнення бажаного ефекту, і все це налічує сотні пристроїв, а також обладнання для виконання процедур копіювання даних, що зберігаються жертвою кібератаки, для публікації чи обміну даними та інформацією, отриманими незаконним шляхом в обмін на невелику плату □8, с. 103□.

Кіберзлочинці все частіше націлюються на програми SaaS через цінні дані, які вони зберігають. Користувачі повинні знати про численні загрози, які виникають у сучасному цифровому світі. Завдяки розвитку технологій і автоматизації процесів електронні системи нещодавно стали вразливими до кібератак. SaaS означає програмне забезпечення як послугу, метод доставки програмного забезпечення, коли постачальник послуг розміщує програми та робить їх доступними для клієнтів через Інтернет. Програми SaaS, призначені для обслуговування кількох користувачів одночасно, називаються мультитенантною архітектурою та є ключовою особливістю програм SaaS. Ця структура забезпечує ефективне використання ресурсів сервера та дозволяє впорядковано розгортати оновлення або вдосконалення для всіх клієнтів одночасно.

Загрози кібербезпеці продовжують створювати серйозні виклики в сучасному цифровому середовищі. Від фішингових атак і вразливостей API до інсайдерських загроз і інцидентів з програмами-вимагачами, керівництво банку має бути пильним, щоб захистити свої конфіденційні дані та інфраструктуру. Фішинг

— це прихована тактика, яку використовують зловмисники, щоб обдурити клієнта та отримати конфіденційну інформацію від нічого не підозрюючих користувачів за допомогою соціальної інженерії. Ці злочинці можуть видавати себе за авторитетну компанію чи банк, надсилаючи електронні листи, повідомлення або веб-сайти, які виглядають справжніми та заслуговують на довіру. Потім вони запитують особисту інформацію, таку як імена користувачів, паролі, номери кредитних карток або номери соціального страхування. Наслідки успішного фішингового шахрайства є жахливими: вони призводять до крадіжки особистих даних, фінансових втрат або несанкціонованого доступу до конфіденційних даних. Дуже важливо залишатися пильним і обережним, роблячи будь-що в Інтернеті, щоб не стати жертвою цих зловмисних атак.

API (інтерфейс програмування додатків) дозволяють різним програмам взаємодіяти, а програми SaaS використовують їх для інтеграції з іншими програмними рішеннями. Однак якщо API не захищені належним чином, вони можуть стати значною загрозою кібербезпеці. Зловмисники можуть використовувати вразливості API, щоб отримати неавторизований доступ, маніпулювати даними, викликати відмову в обслуговуванні або навіть заволодіти серверами. Поширені вразливості API включають слабку автентифікацію, відсутність шифрування та неналежний контроль доступу [19, с. 183].

Інсайдерські загрози стосуються загроз кібербезпеці, які походять зсередини. Співробітник, підрядник або будь-хто інший, уповноважений на доступ до систем банку, може викликати цей тип уразливості. Інсайдерські загрози можуть бути навмисними (наприклад, співробітник продає конфіденційну інформацію конкуренту) або ненавмисними (наприклад, співробітник випадково завантажує шкідливе програмне забезпечення). Інсайдерським загрозам може бути особливо важко протистояти через рівень доступу, який мають ці особи.

Програми-вимагачі – це різновид шкідливих програм, які шифрують файли жертви. Потім зловмисник вимагає від жертви викуп за відновлення доступу до даних після оплати. Несплата викупу часто призводить до остаточної втрати або несанкціонованого розголошення даних. Фішингові електронні листи, шкідлива

реклама або відвідування заражених веб-сайтів служать засобами розповсюдження програм-вимагачів. Атаки програм-вимагачів, які в останні роки зростають, спрямовані на окремих людей.

Атаки DDoS (розподілена відмова в обслуговуванні) — це коли зловмисники надсилають великі пакети даних цільовим системам установ, підприємств або домашніх користувачів, щоб заблокувати або вимкнути їх на тривалий період часу. Для боротьби з цими загрозами постачальники SaaS і користувачі повинні впроваджувати потужні заходи кібербезпеки, включаючи шифрування даних, надійний контроль доступу, безпечні API, регулярні перевірки безпеки та навчання співробітників. Надавайте пріоритет безпеці та дотримуйтеся відповідних норм конфіденційності даних.

Витоки даних займають центральне місце, оскільки вони передбачають неавторизоване отримання конфіденційних даних, що зберігаються на платформі SaaS. Ці дані містять інформацію, що охоплює дані клієнтів, фінансові записи, інтелектуальну власність та інші конфіденційні дані, які можуть бути використані для отримання фінансової вигоди чи зловмисних цілей. Викрадення облікового запису – компрометація облікових даних користувача за допомогою фішингу або інших незаконних способів, які дозволяють зловмиснику захопити контроль над обліковим записом, сприяючи несанкціонованому доступу до конфіденційних даних і подальшому поширенню зловмисного програмного забезпечення. Ці скомпрометовані облікові записи (боти) служать інструментами для шпигунства – діяльності, що включає стеження за комунікаціями, відстеження поведінки користувачів і збір конфіденційної інформації про окремих осіб, організації чи державні установи. Крім того, зловмисник може маніпулювати даними, вносячи дезінформацію та впливаючи на прийняття рішень, використовуючи фальсифіковану інформацію на платформах соціальних мереж.

Маніпулюючи спілкуванням, зловмисники можуть викрадати конфіденційні дані або запроваджувати шкідливий вміст. Експлойти нульового дня позначають вразливості програмного забезпечення, які залишаються нерозкритими для відповідних сторін, відповідальних за їх усунення, включаючи постачальника

програмного забезпечення. Якщо вразливість залишається неусуненою, зловмисники можуть використати її, щоб негативно вплинути на рівень інформаційного ступіню захищеності збереження великих даних. Усі вищезазначені загрози кібербезпеці потребують надійних заходів захищеності для запобігання. Ці загрози включають підтримку в актуальному стані програмного забезпечення та систем, впровадження надійних заходів контролю доступу та автентифікації, проведення регулярних тренінгів із захищеності для співробітників обраного банку та впровадження комплексної стратегії захищеності. Саме тому система інформаційного ступіню захищеності збереження великих даних у банку має постійно вдосконалюватися.

Пандемія COVID-19 значно прискорила запровадження трендів віддаленої роботи, яка, як очікується, збережеться в бізнес-середовищі після пандемії. Програми SaaS зіграли вирішальну роль у цьому переході, дозволивши банкам адаптуватися та процвітати, незважаючи на труднощі. Раптовий перехід до віддаленої роботи вимагав надійних рішень для співпраці та спілкування, і програми SaaS змогли б задовольнити цю потребу. Такі інструменти, як Zoom, Microsoft Teams, Slack і Google Workspace, дозволили б командам ефективно працювати разом, незважаючи на фізичну віддаленість. Ці інструменти полегшують співпрацю в режимі реального часу, відеоконференції, обмін файлами та керування проєктами, забезпечуючи плавний перехід до віддаленої роботи.

Оскільки додатки SaaS базуються на використанні хмарних технологій та є доступними через мережу Інтернет, співробітники можуть отримати доступ до своєї роботи з будь-якого місця, будь-коли та на будь-якому пристрої з підключенням до Інтернету. З переходом до віддаленої роботи банки все більше турбуються про рівень захищеності даних. Проте, програми SaaS пропонують надійні заходи захищеності, такі як шифрування даних, автентифікація користувачів і регулярне оновлення системи захищеності, щоб гарантувати, що конфіденційні дані залишаються в безпеці навіть в процесі застосування віддаленого доступу.

Пандемія спричинила зміни в бізнес-ландшафті, зробивши програми SaaS

безцінним активом завдяки їх масштабованості, а тому керівництво банку зможе врегулювати використання програмного забезпечення відповідно до своїх потреб та інтересів плавно впроваджувати нові функції чи інструменти. Ця гнучкість дозволяє надавати банківські послуги оперативно в умовах, що швидко змінюються.

SaaS позбавляє керівництво обраного банку від необхідності підтримувати свою програмну інфраструктуру та сервери, що призводить до значної економії коштів. Це особливо допомогло під час пандемії. Програми SaaS спрощують віддалену роботу та співпрацю, забезпечують безпеку даних, пропонують гнучкість і масштабованість. У міру того, як бізнес-ландшафт змінюється, SaaS-додатки ставатимуть ще важливішими, особливо в міру того, як запроваджуватимуться дистанційні та гібридні моделі роботи. Хоча інтеграція SaaS може значно підвищити ефективність і продуктивність, важливо підходити до них із повною та сильною стратегією кіберзахищеності. Витративши час на впровадження та підтримку надійних способів захищеності, обраний банк зможе зменшити потенційні ризики та краще захистити конфіденційні дані клієнтів.

Постачальники SaaS функціонують як процесори даних, керуючи та зберігаючи особисті дані від імені своїх клієнтів, які діють як контролери даних. Постачальники SaaS повинні врахувати декілька важливих заходів протидії ризиків проявів кіберзлочинності:

– постачальники програми SaaS повинні укладати відповідні угоди про обробку даних зі своїми клієнтами, розмежовуючи відповідні обов`язки обох сторін щодо обробки персональних даних;

– для захисту особистих даних постачальники SaaS повинні впроваджувати відповідні заходи захищеності, такі як шифрування, контроль доступу, часті перевірки захищеності та плани реагування на інциденти;

– під час передачі персональних даних постачальники програми SaaS повинні надавати гарантії збереження конфіденційної інформації клієнтів.

Провайдери SaaS повинні активно інформувати своїх клієнтів щодо збереження конкретних категорій особистої інформації, яка збирається, і чітких

цілей, для яких така інформація обробляється. Постачальникам програми SaaS рекомендується активно допомагати своїм клієнтам у дотриманні прав споживачів, які включають сприяння реалізації механізмів для виконання запитів на відмову та видалення даних [10, с. 14].

Постачальники програми SaaS повинні забезпечити впровадження відповідних заходів захищеності, щоб захистити особисту інформацію та встановити відповідні процедури для реагування та повідомлення про будь-які порушення даних. Постачальники програми SaaS мають виконувати юридичні зобов`язання, зміцнюючи довіру клієнтів і демонструючи зобов`язання щодо захисту персональних даних клієнтів.

Постачальники програми SaaS, які працюють у всьому світі або надають послуги клієнтам у різних юрисдикціях, повинні знати та дотримуватися відповідних законів і норм щодо захисту даних стосовно транскордонної передачі даних, що включає впровадження відповідних заходів захищеності, проведення оцінки впливу передачі даних і забезпечення дотримання конкретних зобов`язань, таких як отримання згоди або використання затверджених механізмів захисту конфіденційних даних.

Недотримання правил передачі даних може призвести до юридичних наслідків, зокрема штрафних санкцій і шкоди репутації. Тому постачальники програми SaaS повинні бути в курсі вимог у відповідних юрисдикціях і встановити надійні механізми передачі даних для захисту конфіденційності та захищеності персональних даних під час передачі даних.

Виявлення кіберзлочинності стає все важчим, оскільки кіберзловмисники інвестують величезні суми грошей у власні мережі та інфраструктуру, а тому органи, відповідальні за боротьбу з цим явищем, реагують із запізненням. Удосконалення системи кіберзахищеності та дотримання нормативних вимог є постійним і багатогранним процесом. Провайдери SaaS можуть реалізовувати різноманітні заходи для покращення захисту системи великих даних та досягнення нормативної відповідальності за це.

Створення надійної системи управління інформаційною безпекою (СУІБ),

наприклад, на основі стандарту ISO 27001, може забезпечити комплексний підхід до управління ризиками інформаційного ступіню захищеності. СУІБ містить політики, процедури та засоби контролю для управління процесами управління інформаційними ризиками обраного банку. Слід переконатися, що все програмне забезпечення, системи та програми регулярно оновлюються та виправляються. Це може допомогти захистити від вразливостей, якими можуть скористатися кіберзлочинці.

Слід застосувати надійні заходи контролю доступу, такі як двофакторна автентифікація, контроль доступу на основі ролей і принципи найменших привілеїв, щоб мінімізувати ризик несанкціонованого доступу до конфіденційних даних і систем. Необхідно використовувати спосіби безпечної розробки, щоб зменшити ймовірність появи вразливостей захищеності у програмі SaaS. Ці заходи повинні включати використання фреймворків захищеності, проведення перевірок коду та регулярне тестування програмного забезпечення на вразливості. Слід проводити регулярні перевірки ргоботи системи. Це може допомогти виявити потенційні прогалини у програмі SaaS щодо досягнення відповідностей та виправити їх, перш ніж вони стануть проблемами.

Формулювання юридичної політики для кращого захисту залежить від контексту, який мається на увазі. Однак, враховуючи контекст кіберзахищеності та захисту даних, необхідно запровадити наступні заходи підвищення рівня ступіню захищеності великих даних в банку за рахунок застосування моделі хмарної піраміди та способу SaaS, до яких належать:

– розширення сфери дії законів про захист даних: багато юрисдикцій у всьому світі мають спеціальні закони про захист даних, проте, їх положення слід частіше вдосконалювати;

– політика управління банком повинна дозволити клієнтам видаляти свої непотрібні дані з існуючих записів, що допоможе зберегти контроль над своїми даними та може бути особливо важливим фактором в епоху цифрових технологій, коли дані можна легко копіювати та поширювати;

– щодо права на перенесення даних, то особи повинні мати право

отримувати персональні дані у структурованому, широко використовуваному та машиночитаному форматі;

– політика посилення механізму отримання згоди клієнтів повинна зобов`язувати керівництво обраного банку отримувати чітку та інформовану згоду від окремих осіб перед тим, як дані збиратимуться, використовуватимуться чи поширюватимуться;

– політика сповіщення про порушення захищеності має передбачати надання вимог керівництву банку повідомляти постраждалих осіб і відповідні регуляторні органи у разі порушення даних, адже це зможе допомогти окремим особам захистити себе від потенційної шкоди та дозволить регуляторам притягувати шахраїв до відповідальності;

– проведення обов`язкової оцінки впливу функціонування системи збереження конфіденційних клієнтів обраного банку, що зможе допомогти визначити потенційні ризики конфіденційності та вжити заходів для їх пом`якшення;

– збільшення обсягів штрафів за відповідальність фахівців обраного банку за недбалу практику обробки даних;

– введення додаткового захисту даних дітей за рахунок звернення згоди батьків на збір даних;

– застосування штучного інтелекту та машинного навчання, що вирішуватимуть унікальні проблеми конфіденційності й етики застосування хмарних технологій в банку.

Крім того, використання штучного інтелекту та машинного навчання викликає серйозні юридичні та етичні питання, наприклад, хто несе відповідальність, коли система штучного інтелекту завдає шкоди, або як запобігти дискримінації та упередженості в застосуванні його алгоритмів. Поява квантових обчислень може зробити багато поточних способів шифрування застарілими, потенційно відкривши новий кордон для упередження кібератак.

Кібербезпека має вирішальне значення для постачальників програмного забезпечення як послуги (SaaS). Не лише для захисту власної інфраструктури, але

й для захисту даних своїх клієнтів. Програми SaaS повинні активно визначати потенційні загрози, зменшувати ризики та ефективно реагувати на інциденти захищеності. Політики та правила відіграють важливу роль у захисті даних і забезпеченні дотримання стандартів захищеності. Юридичний захист можна посилити, заохочуючи прозорість, посилюючи вимоги до звітності, запроваджуючи конфіденційність даних, сприяючи шифруванню та забезпечуючи правові засоби захисту від порушень. Технологічний прогрес призведе до появи нових типів кіберзагроз і нових правових проблем. До них належать загрози для штучного інтелекту, машинного навчання, пристроїв Інтернету речей.

Юридичні та етичні наслідки цих загроз необхідно враховувати завчасно, а закони та нормативні акти слід оновлювати відповідно. Кібербезпека не є статичною сферою: у міру розвитку технологій змінюються і загрози, з якими стикаться клієнти банку. Провайдери SaaS повинні знати про нові загрози та бути готовими до них. Політики також відіграють вирішальну роль у створенні регуляторного середовища, яке сприяє безпеці, захищає права людей і сприяє інноваціям.

Проактивний підхід до кіберзахищеності, зосереджений на запобіганні, виявленні та швидкому реагуванні на загрози, може значно змінити ситуацію. Ефективний підхід до кіберзахищеності також, має передбачати проведення регулярного навчання, використання передових технологій для боротьби із загрозами, що розвиваються. Цей підхід вимагає запровадження збалансованої та комплексної стратегії, яка поєднує технології, людей, процеси.

Отже, кібербезпека та відповідне законодавство мають першочергове значення в сучасну цифрову епоху, особливо для постачальників програмного забезпечення як послуги (SaaS). Зберігаючи значний обсяг даних, обраний банк залучатимуть постачальників SaaS реалізувати вирішальну роль у збереженні захищеності, цілісності та конфіденційності цифрових активів клієнтів банку.

# 3 ЗАСТОСУВАННЯ МЕТОДИКИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ВЕЛИКИХ ДАНИХ НА ОСНОВІ МОДЕЛІ ХМАРНОЇ ПІРАМІДИ ТА СПОСОБУ SAAS

## 3.1 Архітектура способу підвищення захищеності великих даних на основі впровадження моделі хмарної піраміди та способу SaaS

Аналізуючи ключові аспекти концепції Cloud Computing та основні моделі IDS (Intrusion Detection System або Система виявлення атак) пропонується узагальнена архітектура IDS Snort та її модернізацію для використання аналітичної системи на основі концепції Cloud Computing та здатної аналізувати об'ємну інформацію про тривоги. Ця система є інтегрованою платформою управління тривогами, розгорнутою на інфраструктурі хмарних обчислень. На рисунку 3.1 представлена узагальнена архітектура системи виявлення вторгнень Snort.

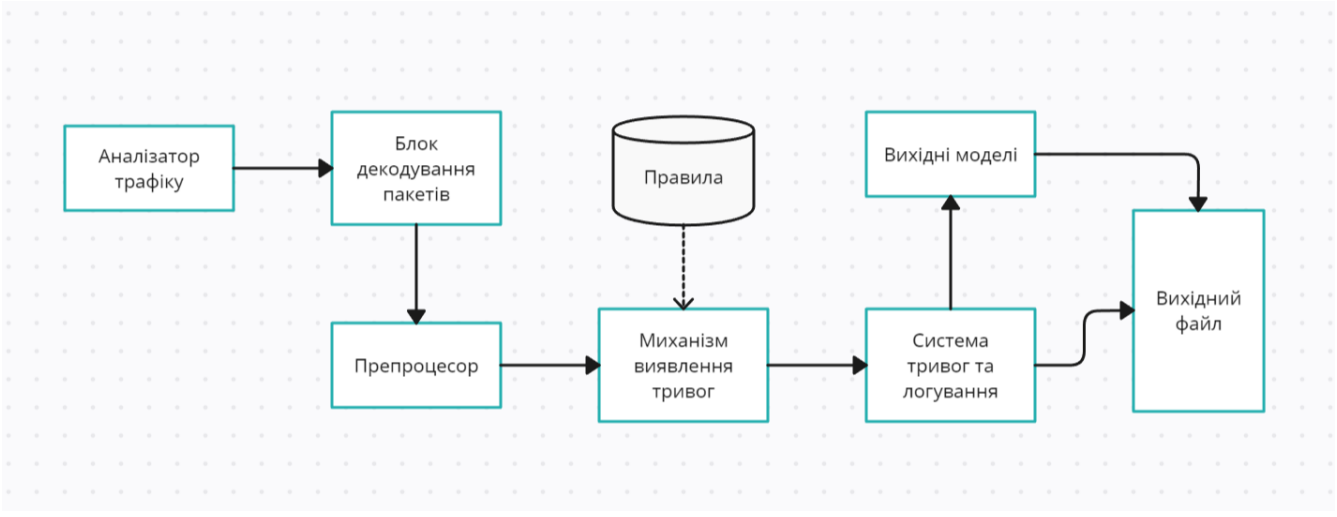



Рис.3.1. Архітектура Система виявлення атак Snort

Генератор тривог є програмним забезпеченням, призначеним для функціонування в мережі та виявлення спроб вторгнення та аналізу мережевої активності. Мета програмного забезпечення полягає в наданні оригінального

висновку у текстовому файлі. У випадку, який розглядається, цей продукт представлений системою IDS Snort. Вона володіє різноманітними функціями і дозволяє користувачеві створювати правила, а результати її роботи зберігаються у текстовому файлі.

На рис 3.2 пропонується удосконалена архітектурана на основі Cloud Computingта алгоритму MapReduce.

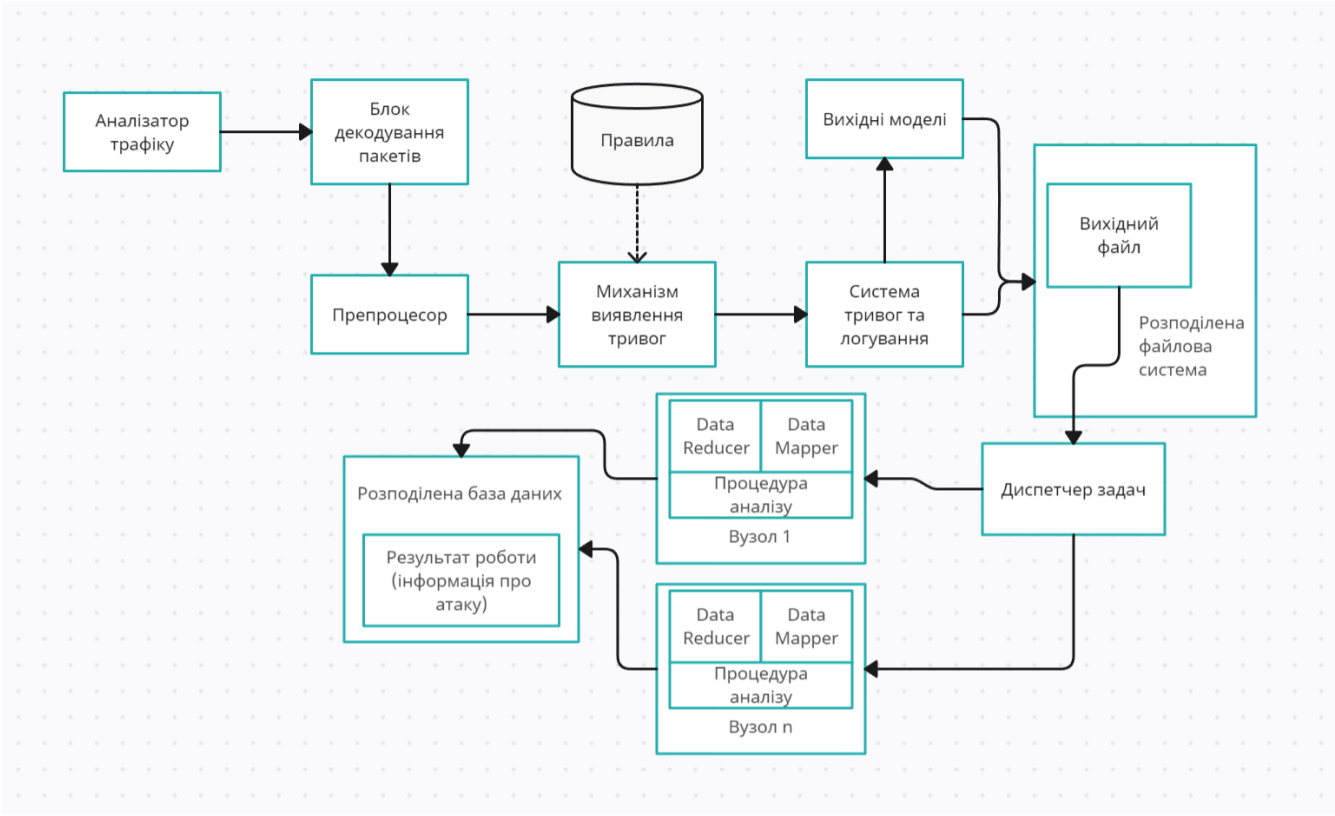



Рис. 3.2. Удосконалена архітектура системи аналізу

Платформа Cloud Computing повинна забезпечувати використання алгоритму MapReduce та підтримувати розподілені файлові системи. Прикладом такої платформи є віртуалізація двох служб Apache Java: HBase і Hadoop. Hadoop - це комбінація Tokyo MapReduce та Tokyo File System, структура, заснована на цій технології, яка підтримує обробку великої кількості інформації в кластерах. Hadoop прозоро забезпечує додатки надійністю та швидкістю операцій з даними. Hadoop реалізує обчислювальну парадигму, відому як MapReduce. Відповідно до цієї парадигми, програма розбита на велику кількість невеликих завдань, кожне з

яких може виконуватися на кожному з вузлів кластера. Hadoop також має розподілену файлову систему, яка використовується для зберігання обчислювальних даних у вузлах кластера, що забезпечує дуже високу сукупну пропускну здатність кластера. Ця система дозволяє легко масштабувати вашу програму до тисяч вузлів та петабайт даних. Apache Hadoop - написана на мові Java платформа з відкритим вихідним кодом для розподіленого зберігання та обробки великих та не пов'язаних між собою даних. Звучить складно, але зараз розберемося.

Під терміном "великі дані" розуміють інформацію, що відрізняється різноманітністю, високою швидкістю надходження та постійним зростанням обсягу, що не може бути ефективно обробленою на одному комп'ютері. Визначення "великі дані" охоплює не лише саму інформацію, а й методи її обробки, включаючи зберігання та аналіз.

Apache Hadoop дозволяє розділити великі обсяги даних (в терабайтах або петабайтах) на менші фрагменти та розподілити їх на обчислювальному кластері - групі комп'ютерів, які працюють разом як єдина система.

У випадку аналітичної обробки даних завдання розбивається між кількома робочими машинами, які паралельно виконують свої частини роботи. Це може стосуватися від одного до кількох тисяч машин. Екосистема Hadoop складається з чотирьох ключових компонентів: HDFS, YARN, MapReduce і Common, а також численних інструментів для розширення функціональності.

Yet Another Resource Negotiator (YARN) виступає як диспетчер ресурсів у системі Hadoop, керуючи вузлами кластера, плануючи їхню роботу та розподіляючи обчислювальні ресурси. YARN відстежує динамічне виділення ресурсів кластера для додатків Hadoop та контролює виконання завдань обробки, підтримуючи різні підходи до планування завдань, такі як FIFO (First In, First Out - "першим прийшов - першим пішов").

Hadoop Common представляє собою набір бібліотек та утиліт для роботи з

різними компонентами Hadoop, забезпечуючи їхню взаємодію та безпеку. Деякі утиліти включають Common Configuration для налаштування програм Hadoop за допомогою файлів XML, Common IO для роботи з різними файловими системами (наприклад, HDFS та Amazon S3) і Common Security, що включає утиліти для безпеки, такі як системи автентифікації та авторизації.

У екосистему також входить багато інших інструментів та рішень, що використовуються для розширення функціональності чотирьох основних компонентів. До них входять Pig, платформа для аналізу великих даних, яка представляє їх як потоки даних, та Hive, система управління базами даних, яка дозволяє читати та записувати масиви даних у розподіленому сховищі та використовується для SQL-подібних запитів до великих даних.

HBase - це база даних NoSQL, яка працює поверх Apache Hadoop і надає доступ до великих масивів даних в режимі реального часу як для читання, так і для запису.

Spark MLlib - це бібліотека машинного навчання для Apache Spark, яка масштабується та надає алгоритми машинного навчання. ZooKeeper - це сервіс для координації розподілених систем та їх управління. Oozie - це система планування робочих процесів для управління завданнями Hadoop.

Інформаційні вузли, або вузли обмінюються блоками інформації за допомогою протоколу блоків, що підтримується Hadoop. Вони постійно з'єднуються для балансування навантаження, контролю потоку даних та реплікації даних.

Розподілена файлова система (HDFS) є файловою системою, яка може взаємодіяти з кількома вузлами в мережі.

Диспетчер задач (MapReduce) складається з одного Трекера задач та декількох Трекерів завдань.

Для реалізації платформи CloudComputing можна використовувати розподілену базу даних HBase, яка підтримує таблиці з великою кількістю рядків

та стовпців. На рис. 3.3. представлена архітектура MapReduce.

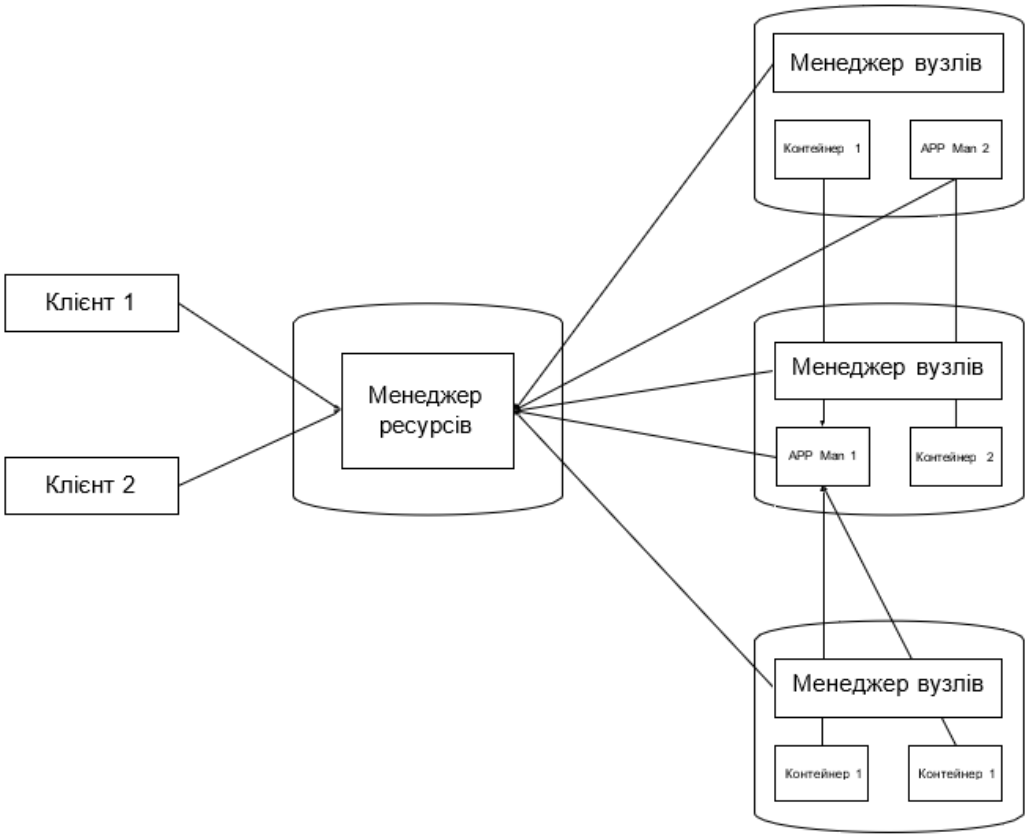



Рис. 3.3. Архітектура роботи MapReduce

MapReduce можна вважати ключовою технологією в галузі Big Data через її спрямованість на паралельні обчислення у розподілених кластерах. Основна ідея MapReduce полягає у розділенні масиву інформації на частини, обробці кожної частини паралельно на окремих вузлах, та після цього об'єднанні всіх результатів.

Програми, які використовують MapReduce, автоматично розпаралелюються та виконуються на розподілених вузлах кластера, а виконавча система бере на себе деталі реалізації, такі як розбиття вхідних даних, поділ завдань по вузлах кластера, обробка збоїв та обмін повідомленнями між розподіленими комп'ютерами. Це дозволяє програмістам легко та ефективно використовувати ресурси розподілених систем обробки великих даних.

Технологія MapReduce є практично універсальною і може бути застосована в різних областях, таких як індексація веб-контенту, підрахунок слів у великих файлах, статистика звернень до конкретної адреси, обчислення обсягу веб-сторінок

з кожного URL-адреси, побудова списків адрес з потрібними даними та інші завдання обробки великих масивів розподіленої інформації. Технологія також застосовується у розподіленому пошуку, сортуванні даних, обробці статистики логів мережі, побудові інвертованих індексів, кластеризації документів, машинному навчанні та статистичному машинному перекладі. Крім того, MapReduce успішно адаптована для багатопроцесорних систем, добровільних обчислювань, динамічних хмарних та мобільних середовищ.

MapReduce включає в себе кілька важливих характеристик:

1. Розподілене виконання операцій попередньої обробки (map) та згортки (reduce): Операції map можуть виконуватись незалежно одна від одної та паралельно на різних вузлах кластера. Кількість одночасно виконуваних функцій map обмежена джерелом вхідних даних та кількістю доступних процесорів. Аналогічно, велика кількість вузлів може виконувати згортку (reduce) після того, як кожен обробив результати функції map для конкретного значення ключа.

2. Швидкість обробки великих обсягів даних: Механізм MapReduce дозволяє ефективно опрацьовувати великі об'єми даних. Наприклад, за кілька годин ця технологія може відсортувати цілий петабайт даних.

3. Відмовостійкість та оперативне відновлення після збоїв: При відмові робочого вузла, що виконує операцію map або reduce, його робота автоматично передається іншому робочому вузлу, якщо доступні вхідні дані для операції, що проводиться. Це забезпечує високу надійність та швидке відновлення системи після можливих збоїв.

Кластер В кластері HDFS (Hadoop Distributed File System) визначені такі компоненти:

1. **NameNode (вузол імен або сервер імен)**: Єдиний у кластері, відповідає за управління простором імен файлової системи HDFS. Зберігає дерево файлів та метадані файлів і каталогів. Керує відкриттям та закриттям файлів, створенням та видаленням каталогів, керуванням доступом та відповідністю між файлами та блоками даних.
2. **Secondary NameNode (вторинний вузол імен)**: Один у кластері,

відповідає за створення резервної копії образу HDFS та логу транзакцій. Використовується для швидкого ручного відновлення NameNode у разі його виходу з експлуатації.

3. **DataNode (вузол даних)**: Багато серверів у кластері, відповідають за файлові операції та роботу з блоками даних. Виконують команди від NameNode зі створення, видалення та реплікації блоків. Здійснюють запис та читання даних та періодично надсилають повідомлення про стан (heartbeats).

4. **Клієнт (client)**: Користувач або програма, що взаємодіє через API з розподіленою файловою системою. Має право на операції з файлами та каталогами, такі як створення, видалення, читання, запис, перейменування та переміщення.

5. **HDFS**: Невід'ємна частина Hadoop, проекту верхнього рівня Apache Software Foundation та основа інфраструктури великих даних (Big Data). Використовується як розподілена файлова система загального призначення, не тільки для запуску MapReduce-задач, але і для роботи розподілених СУБД (HBase) і систем машинного навчання (Apache Mahout).

Кожен з компонентів має свою роль в забезпеченні ефективної та надійної роботи розподіленої файлової системи HDFS.

Програмний аналізатор нормалізує файли журналу тривоги IDS та передає їх для подальшої обробки. Кожен сигнал тривоги включає велику кількість параметрів, проте аналізатор виділяє лише ті, які необхідні, та передає їх для подальшої обробки.

Процедура аналізу включає два основних етапи: DataMapper та DataReducer.

**1. DataMapper:**

- Використовується для обробки вхідних даних.

- Результатом роботи DataMapper є список пар типів "ключ-значення".

- Кожен сигнал тривоги перетворюється у відповідний список пар ключ-значення.

**2. CloudComputing Framework:**

- Збирає всі пари з однаковим ключем та групує їх.

- Проводить групування в залежності від значення ключа, що спрощує подальшу обробку.

**3. DataReducer:**

- Використовується для прив'язки даних, отриманих від DataMapper.

- Результати обробки передаються до бази даних для подальшого збереження.

Цей підхід дозволяє оптимізувати та нормалізувати дані з журналу тривоги, обираючи лише необхідні параметри, і подальше зберігання та обробка їх у відповідних групах для отримання інформації, яка важлива для подальших дій чи аналізу.

## 3.2 Процедура інтеграції тривоги

Кореляція тривог Процес кореляції тривог - це аналітичний процес, який генерує звіт для мережі на основі попереджень, створених системою IDS. Різні підходи включають багатофазний аналіз послідовності тривог, і один із таких підходів виглядає наступним чином (Модель Андерсона та Вальдеса):

- Аналізує тривоги як сукупність подій низького рівня.

- Використовує дані атак та подібні метрики для об'єднання подій в одну атаку.

- Залежить від пулу вхідних даних, що включає детальний опис характеристик захищеності та пріоритетів тривоги.

Хоча існують різні способи кореляції тривог, немає єдиної думки про те, як слід визначати цей процес та як оцінювати його. Проте, Фредерік запропонував підхід до інтеграції тривожності, результати якого свідчать про високий рівень зниження швидкості.

Основні етапи поєднання тривожності визначаються на основі концепції Фредеріка, і вони включають наступне:

1. Перевірка можливості об'єднання:

- Визначення того, чи може raw-alert та meta-alert бути об'єднані.

- Перевірка співпадіння ключів та значень.

2. Перенесення відповідних тривог:

- Розпізнавання першої тривоги та переміщення її в meta-alert.

- Обробка наступних тривог відповідно до їхніх ключів та значень.

## 3.2 Інтеграція IDS в Cloud Computing

На рисунку 3.4 представлено послідовність роботи Системи Великих Даних (СВД) з аналізатором лог-файлів. Основні елементи цієї системи включають:

1. Лог-файл:
   - Файл із записами тривог, що генеруються аналізатором.
2. Regular Parser (Регулярний розбірник):
   - Компонент, який відповідає за розбір та обробку лог-файлу.
   - Виділяє необхідні параметри та інформацію з кожного запису тривоги.
3. Analysis Procedure (Процедура аналізу):
   - Здійснює аналіз відібраних параметрів та визначає, які з них потрібні для подальшої обробки.
4. Data Mapper (Карта даних):
   - Використовується для роботи з вхідними даними та створення списку пар типу

"ключ-значення".

5. Data Reducer (Редуктор даних):

- Використовується для прив'язки даних до Data Mapper.

- Результати обробки вносяться в розподілену базу даних в CloudComputing архітектурі.

6. CloudComputing Distributed Database (Розподілена база даних в CloudComputing архітектурі):

- Розподілена база даних, яка зберігає оброблені та відібрані дані від Data Reducer.

7. Мета-файл:

- Файл, який передається в розподілену файлову систему.

- Містить мета-дані та проміжні результати роботи Диспетчера задач між Data Mapper та Data Reducer.

Ця послідовність дій дозволяє СВД ефективно аналізувати та обробляти великі обсяги лог-даних, використовуючи розподілені технології та бази даних в хмарному середовищі.

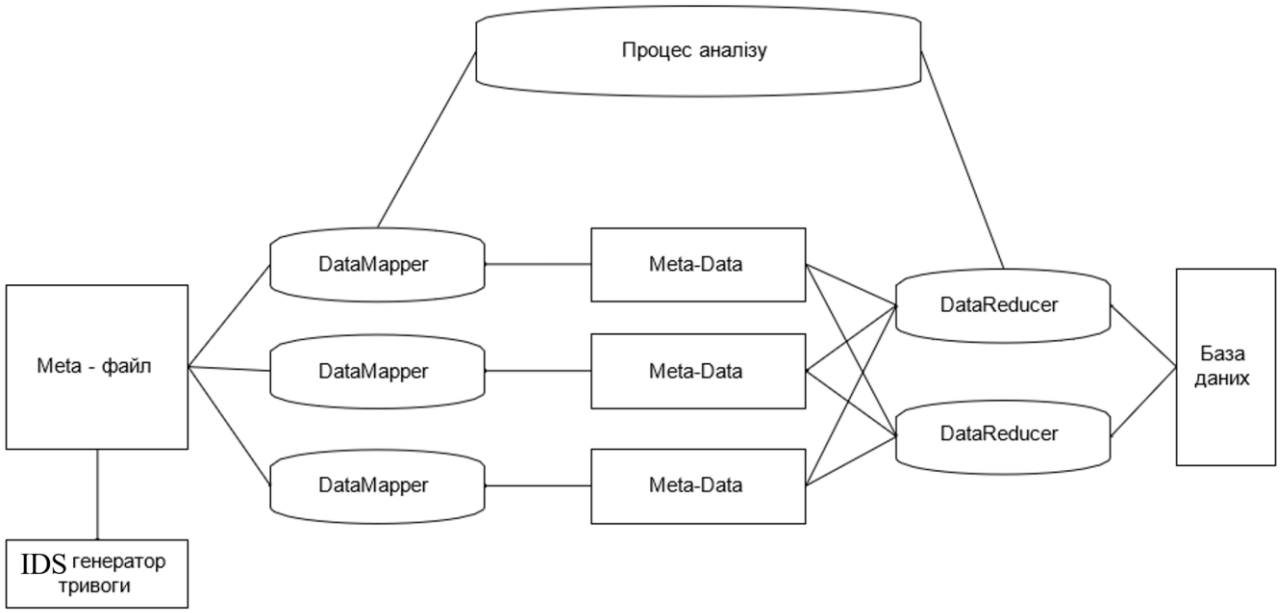



Рис. 3.4. Послідовність роботи IDS з аналізатором лог файлів

На Описаний процес аналізу та обробки тривог виявляється досить

структурованим та ефективним. Розглянемо основні етапи цієї процедури:

1. Збір тривог:

- Генератор тривоги збирає підозрілі пакети та записує інформацію у файл журналу.

2. Регулярний парсер:

- Перший компонент, який обробляє неструктурований файл журналу тривог.

- Витягує необхідну інформацію та створює базовий метафайл.

3. Відправка метафайлу:

- Метафайл відправляється до розподіленої системи для подальшої обробки.

4. Розподіл завдань:

- Диспетчер завдань запускає DataMapper та призначає завдання кожному вузлу.

5. DataMapper:

- Робить розподілену обробку даних на різних вузлах системи.

6. DataReducer:

- Зменшує надмірність та сукупну інформацію.

- Об'єднує сигнали тривог за заданими правилами.

7. Результати в базі даних:

- Оброблені та зменшені дані зберігаються у розподіленій базі даних.

Процес інтеграції тривог включає в себе виявлення та групування спільних атрибутів для об'єднання пов'язаних тривог. Такий підхід дозволяє ефективно аналізувати та виявляти зв'язки між різними тривогами, що може бути корисним для виявлення та реагування на загрози.

Таблиця 3.1

Вхідні сигнали тривоги

| ID | IP_DST | Сигнатура | Параметри |
|---|---|---|---|
| I1 | IP_1 | A | a,b |
| I2 | IP_1 | A | a,b |
| I3 | IP_2 | A | a,b |
| I4 | IP_2 | A | a,c |
| I5 | IP_3 | A | a,b |
| I6 | IP_3 | B | a,b |

Таблиця 3.2

Вихідні сигнали тривоги

| ID | IP_DST | Сигнатура | Параметри |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | 2 | 3 | 4 |
| R1 | IP_1 | A | a,b |
| R2 | IP_2 | A | a,b,c |
| R3 | IP_3 | A | a,b |
| R4 | IP_3 | B | a,c |

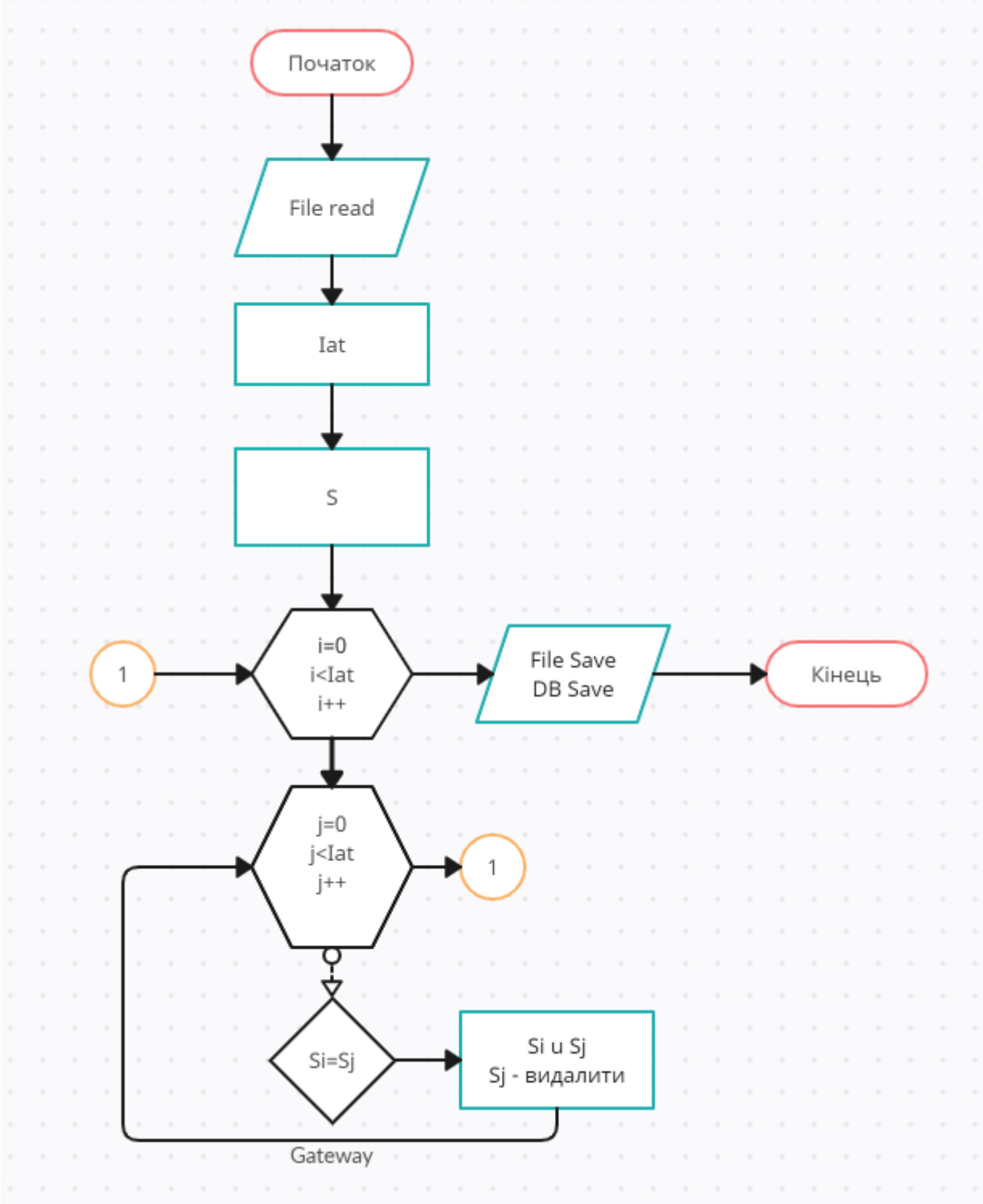



Рис. 3.6. Алгоритм роботи системи аналізу

**Iat :**

Src_ip – IP адреса джерела

Dest_ip – IP адреса призначення

Protocol – протокол

Src_port – порт джерела

Dest_port – порт призначення

Signature – ID сигнатури

Sig_name – Назва сигнатури, відповідно до ID

Sig_class_ID – ID класифікації сигнатури

Sig_priority – пріоритет

**S:**

(id, dest_ip, signature)

Створення нового формату файлів тривог виокремлює основні дані, необхідні для виявлення атак, та відкидає непотрібну інформацію, виключаючи її із нової структури (див. Таблицю 3.3).

Таблиця 3.3

Структура вхідного файлу для початку аналізу

| | |
|---|---|
| ip_dst | IP адреса призначення |
| signature | ID сигнатури, унікальне значення для ідентифікації сигнатури |
| sig_name | Назва сигнатури, відповідно до ID сигнатури |
| sig_class_id | ID класифікації сигнатури |
| sig_priority | Пріоритет сигнатури |
| ip_src | IP адреса джерела |
| ip_proto | TCP/IP протокол |
| port_dst | Порт призначення |
| port_src | Порт джерела |

Цю інформацію використається для формування нової структури.

Проводилися експерименти для отримання результатів та оцінки ефективності нашої аналітичної системи. У результаті ми отримали такі параметри: час аналізу файлів тривог та кількість отриманих сигналів тривог.

Таблиця 3.4

Результати експерименту

| Вхідна кількість тривог | Час аналізу (сек.) | | Прискорення швидкості обробки даних (сек.) |
|---|---|---|---|
| | Тестова система 1 | Тестова система 2 | |
| 280 | 1,4 | 4,1 | -2,7 |
| 380 | 1,9 | 4,2 | -2,3 |
| 440 | 2,1 | 4,2 | -2,1 |
| 750 | 3,0 | 4,8 | -1,8 |
| 1100 | 4,8 | 5,2 | -0,4 |
| 1700 | 8,6 | 5,5 | 3,1 |
| 2100 | 15,5 | 5,9 | 9,6 |
| 3390 | 19,6 | 6,5 | 13,1 |
| 5815 | 381,1 | 7,1 | 374 |
| 6340 | 390,5 | 8,3 | 382,2 |
| 12670 | 680,3 | 9,5 | 670,8 |

Основна відмінність між цими системами полягає у типі архітектури - централізованій та розподіленій. Ще однією значущою різницею є те, що Snort дозволяє генерувати записи в базу даних MySQL безпосередньо і отримувати результати з неї, тоді як у нашій системі результати надходять із системи, яка отримує їх безпосередньо з лог-файлу Snort.

З результатів (див. табл. 3.4) чітко випливає, що Тестова система 1 є ефективною, коли кількість тривог для обробки не перевищує 1100, проте цей метод вимагає значно більше часу, якщо кількість тривог перевищує 5000. У нашій системі для виконання аналізу потрібно лише 4-9 секунд. Важливо відзначити, що використання більшої кількості екземплярів дозволить ще швидше обробляти інформацію. Однак, якщо кількість тривог менше 1000, наша система вимагатиме значно більше часу, ніж традиційна. Це пов'язано з тим, що велика кількість обчислювальних вузлів вимагає більше часу для синхронізації та обміну даними між ними.

# ВИСНОВКИ

В роботі було викладено методику підвищення ступіню захищеності великих даних в банку на основі впровадження моделі хмарної піраміди та способу SaaS та визначено економічну ефективність, яка пов’язана із застосуванням цієї методики.

Оскільки програми надаються як послуги, зменшується кількість ресурсів, що споживаються, а також підвищилась швидкодія програм.

Також на базі цієї методики були запропоновані та реалізовані наступні рішення.

1. Аналітика в галузі ризик-менеджменту та забезпечення вимог регуляторів. Для епізодично здійснених аналітичних розрахунків потрібні більші обсяги вичислень. Зачастую їх розумно виробляти не на власній серверній площадці, а у зовнішньому «облаці» — таким чином банк позбавляється від необхідності придбати додаткову IT-інфраструктуру та зменшує навантаження на вже наявну. Як показує світовий досвід, перенос розрахунків моделей ризиків або ценоутворення в «облаці» дає великий економічний ефект. Розуміється, ці розрахунки можуть виконуватися і в гібридному «облаці», у цьому випадку можуть бути задіяні за необхідності, зовнішні ресурси.

2. Аналіз даних про ринки. Багато банків збирають і аналізують зовнішні (публічні) дані про стан цікавлять їх ринків. Оскільки ці дані отримані з відкритих джерел і не містять конфіденційних сведень, але при цьому включають більші обсяги інформації, тому зберігати та аналізувати їх зручніше всього в «облаці».

3. Аналіз внутрішніх даних і підготовка звітності. Крім того, у банків не завжди є можливість задіяти для вирішення цих завдань власні серверні потужності — хоча тому, що вони можуть бути зайняті виконанням критично важливих для бізнесу банку, і запуск додатків аналітичних завдань на цих же серверах може призвести до серйозного уповільнення фінансових транзакцій.

4. Аналітика, яка примзначена для запобігання шахрайським операціям. Користуючись облачними сервісами, банк може ефективно аналізувати клієнтські дані, визначати типові сценарії поведінки та у разі виявлення нестандартних сценаріїв сигналізувати про них, як про потенційно шахрайські. При виявленні

явно шахрайських схем аналітичний облачний сервіс може подати сигнал тривоги. Також хмарні сервіси використовуются для аналізу відео та розпізнавання осіб.

5. Аналіз поведінки клієнта. Хмарні сервіси машинного навчання (Machine Learning), такі як Microsoft Stream Analytics і HD Insight, допомагають досліджувати поведінку клієнтів, висунути гіпотези, а потім перевірити їх на достовірність. Наприклад, раннє виявлення тенденції до того, що клієнт покине банк, дасть можливість вчасно прийняти заходи щодо його утримання.

6. Трейдинг. Банкам, активно розвиваючим трейдинговий бізнес, необхідно дуже швидко, в режимі реального часу, аналізувати більші потоки даних про поточний стан ринку, зводки біржових новин, повідомлення новинних лент і пр. Для цього розумно використовувати обласні ресурси, тим самим знизивши навантаження не тільки на власні сервери банку, але і на його телекомунікаційні канали.

7. Сервіси для мобільних пристроїв і сайтів. Хостинг сайтів, управління мобільними пристроями, доставка контенту на зовнішні пристрої — для вирішення цих завдань вигідно використовувати публічні сервіси. Найбільш ефективна схема — розміщення в «хмарі» сайту, орієнтованого на обслуговування розничних клієнтів. Це звільнює банк від клопоту із забезпеченням достатньої пропускної здатності телекомунікацій, резервуванням потужностей на випадок пікових навантажень і т.д.

Завдяки застосуванню хмарної піраміди був забезпечений високий рівень безпеки даних, який у декілька разів вищий, ніж попередні рішення. Також стало можливим збільшення швидкості обробки данних, оскільки використовувались розподілені хмарні обчислення. Завдяки таким обчисленням ефективність обробки великих даних піднімається на якісно новий рівень, і це дозволяє обробляти величезні обсяги даниз швидко та без великих затримок.

Також завдяки хмарный піраміді та SAAS стало можливим підвищити швидкість виконання резервного копіювання та відновлення даних.

Також був проведений експеримент, який підтвердив прискорення швидкості обробки даних під час розподілених хмарних обчислень.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Akter S., Michael K., Uddin M. R., McCarthy G., Rahman M. Transformation of business with the help of digital innovations: the use of artificial intelligence, blockchain, cloud and data analytics. *Ann Opera*. 2020. № 308, P. 7–39.

2. Corbett C. J. How sustainable is big data? *Opera producer driver*. 2018. № 27, P. 1685–1695.

3. Georgakopoulos D., Papazoglou M. P., Eric Yu Service-oriented computing. *Cooperative Information Systems*. 2022. № 7, P. 210–212.

4. Gupta H., Sharma S. Security challenges in implementing the internet of things for smart network. *Communication Systems Of Network Technologies.* 2021. № 18, P. 761–765.

5. Hajiheidari N., Delgosha M. S., Wang Yu. Researching the ways of success implementation of big data analytics in banking and financial services: comprehensive approach. *Individual Management Data System.* 2021. № 121, P. 2498–2529.

6. Hassani H., Huang X., Silva E. Big data-based banking blockchain. *Joint Management Analitics.* 2018. № 5, P. 256–275.

7. Hasan M., Popp J., Olah J. The current landscape and impact of big data on finance. *Joint Big Data*. 2020. № 7, P. 21.

8. Huang M., Liu A., Xiong N. N. Effective service-oriented architecture network management for 5G-enabled IoT. *Computer Networks*. 2020. № 173, P. 107–108.

9. Hung J. L., He V., Shen J. Big data analytics for supply chain relationships in banking. *Industrial Sign Driver*. 2019. № 86, P. 144–153.

10. Jangjou M., Sohrabi M. K. A comprehensive study of security problems on various network layers in cloud computing. *Computer Methods Engineering.* 2022. № 7, P. 1–22.

11. Khraisat A., Gondal P., Vamplew P. Hybrid intrusion detection system, based on a stacked ensemble of epy decision tree classifier and a single machine class support vector. *Electronics.* 2020. № 9, P. 173.

12. More R., Moily Y. Big data analysis in the banking sector. *International Joint New Technology.* 2021. № 11, P. 1–5.

13. Ngo J., Hwang B. G., Zhang C. Factor-based big data and evaluation tool opportunities of predictive analytics for the industry. *Automatic Construction.* 2019. № 110, P. 103–142.

14. Privacy notice. URL: https://www.cdprojekt.com/en/wp-content/uploads-en/2018/05/klauzula-informacyjna_rekrutacja_en.pdf (application date: 30.11.2023).

15. Premium Banking. URL: https://raiffeisen.ua/premium/pro-premium/premium-banking (application date: 30.11.2023).

16. Risk of banking activity. URL: https://corporatefinanceinstitute.com/resources/career-map/sell-side/risk-management/major-risks-for-banks/#:~:text=Major%20risks%20for%20banks%20include,required%20to%20follow%20government%20regulations (application date: 30.11.2023).

17. Security measures when using banking products. URL: https://www.bankinfosecurity.com/5-essentials-banking-security-in-tough-times-a-1074 (application date: 30.11.2023).

18. Shakya S., Smys S. Big data analytics for improved risk management and segregation customers in banking applications. *ISMAC.* 2021. № 3, P. 235–249.

19. Tripathi B. S., Gupta R., Reddy S. R. Training kit platform base cloud architecture for education and research – survey and implementation. *Ubiquitous Networking.* 2021. № 147, P. 172–185.

20. Wang L. C., Chen C. C., Liu J. L. Structure and deployment of an advanced cloud-based planning and scheduling system. *Robotics and Computer-Integrated Production.* 2021. № 70, P. 102–188.

21. Yangui S., Goscinski A. The future generation of service-oriented computing systems. *Future Generation Computer System.* 2021. № 118, P. 252–256.

22. Zhang G., Ravishankar M. N. Exploring the capabilities of providers in the cloud environment: a case study of Alibaba cloud computing. *Information Management.* 2019. № 56, P. 343–355.

23. Zhu X., Young Y. Big data analytics to improve financial performance and stability. *Joint System Science Information.* 2021. № 9, P. 175–191.

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
# (Презентація)

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення

## МАГІСТЕРСЬКА РОБОТА

## «РОЗРОБКА МЕТОДИКИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ВЕЛИКИХ ДАНИХ БАНКІВСЬКОЇ СИСТЕМИ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ»

Виконав: студентка групи ПДМ-62, Юрченко Марія Юріївна

Керівник: к.т.н., доцент, доцент кафедри ІПЗ Негоденко Олена Володимирівна

Київ – 2023

## МЕТА, ОБ'ЄКТ, ПРЕДМЕТ ДОСЛІДЖЕННЯ



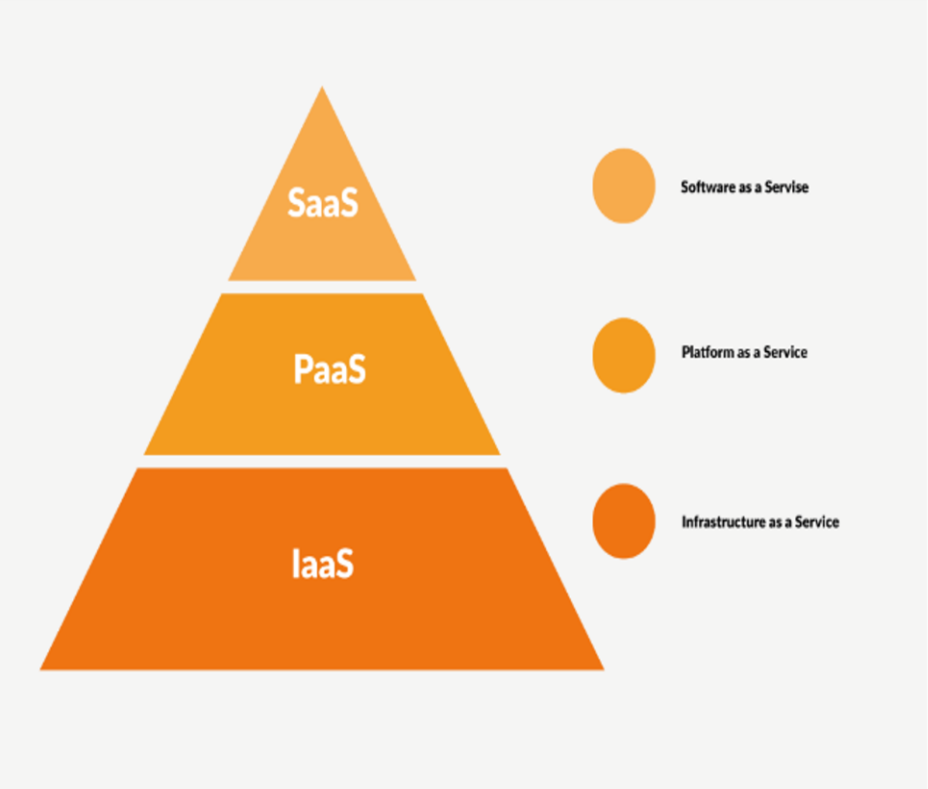
**Мета роботи**: підвищення захищеності великих даних банківської системи за рахунок застосування методу SaaS.

**Об'єкт дослідження:** захист інформаційної безпеки великих даних в банківській діяльності.

**Предмет дослідження**: хмарні технології для підвищення рівня захисту великих даних в банківській діяльності.

3

# Аналіз рівнів хмарної піраміди




4

## Аналіз існуючих моделей захищеності даних а банківський сфері: Порівняння Хмарної піраміди

| Характеристика | IaaS (Infrastructure as a Service) | PaaS (Platform as a Service) | SaaS (Software as a Service) |
|---|---|---|---|
| Рівень Контролю | Високий | Середній | Низький |
| Основний Фокус | Інфраструктура | Розробка додатків | Готовий продукт |
| Управління Операційною Системою | Користувач | Платформа | Постачальник послуг |
| Управління Додатками | Користувач | Користувач | Постачальник послуг |
| Масштабованість | Висока | Висока | Стандартизована |
| Час Впровадження | Середній | Низький | Низький |
| Витрати | Високі | Середні | Низькі |
| Захищеність Даних | Залежить від Користувача | Залежить від Користувача | Обов'язок Постачальника |
| Доступ та Оновлення | Вимагає наявності ПО; користувач відповідає за оновлення | Надаються засоби для розробки та деплойменту; користувач відповідає за розробку | Доступ лише через Інтернет; автоматичні оновлення та немає необхідності в ручних втручаннях користувача |
| Легкість Використання | Вимагає інсталяції та конфігурації; може знадобитися управління операційною системою | Спрощений процес розробки; вимагає налаштування та деплойменту додатку | Простий доступ через браузер; немає необхідності встановлення; |
| Відповідальність за Інфраструктуру | Користувач | Постачальник послуг | Постачальник послуг |
| Відповідальність за Оновлення | Користувач | Користувач | Постачальник послуг |
| Відповідальність за Захищеність Даних | Користувач | Користувач | Постачальник послуг |
| Відп. за Центр Обробки Даних | Користувач | Користувач | Постачальник послуг |
| Автоматизація Організації | Висока | Середня | Висока |

5

## Математична модель хмарної піраміди та методу SaaS

$$\Sigma = (v_0, R, T)$$

- $v_0$ – початковий стан системи;
- $R$ – множина прав доступу до об`єктів;
- $T$ – функція переходу, що переміщує систему з одного стану в наступний при виконанні запитів;

Формули та функції для оцінки рівня безпеки:

1. $\forall s \in S, \forall o \in O, r \in M[s,o] \rightarrow F(o) \leq F(s)$ **- Безпека за читанням**
   - S – Множина суб'єктів
   - O – Множина об'єктів
   - M [s, o] – Множина прав доступу для пари суб'єкт-об'єкт
   - F (s) – Рівень безпеки суб'єкта s
   - F (o) – Рівень безпеки об'єкту o
   - r – Роль r визначає, які дії або операції суб'єкт може виконувати щодо об'єкта
2. $\forall s S, \forall o \in O, w \in M[s,o] \rightarrow F(s) \leq F(o)$ **- Безпека по запису**
   - $w$ – Дія запису $w$ (наприклад, дозвіл на запис)

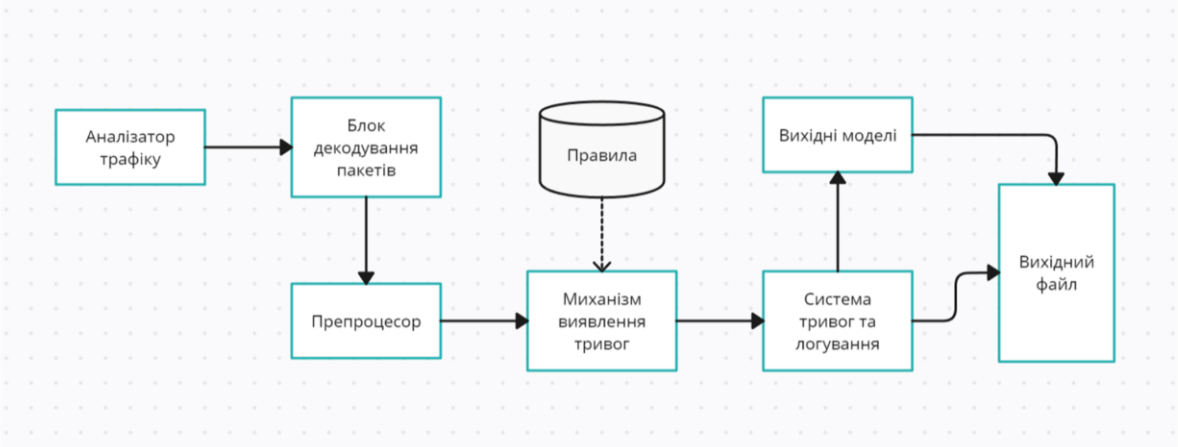
6

## Оцінка критичних параметрів обмежень застосування методу SaaS для забезпечення безпеки великих даних

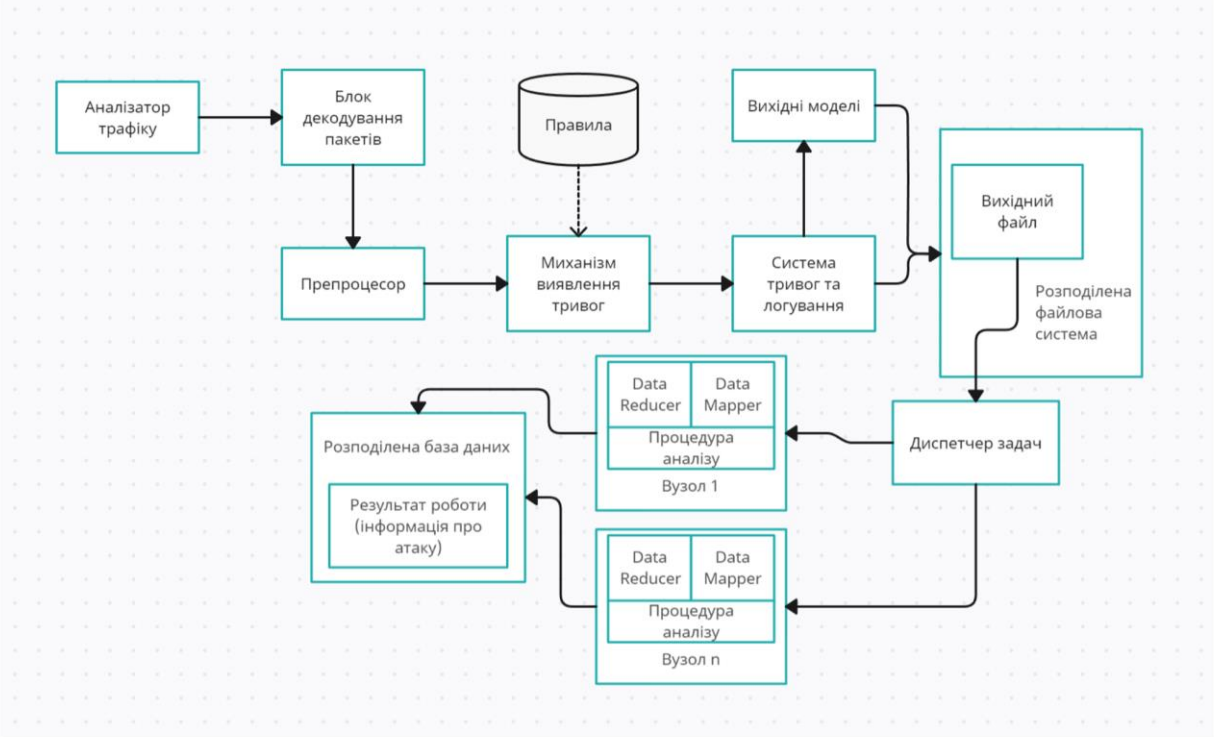
| Назва критичного параметру | Частота проявів | Ваговий критерій, балів із 10 | Сукупна оцінка |
|---|---|---|---|
| Зловживання та нечесне використання хмарних обчислень зловмисникам | 0,01 | 1 | 0,01 |
| Вразливі місця спільних технологій | 0,02 | 2 | 0,04 |
| Втрата / витік даних | 0,03 | 2 | 0,06 |
| Викрадення облікових записів, служб і трафіку | 0,04 | 3 | 0,12 |
| Застосування невідомого ризику профілю | 0,05 | 3 | 0,15 |
| Всього | | | 0,38 |

7

## Архітектура система виявлення атак Snort



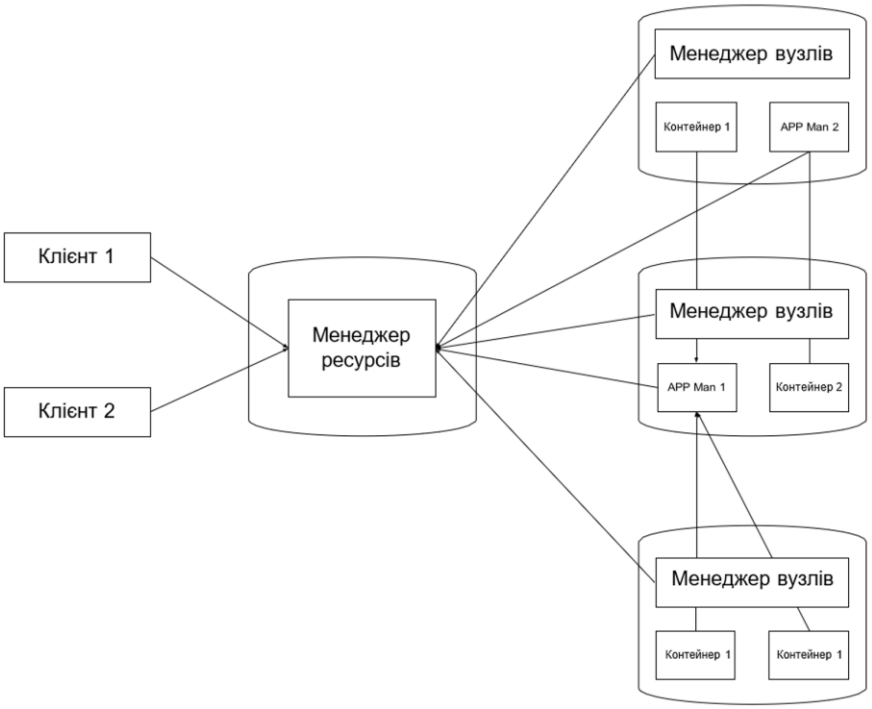

## Удосконалена архітектура системи аналізу




8

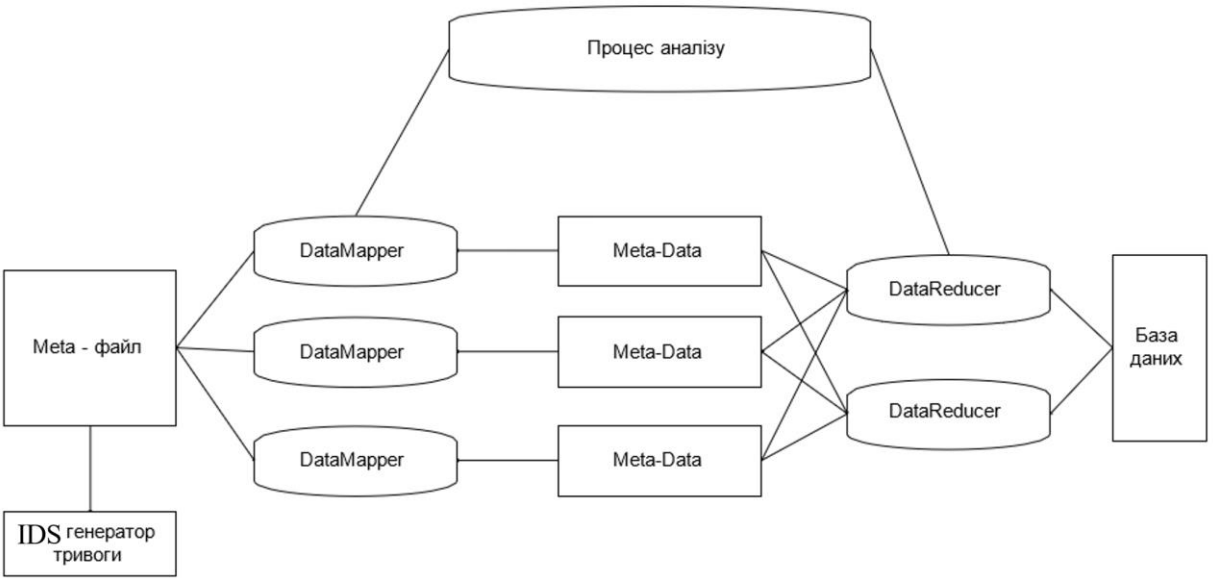
9

## Архітектура роботи MapReduce



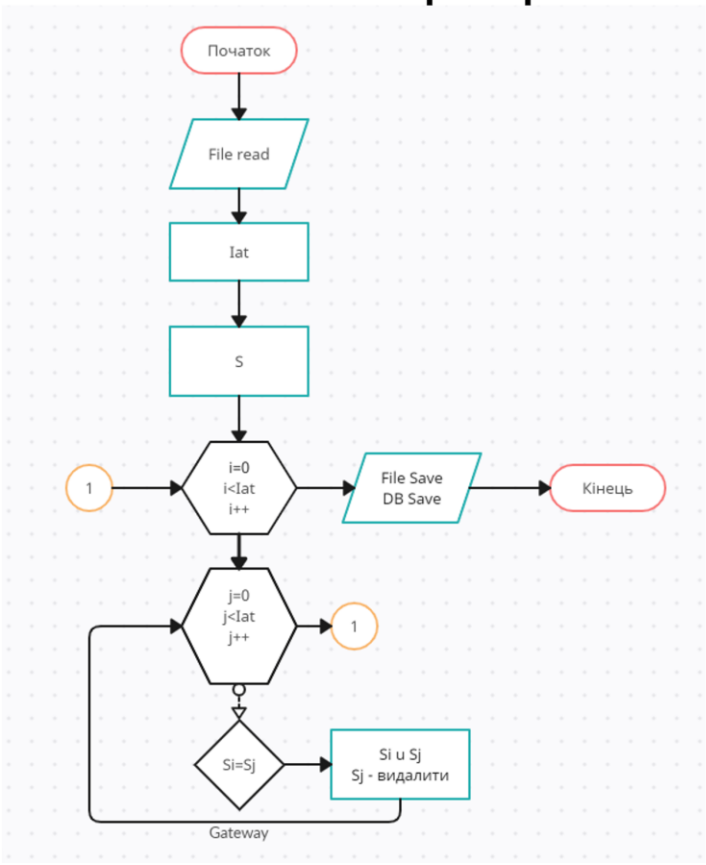

## Послідовність роботи IDS з аналізатором лог файлів

10



11

## Алгоритм роботи системи аналізу




**Iat :**

Src_ip – IP адреса джерела

Dest_ip – IP адреса призначення

Protocol – протокол

Src_port – порт джерела

Dest_port – порт призначення

Signature – ID сигнатури

Sig_name – Назва сигнатури, відповідно до ID

Sig_class_ID – ID класифікації сигнатури

Sig_priority – пріоритет

**S:**

(id, dest_ip, signature)

12

## Результати експерименту

| Вхідна кількість тривог | Час аналізу (сек.) | | Прискорення швидкості обробки даних (сек.) |
|---|---|---|---|
| | Тестова система 1 | Тестова система 2 | |
| 280 | 1,4 | 4,1 | -2,7 |
| 380 | 1,9 | 4,2 | -2,3 |
| 440 | 2,1 | 4,2 | -2,1 |
| 750 | 3,0 | 4,8 | -1,8 |
| 1100 | 4,8 | 5,2 | -0,4 |
| 1700 | 8,6 | 5,5 | 3,1 |
| 2100 | 15,5 | 5,9 | 9,6 |
| 3390 | 19,6 | 6,5 | 13,1 |
| 5815 | 381,1 | 7,1 | 374 |
| 6340 | 390,5 | 8,3 | 382,2 |
| 12670 | 680,3 | 9,5 | 670,8 |

## ВИСНОВКИ

13

1. Проведено аналіз застосування моделі хмарної піраміди та методу SaaS для оцінки рівня інформаційної безпеки даних в банку. Встановлено, що модель хмарної піраміди та метод SaaS ефективно впливають на підвищення рівня інформаційної безпеки в банківському секторі. Вони дозволяють банкам гнучко реагувати на зміни у вимогах безпеки та забезпечувати надійність захисту даних.
2. Побудовано модель хмарної піраміди за рахунок застосування методу SaaS для оцінки забезпечення інформаційної безпеки великих даних в банку.
3. Проведено оцінку критичних параметрів, що стримують розвиток моделі хмарної піраміди для забезпечення інформаційної безпеки великих даних в банку. Встановлено, що ефективний розвиток моделі хмарної піраміди для забезпечення інформаційної безпеки великих даних вимагає уваги до деталей, таких як стійкість до атак, гнучкість та адаптація до банківських стандартів безпеки.
4. Розроблено методику підвищення захищеності великих даних на основі впровадження моделі хмарної піраміди та методу SaaS, яка дозволяє реалізувати інноваційні підходи до захисту конфіденційної інформації та оптимізації роботи з даними клієнтів.
5. Проведено оцінку результативності застосування моделі хмарної піраміди та методу SaaS для забезпечення високого рівня захищеності великих даних. Завдяки застосуванню хмарної піраміди був забезпечений високий рівень безпеки даних, який у декілька разів вищий, ніж попередні рішення. Також стало можливим збільшення швидкості обробки данних, оскільки використовувались розподілені хмарні обчислення. Завдяки таким обчисленням ефективність обробки великих даних піднімається на якісно новий рівень, і це дозволяє обробляти величезні обсяги даниз швидко та без великих затримок.

## АПРОБАЦІЯ РОБОТИ

14

### Тези доповідей:

1. Негоденко О.В., Юрченко М.Ю. Застосування моделі хмарної піраміди та методу Saas для підвищення рівня захищеності великих даних. Журнал “Зв’язок”

15

# ДЯКУЮ ЗА УВАГУ!