**ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЕКОНОМІКИ, УПРАВЛІННЯ, ПРАВА ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**
**КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ**

# Пояснювальна записка

до кваліфікаційної роботи на здобуття ступеня вищої освіти магістр

на тему: «**Моделювання цілісності даних та забезпечення безпеки інформаційної системи підприємства**»

Виконав: здобувач вищої освіти
за освітньо-професійною програмою
Інформаційні управляючі системи та технології
спеціальності 126 Інформаційні системи та технології
освітнього ступеня магістр
групи 126ІСТ_мд_22
Омельяненко В.М.
Керівник: Поночовний Ю.Л.
Рецензент: Брикун О.М.

**Полтава – 2023 року**

# ВСТУП

В сучасному світі, де інформаційні технології займають важливе місце в функціонуванні підприємств, забезпечення цілісності даних та безпеки інформаційної системи стає критичною задачею. Зростання обсягів та складності даних, а також збільшення кількості загроз та атак на інформаційні ресурси підприємств вимагають вдосконалення та розвитку методів моделювання цілісності даних і впровадження ефективних заходів забезпечення безпеки.

*Актуальність дослідження* визначається необхідністю постійного вдосконалення стратегій та методів управління інформаційною безпекою на підприємствах у сучасному інформаційному середовищі. Зміни у технологічному ландшафті, зростання кількості кіберзагроз та постійне еволюційне вдосконалення атак вимагають постійного адаптивного реагування в сфері захисту даних.

Підприємства стикаються з викликами забезпечення цілісності даних та ефективного функціонування інформаційних систем у зростаючому векторі кіберзагроз. Дослідження в даній області набуває стратегічного значення, оскільки дозволяє розробляти передові стратегії та технічні рішення, необхідні для протидії сучасним загрозам.

*Зв'язок роботи з науковими програмами, темами.* Робота відповідає дослідженням в межах науково-дослідної роботи «Розвиток підприємництва: управлінські, економічні, інноваційна та правові аспекти» відповідно до договору №9 від 15.05.2023 р. між ТОВ «ПАФ Гарант» та Полтавським державним аграрним університетом (розділ «Обґрунтування показників оцінювання гарантоздатності розподілених інформаційних систем»).

*Мета кваліфікаційної роботи* полягає в створенні комплексного підходу до забезпечення цілісності даних та безпеки інформаційної системи, що дозволить підприємствам ефективно протистояти сучасним викликам та загрозам в галузі інформаційної безпеки.

*Завданнями* кваліфікаційної роботи є:

– аналіз розвитку інформаційних систем підприємств та вимог до їх інформаційної безпеки;

– моделювання цілісності даних інформаційної системи підприємства;

– моделювання забезпечення безпеки інформаційної системи підприємства.

*Об'єкт дослідження* – процеси функціонування інформаційної системи підприємства в умовах атак на цілісність даних її компонент.

*Предмет дослідження* – моделі цілісності даних та забезпечення безпеки інформаційної системи.

*Методи дослідження*, які були використані в кваліфікаційній роботі ґрунтуються на використанні методів теорії ймовірності, системного та марковського аналізу. Марковський аналіз став основою для моделювання стохастичних процесів у контексті готовності інформаційного ресурсу та розробки моделі оцінювання готовності інформаційної системи на підприємстві.

*Інформаційна база* кваліфікаційної роботи складається з наукових статей, міжнародних аналітичних видань і звітів, матеріалів наукових конференцій інтернет-ресурсів, що місять інформацію про архітектуру сучасних інформаційних систем, а також даних, отриманих від провідних IT-компаній у сфері забезпечення цілісності даних та кібербезпеки.

*Елементи наукової новизни* полягають у розроблені та досліджені аналітичної моделі функціонування інформаційної системи в умовах атак на цілісність даних для забезпечення її безпеки.

*Практична значущість* роботи полягає в можливості повторного застосування та модифікації розробленого програмного коду моделі для оцінювання показника готовності інформаційних систем в умовах атак на цілісність даних, конфіденційність та доступність. Отримані результати можуть бути корисними для IT фахівців при моделюванні спеціалізованих інформаційних управляючих систем. Отримані результати мають велике значення для підприємств, які прагнуть забезпечити надійність та безпеку своїх інформаційних систем, сприяючи підвищенню конкурентоспроможності та стійкості в умовах сучасного інформаційного середовища.

*Апробація результатів* дослідження відбувалася шляхом оприлюднення доповідей на наукових конференціях, семінарах.

*Публікації.* За результатами проведеного дослідження опубліковано тези: «Аналіз засобів захисту конфіденційних даних системи управління підприємством в СКБД MySQL», Матер. Міжнародної науково-практичної конференції, 28 вересня 2023 р. м. Полтава; «Застосування методів та технологій для забезпечення безпеки баз даних в сучасному цифровому світі», Матер. науково-практичної конференції за підсумками виробничої практики здобувачів вищої освіти спеціальності «Інформаційні системи та технології», 17 вересня 2023 р., м. Полтава; «Забезпечення безпеки та цілісності даних в інформаційних системах підприємств», Матер. Міжнародної наукової конференції, 4-6 жовтня 2023 р., м. Львів.

*Структура та обсяг кваліфікаційної роботи* логічно пов'язані з задачами досліджень. Робота містить перелік умовних позначень, вступ, три розділи основної частини, висновки, список використаних джерел, додатки. Загальний обсяг текстової частини дипломної роботи складає 65 сторінок формату А4. Вона містить 18 рисунків і 5 таблиць. В роботі використано 48 науково-технічних джерел.

# РОЗДІЛ 1
# АНАЛІЗ РОЗВИТКУ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВ ТА ВИМОГ ДО ЇХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 1.1 Розвиток інформаційних систем від локальних до хмарних рішень

В сучасному світі швидко зростає роль інформаційних технологій, що супроводжується постійним вдосконаленням систем, які їх використовують. Однією з ключових тенденцій є перехід від локальних інформаційних систем до хмарних рішень. Аналіз цього процесу дозволяє зрозуміти переваги та виклики, які супроводжують цю зміну [1].

На початковому етапі розвитку підприємства використовували локальні інформаційні системи. Вони відіграли ключову роль на початковому етапі розвитку підприємств. Це були внутрішньо-організаційні рішення, які працювали на місцевих серверах. Вони були досить обмеженими у плані масштабування та гнучкості. Робочі процеси були локалізованими, а доступ до даних обмежувався фізичним розташуванням обладнанню [2].

Основними характеристиками локальних інформаційних системах є:

– внутрішньо–організаційні рішення;

– повний контроль над інфраструктурою;

– застосовується для внутрішніх потреб підприємства.

Перевагами локальних інформаційних системах є:

– безпека даних – локальні системи забезпечують високий рівень безпеки, оскільки дані зберігаються в межах внутрішньої мережі;

– контроль – в локальних системах мають повний контроль над обладнанням та програмним забезпеченням.

Недоліками локальних інформаційних системах є:

– обмежена гнучкість – обмежена гнучкість доступу до даних;

– високі витрати – великі витрати на обладнання, обслуговування та оновлення.

Для подолання обмежень локальних систем були введенні клієнт-серверні та розподілені системи. Ці моделі дозволяли розміщувати частину функціоналу на клієнтських комп'ютерах, спрощуючи завдання серверів та покращуючи ресурсне використання. Однак ці системи вимагали складного адміністрування та можливості виникнення проблем з безпекою даних [3].

Основними характеристиками введенні клієнт-серверні та розподілені системи є:

– використання моделі клієнт-сервера для покращення ресурсного використання;

– розміщення частини функціоналу на клієнтських комп'ютерах;

– підвищення ефективності та доступності системи.

Перевагами розподілених систем є:

– спільна робота – можливість спільної роботи та обміну даними;

– більша доступність – забезпечення більшого доступу до даних для різних відділень.

Недоліками розподілених систем є:

– складне адміністрування – адміністрування може бути складним;

– висока вартість – високі витрати на обслуговування.

Віртуалізація стала ключовим етапом у вдосконаленні інформаційних систем. Вона дозволила розділити фізичні ресурси серверів на віртуальні екземпляри, підвищуючи масштабованість і ефективність [4].

Основними характеристиками віртуалізації є:

– розділення фізичних ресурсів серверів на віртуальні екземпляри;

– підвищення масштабованості та ефективності використання обладнання.

Однак справжнім проривом стали хмарні рішення. Хмарні рішення дозволяють зберігати та обробляти дані на віддалених серверах. Користувачі можуть працювати з даними з будь-якого місця. Вони дозволяють підприємствам зосереджуватися на своїй основній діяльності, перекладаючи технічні аспекти на постачальників хмарних послуг [5].

Основними характеристиками хмарних рішень є:

– доступ до ресурсів через Інтернет;

– гнучкість та масштабованість ресурсів;

– висока доступність та обслуговування;

– зменшення витрат на інфраструктуру.

Перевагами хмарних рішень є:

– економія коштів – зменшення витрат на обслуговування;

– масштабованість – легко масштабувати ресурси до потреб.

Недоліками хмарних рішень є:

– залежність від Інтернету – робота вимагає постійного доступу до Інтернету;

– безпека – дані зберігаються на віддалених серверах.

З появою хмарних технологій і переходом багатьох підприємств до хмарних сервісів стає критично важливим забезпечення інформаційної безпеки. Хмарні сервіси дозволяють зберігати, обробляти та обмінюватися даними віддалено, що вносить свої особливості та виклики у сферу безпеки інформації.

Щоб забезпечити інформаційну безпеку, підприємства повинні вживати різноманітні заходи, такі як шифрування даних, встановлення міцних паролів, регулярне оновлення програмного забезпечення та впровадження систем моніторингу безпеки [6]. Крім того, важливо мати чітку стратегію управління ідентичністю та доступом, щоб обмежити доступ до даних лише необхідним працівникам. інформаційна безпека вимагає комплексного підходу та постійного вдосконалення стратегій відповіді на зростаючі виклики у цьому цифровому просторі.

Вимогами до інформаційної безпеки є:

– захист конфіденційності, цілісності та доступності даних;

– використання шифрування для захисту конфіденційної інформації;

– моніторинг та аудит безпеки системи;

– забезпечення безпеки даних під час зберігання в хмарних сервісах.

Більш детальний порівняльний аналіз характеристик локальних систем, розподілених систем та хмарних рішень зображений в таблиці 1.1.

Таблиця 1.1 – Порівняльний аналіз характеристик локальних систем, розподілених систем та хмарних рішень

| Характеристика | Локальні системи | Розподілені системи | Хмарні рішення |
|---|---|---|---|
| Безпека даних | Висока, оскільки дані локалізовані | Залежить від забезпечення мережі | Залежить від рівня захисту хмари |
| Контроль | Повний контроль над обладнанням | Обмежений через розподіленість | Обмежений, контроль залишається у хмарі |
| Спільна робота | Обмежена | Можлива, але складніше адміністрування | Легка спільна робота та обмін даними |
| Мобільність | Обмежена | Залежить від реалізації мереж | Висока, доступ з будь-якого пристрою |
| Вартість | Високі витрати на обладнання | Високі витрати на адміністрування | Зменшення витрат, оплата за використані ресурси |
| Масштабованість | Обмежена | Масштабована, але складніше адміністрування | Легка масштабованість, гнучкість |
| Доступність | Залежить від локальної мережі | Більша через розподіленість | Висока, доступ через Інтернет |
| Залежність від Інтернету | Ні | Так | Так |
| Адміністрування | Просте | Складне | Легке, управління у хмарі |
| Економія коштів | Менше економії | Середня економія | Значна економія |

Перехід від локальних до хмарних інформаційних систем визначає новий етап в розвитку технологій. Цей шлях дозволяє компаніям забезпечувати високу продуктивність та гнучкість в умовах постійних змін у сучасному бізнес-середовищі.

Впровадження хмарних технологій розширює можливості підприємств, забезпечуючи ефективне використання ресурсів, гнучкість у розмірі та обсязі даних, а також підвищену доступність та мобільність. Крім того, швидкість впровадження хмарних рішень дозволяє компаніям швидко адаптуватися до нових викликів та збільшити ефективність своєї діяльності. З важливих переваг є також забезпечення високої доступності та безпеки даних.

## 1.2 Склад та завдання сучасної інформаційної системи підприємства

Інформаційна система – це сукупність ресурсів, методів і людських ресурсів, які використовуються для зберігання, обробки та надання інформації для досягнення конкретної мети. Інформаційна система забезпечує зібрання, зберігання, обробку, пошук та видачу інформації, необхідної для ухвалення рішень в будь-якій сфері [7]. Вона полегшує аналіз проблем і створення нових продуктів. Основним технічним засобом обробки інформації у цьому контексті є персональний комп'ютер (ПК).

Інформаційна система містить дані про організацію та її оточення. Три основні операції – збір, обробка та вивід – формують інформацію, необхідну для функціонування підприємства. Зворотний зв'язок представляє собою інформацію, яка повертається від відповідних людей або процесів у підприємстві для оцінки та коригування введених даних (рисунок 1.1).

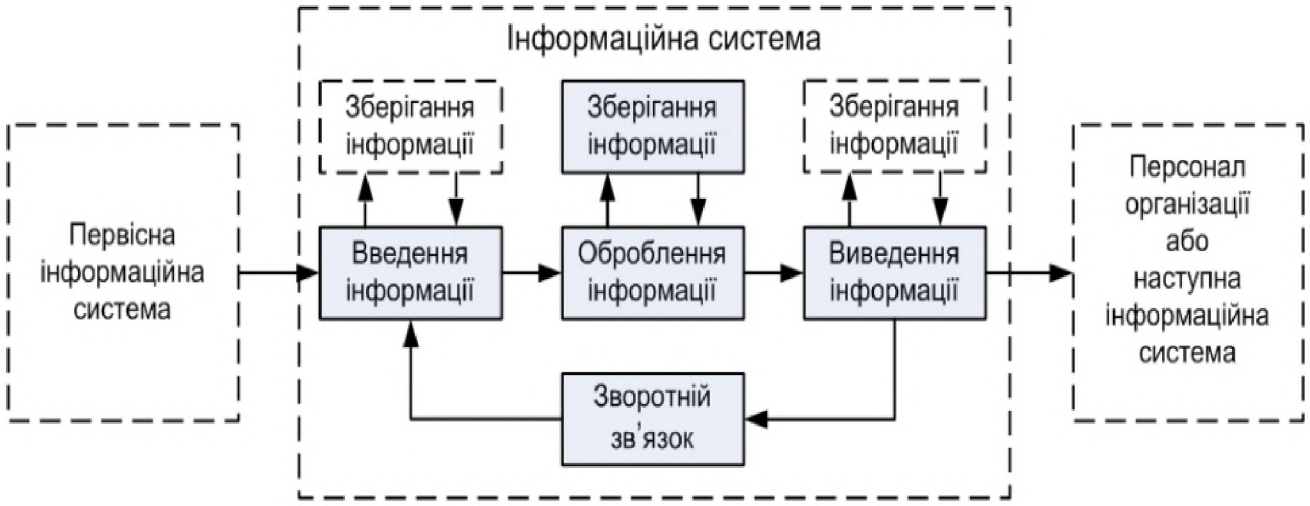


Рисунок 1.1 – Взаємозв’язок елементів ІС

Сучасні підприємства стикаються з різноманітними викликами та впровадження ефективної інформаційної системи стає ключовим фактором їх успішності. Склад інформаційної системи підприємства включає в себе комплекс технологій, програм, обладнання та персоналу, спрямований на оптимізацію бізнес-процесів.

Сучасна інформаційна система підприємства складається з декількох ключових компонентів, які взаємодіють для забезпечення ефективного управління різними аспектами бізнесу. Основні складові такої системи включають:

1. Апаратне забезпечення:

– сервери – для забезпечення зберігання та обробки даних;

– комп'ютери та ноутбуки – для роботи персоналу та доступу до системи;

– мережеве обладнання – роутери, комутатори для забезпечення мережевого з'єднання.

2. Програмне забезпечення:

– операційна система – забезпечує базовий функціонал для виконання програм та обслуговування апаратного забезпечення;

– бази даних – для зберігання та управління даними підприємства;

– ERP-системи – для автоматизації та управління основними бізнес-процесами, такими як фінанси, логістика, виробництво і людські ресурси;

– CRM-системи – для ведення і управління відносинами з клієнтами;

– BI-системи – для аналізу та виведення стратегічної інформації.

3. Мережева інфраструктура:

– локальні та глобальні мережі, що забезпечують зв'язок між різними компонентами системи та користувачами.

4. Людський фактор:

– IT-спеціалісти – для розробки, впровадження та підтримки системи;

– користувачі – персонал підприємства, який користується інформаційною системою у своїй повсякденній роботі.

5. Дані та інформація:

– системи зберігання даних – для безпечного та ефективного зберігання великих обсягів інформації;

– дані процесів бізнесу – включають в себе дані про клієнтів, транзакції, запаси тощо.

6. Процеси та процедури:

– стандарти та процедури – для коректної роботи інформаційної системи та забезпечення її безпеки.

7. Безпека та захист:

– системи захисту інформації – для захисту використовують шифрування, антивіруси, системи контролю доступу.

Важливою функцією інформаційної системи є забезпечення збереження та обробки великого обсягу даних. Це допомагає підприємству не лише ефективно використовувати наявні ресурси, але і приймати обґрунтовані стратегічні рішення на основі аналізу інформації.

Інформаційна система підприємства відіграє важливу роль у забезпеченні безпеки та конфіденційності даних. Захищена від несанкціонованого доступу система дозволяє уникнути витоку важливої інформації та зберегти репутацію підприємства [8].

Одним із головних завдань інформаційної системи є автоматизація та управління внутрішніми та зовнішніми процесами підприємства. Це включає в себе облік товарів на складі, замовлення, постачання, фінансовий облік та інші аспекти діяльності. Інформаційна система дозволяє в режимі реального часу відслідковувати стан ресурсів, планувати виробництво та вчасно реагувати на зміни в бізнес-середовищі.

Сучасна інформаційна система підприємства виконує різноманітні завдання, спрямовані на поліпшення ефективності, контроль над процесами та підтримку прийняття рішень. Основні завдання такої системи включають:

– автоматизація бізнес-процесів – заміна ручних операцій автоматизованими системами для прискорення виробничих і адміністративних процесів;

– управління ресурсами – використання людських, фінансових та матеріальних ресурсів підприємства;

– забезпечення доступу до інформації – забезпечення швидкого та безпечного доступу до необхідної інформації для всіх рівнів персонал;

– інтеграція бізнес-процесів – забезпечення взаємодії між різними функціональними областями підприємства для уникнення інформаційних проблем;

– аналіз та звітність – забезпечення можливості аналізу даних для прийняття управлінських рішень та генерації звітів;

– CRM – ведення бази даних клієнтів, взаємодія з ними та покращення обслуговування клієнтів;

– ERP – координація різних функціональних областей, включаючи фінанси, виробництво, логістику та інші, для забезпечення їх взаємодії та оптимізації.

– Безпека інформації – захист конфіденційної інформації та забезпечення безпеки інформаційних систем;

– моніторинг та контроль – системи для моніторингу та контролю за різними аспектами діяльності підприємства;

– інновації та гнучкість – забезпечення можливості швидко реагувати на зміни в бізнес-середовищі та впровадження інновацій;

– спільна робота та комунікація – забезпечення ефективної комунікації та спільної роботи між співробітниками;

– аналітика – відстеження та аналіз результатів діяльності для пошуку можливостей для вдосконалення [9].

Структура інформаційної системи складається з різних частин, які називаються підсистемами. Підсистема – окрема частина системи, яка виділяється за певною ознакою. Загальну структуру інформаційної системи можна розглядати як сукупність підсистем незалежно від області застосування, причому підсистеми відповідають за різні аспекти функціонування системи [10].

Підсистема інформаційного забезпечення має завдання вчасно створювати та надавати достовірну інформацію для забезпечення процесу управління та ухвалення управлінських рішень (рисунок 1.2).


Рисунок 1.2 – Складові забезпечення ІС

Отже, сучасна інформаційна система є необхідним інструментом для оптимізації діяльності підприємства. Її роль полягає в сприянні підвищенню продуктивності, зниженні витрат та покращенні конкурентоспроможності на ринку. Ця система дозволяє ефективно збирати, обробляти та надавати інформацію, що допомагає у прийнятті обґрунтованих управлінських рішень. Завдяки інтеграції різних підсистем інформаційного забезпечення, підприємство може швидко реагувати на зміни в економічному середовищі та вдосконалювати свої бізнес-процеси. Такий підхід дозволяє досягти не лише ефективності, але й стати більш гнучким та адаптивним до викликів сучасного бізнес-середовища.

## 1.3 Аналіз стандартів галузі інформаційної безпеки

Інформаційна безпека охоплює комплекс заходів та політик, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Це включає заходи з захисту від несанкціонованого доступу, збереження цілісності даних, та забезпечення доступності інформації у випадку потреби. Головна мета полягає в тому, щоб уникнути порушень безпеки, забезпечити конфіденційність особистої та важливої інформації, а також гарантувати, що системи та дані залишаються цілими і доступними в умовах різних загроз.

Система управління інформаційною безпекою є частиною загальної системи управління, спрямованою на розробку, впровадження, ефективне функціонування, моніторинг, періодичний огляд, підтримку та постійне вдосконалення заходів інформаційної безпеки.

Створення системи управління інформаційною безпекою (СУІБ) дозволяє чітко визначити взаємозв'язок між процесами та підсистемами інформаційної безпеки, визначити відповідальних за них осіб, а також з’ясувати, які фінансові та трудові ресурси необхідні для їх ефективного функціонування.

Основні завдання системи управління інформаційною безпекою включають:

– визначення та оцінка потенційних небезпек для інформаційної безпеки;

– розроблення та впровадження стратегій зменшення ризиків в галузі інформаційної безпеки;

– моніторинг виконання вказаних стратегій;

– впровадження необхідних виправлень у процеси зниження ризиків в інформаційній безпеці.

Ефективне керівництво інформаційною безпекою ґрунтується на таких принципах:

– комплексний підхід – управління інформаційною безпекою має бути всебічним, охоплювати всі аспекти інформаційної системи і враховувати всі фактори, що можуть створити ризики, які впливають на інформаційну систему підприємства;

– відповідність бізнес-цілям і стратегії підприємств;

– висока ступінь управління;

– відповідність використовуваної інформації;

– ефективність у продуктивності та витратами в інформаційній безпеці;

– постійність управління;

– системний підхід – об’єднання управлінських процесів в цикл, який включає планування, впровадження та забезпечення зв’язку між етапами.

Основна мета управління інформаційною безпекою – впровадження відповідних заходів для усунення або зменшення впливу різних загроз і вразливостей, пов'язаних з безпекою, на діяльність організації. Управління інформаційною безпекою сприятиме досягненню необхідних якісних характеристик послуг, що надаються організацією, таких як доступність послуг, збереження конфіденційності та цілісності даних. Стандарти безпеки на різних рівнях встановлюють не тільки обсяг, але й конкретні аспекти діяльності підприємства. За таких умов єдиним варіантом є розробка та впровадження окремого та незалежного процесу управління, а саме системи управління інформаційною безпекою.

На рисунку 1.3 зображено систему управління інформаційної безпеки.


Рисунок 1.3 – Система управління інформаційної безпеки

Створення системи управління інформаційною безпекою включає в себе такі етапи:

– розроблення політик безпеки;

– уточнення в області застосування системи управління інформаційною безпекою

– здійснення оцінки ризиків:

– здійснення контролю над ризиками;

– вибір належних засобів контролю;

– заява щодо відповідності.

Система управління інформаційною безпекою (СУІБ) забезпечує вибір методів і засобів контролю та захисту інформації, які є адекватними і пропорційними, сприяючи отриманню довіри зацікавлених сторін. Важливо враховувати інші стандарти в галузі інформаційної безпеки, оскільки в світовій практиці використовуються різні нормативи і методи, такі як ISM3, COBIT, ITIL / ITSM, BSI-100-2, ISO13335-4, CRAMM, ISO15408. Варто відзначити, що всі ці стандарти сумісні з ISO 27001 та ділять загальні принципи.

Стандарти інформаційної безпеки – це набір правил та вказівок, які визначають вимоги до процесів, заходів та технологій, спрямованих на забезпечення безпеки інформації. Ці стандарти охоплюють як внутрішні, так і міжнародні аспекти, і також встановлюють методи контролю для перевірки відповідності цим вимогам [12].

Основна мета стандартів інформаційної безпеки полягає у створенні бази для взаємодії між виробниками, споживачами та фахівцями з сертифікації, кожна з яких має власні інтереси. Ці стандарти призначені для вирішення проблем інформаційної безпеки через створення спільних вимог та норм, які сприяють ефективній взаємодії усіх зацікавлених сторін.

Створення стандартів в галузі інформаційної безпеки має на меті вирішення ключових завдань:

– розробка та уніфікація термінології для чіткого розуміння концепцій в інформаційній безпеці;

– визначення стандартів для вимірювання рівня інформаційної безпеки, щоб мати об'єктивні критерії оцінки;

– забезпечення сумісності технічних та інформаційних засобів, що гарантує безпеку, для забезпечення ефективності їх взаємодії;

– зібрання та поширення найкращих практик в галузі інформаційної безпеки для професійного обміну знаннями;

– встановлення обов'язкових стандартів і вимог для забезпечення виконання визначених норм і стандартів у сфері інформаційної безпеки.

Існують такі міжнародні стандарти інформаційної безпеки:

1. BS 7799 – 1: 2005 – кодекс практики управління інформаційною безпекою, що включає 127 механізмів контролю для побудови систем управління інформаційною безпекою [13].

2. BS 7799 – 2: 2005 – це специфікація систем управління інформаційною безпекою, використовується для сертифікації СУІБ організацій.

3. BS 7799-3: 2006 – стандарт в галузі управління ризиками інформаційної безпеки.

4. ISO/IEC 17799 – описує практичні правила управління інформаційною безпекою [14].

5. ISO/IEC 27001 – міжнародний стандарт для системи управління інформаційною безпекою, базується на BS 7799-2: 2005.

6. ISO/IEC 27002 – стандарт, що базується на ISO/IEC 17799: 2005, забезпечує практичні правила управління інформаційною безпекою [15].

7. ISO/IEC 27005 – керівництво з управління ризиками інформаційної безпеки, базується на BS 7799-3: 2006 [16].

8. Інші Стандарти – включають ISO/IEC 15408, FIPS 140, CWA 14167, CWA 14170, CWA 14171, CWA 14172, і настанови ETSI для електронного підпису.

Існує кілька ключових стандартів галузі інформаційної безпеки, які підприємства можуть використовувати для захисту своєї інформації та систем. Ось декілька з них:

1. ISO/IEC 27001 – цей стандарт встановлює систему управління інформаційною безпекою (ISMS). Він охоплює широкий спектр аспектів, включаючи політику безпеки, управління ризиками, фізичну безпеку, інциденти та багато іншого [17].

Переваги:

– глобально визнаний;

– сприяє впровадженню злагодженого підходу до інформаційної безпеки.

2. NIST SP 800-53 – розроблений Національним інститутом стандартів і технологій (NIST) США, цей документ містить набір контрольних заходів для федеральних інформаційних систем та організацій [18].

Переваги:

– застосовується в різних секторах;

– орієнтований на конкретні технічні та організаційні заходи безпеки.

3. COBIT (Control Objectives for Information and Related Technologies) – розроблений ISACA, COBIT надає фреймворк для управління та контролю над інформаційними технологіями підприємства [19].

Переваги: спрямований на досягнення бізнес-цілей через ефективне використання IT та забезпечення відповідності.

4. PCI DSS (Payment Card Industry Data Security Standard) – розроблений групою стандартів безпеки платіжних карт, цей стандарт стосується захисту інформації про платіжні картки [20].

Переваги:

– забезпечує безпеку транзакцій та даних про картки.

Більш докладно про аналіз стандартів інформаційної безпеки для підприємств написано в таблиці 1.2.

Таблиця 1.2 – Порівняльний аналіз стандартів інформаційної безпеки для підприємств

| Критерій | ISO/IEC 27001 | NIST SP 800-53 | COBIT | PCI DSS |
|---|---|---|---|---|
| Зміст | Управління ISMS | Контрольні заходи | Управління IT | Захист даних картки |
| Глобальне визнання | Так | Так | Так | Так |
| Сфера застосування | Універсальна | Федеральні системи | Управління IT | Фінансові установи |
| Орієнтація | Процеси, ризики | Технічні та організаційні заходи | Бізнес-цілі, IT | Платіжні дані |
| Підходи до безпеки | Комплексний | Технічний та організаційний | Бізнес-орієнтований | Специфічний для карток |
| Управління ризиками | Так | Так | Так | Так |
| Відповідність | Залежить від контексту | Залежить від контексту | Залежить від контексту | Обов'язкова |
| Гнучкість | Висока | Середня | Висока | Низька |
| Орієнтованість на IT | Частково | Так | Так | Частково |

Ці стандарти демонструють стратегічний підхід до забезпечення інформаційної безпеки та сприяють підприємствам у визначенні та реалізації відповідних заходів для захисту їх інформаційних ресурсів.

Один із основних елементів, що сприяє успішному функціонуванню системи управління інформаційною безпекою підприємства, полягає в її заснуванні на міжнародних стандартах ISO/IEC 27001.

На міжнародному рівні стандарти інформаційної безпеки, такі як ISO/IEC 27001 грають визначальну роль. Ці стандарти встановлюють загальні принципи управління інформаційною безпекою, а також надають систематичний підхід до ідентифікації, оцінки та керування ризиками [21].

Аналіз стандартів галузі інформаційної безпеки свідчить про їхню важливість для будь-якої організації, що працює в сфері цифрових технологій. Впровадження відповідних стандартів допомагає підвищити рівень захищеності, забезпечуючи відповідність та довіру як клієнтів, так і партнерів.

## Висновки до розділу 1

В даному розділі було розглянуто перехід від локальних до хмарних інформаційних систем, який визначає етап в розвитку технологій. Цей шлях дозволить компаніям забезпечувати високу продуктивність та гнучкість в умовах постійних змін у сучасному бізнес-середовищі.

Досліджено склад та завдання сучасної інформаційної системи та її роль в продуктивності діяльності підприємства. Сучасна інформаційна система є необхідним інструментом для оптимізації діяльності підприємства. Її роль полягає в сприянні підвищенню продуктивності, зниженні витрат та покращенні конкурентоспроможності на ринку. Ця система дозволяє ефективно збирати, обробляти та надавати інформацію, що допомагає у прийнятті обґрунтованих управлінських рішень

В останньому пункті розглянуто стандарти інформаційної безпеки та які завдання вони виконують. Ці стандарти демонструють стратегічний підхід до забезпечення інформаційної безпеки та сприяють підприємствам у визначенні та реалізації відповідних заходів для захисту їх інформаційних ресурсів.

Аналіз стандартів галузі інформаційної безпеки свідчить про їхню важливість для будь-якої організації, що працює в сфері цифрових технологій. Впровадження відповідних стандартів допомагає підвищити рівень захищеності, забезпечуючи відповідність та довіру як клієнтів, так і партнерів.

# РОЗДІЛ 2
# МОДЕЛЮВАННЯ ЦІЛІСНОСТІ ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

## 2.1 Склад та вимоги до цілісності даних, як складової інформаційної безпеки

Інформаційна безпека є невід'ємною складовою успішної діяльності сучасних організацій у цифровому віці. З метою створення ефективних та стійких систем захисту інформації виникає необхідність використання стандартів галузі інформаційної безпеки.

Інформаційна безпека – це процеси та засоби, спрямовані на збереження та захист інформації, а також основних компонентів, включаючи системи та обладнання, призначені для обробки, зберігання та передачі цієї інформації. Це включає в себе різноманітні технології, стандарти та методи управління, необхідні для ефективного забезпечення безпеки інформації [11].

Об'єктом інформаційної безпеки вважається інформація, яка стосується різних сфер, таких як державні справи, службова діяльність, комерційні інтереси, інтелектуальна власність та особисті дані. Також важливі її засоби обробки та передачі, а також інфраструктура, пов'язана з цим процесом.

Суб'єктами інформаційної безпеки є організації та структури, що в певному вимірі здійснюють заходи для забезпечення інформаційної безпеки.

В екстремальних ситуаціях роль інформаційної безпеки набуває особливого значення, оскільки будь-яка неточна інформація може призвести до загострення ситуації.

Ключовим елементом у забезпеченні безпеки інформації та управлінні ризиками поширення даних є визначення різних рівнів захисту для різних видів інформації. Враховуючи, що всі дані неоднакові, важливо встановити їм відповідні класи захисту. Перший етап цього процесу – визначення ідентифікаційної інформації на найвищому рівні управління. Далі, розробляється політика

класифікації, яка визначає різні мітки для класифікації, встановлює оцінку для кожного типу інформації та надає конкретні заходи безпеки для кожної категорії. Сутність інформаційної безпеки зображено на рисунку 2.1.

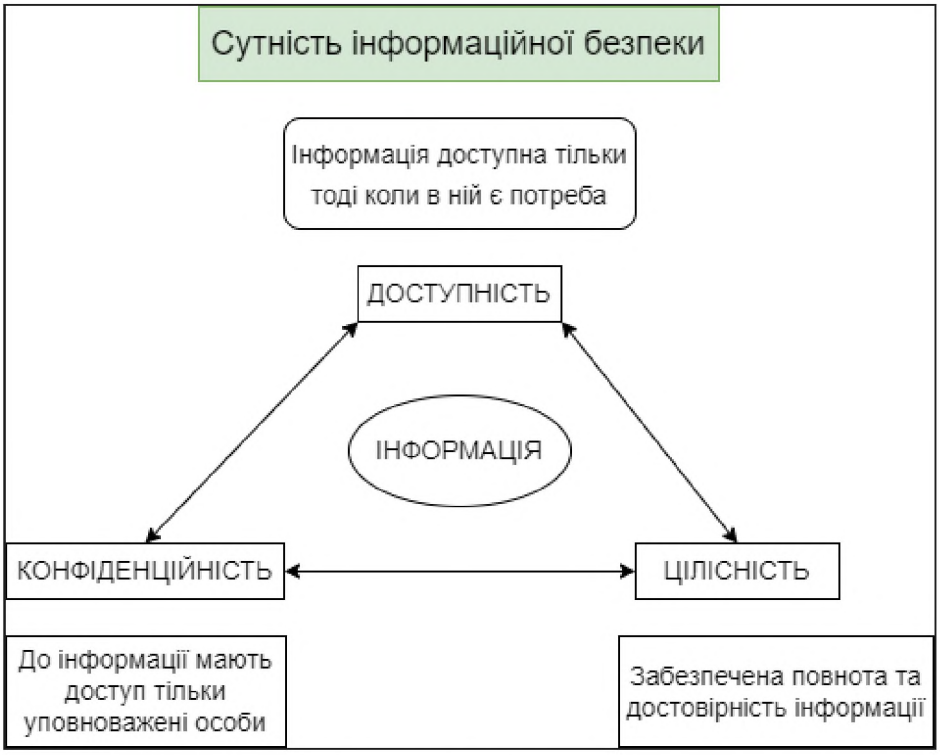


Рисунок 2.1 – Сутність інформаційної безпеки

Конфіденційність – це принцип передбачає захист інформації від несанкціонованого доступу. Забезпечення конфіденційності є невід'ємною частиною будь-якої системи інформаційної безпеки.

Цілісність – це принцип який гарантує, що інформація залишається незмінною та невикривленою.

Доступність – захищає від забруднення інформації чи блокування доступу до неї. Забезпечення доступності гарантує продуктивну та неперервну роботу системи.

З урахуванням загроз та ризиків, пов'язаних із сучасною технологічною інфраструктурою, інформаційна безпека стає стратегічно важливою для всіх організацій.

Інформаційна безпека означає захист інформації та інфраструктури від непередбачених чи умисних впливів, незалежно від того, чи вони мають

природний, чи штучний характер. Мета – забезпечити власників та користувачів від можливих негативних наслідків [22].

Інформаційна безпека використовується у різноманітних сферах життя: політичній, економічній, соціальній та духовній. Важливо оберігати її від витоку, щоб мінімізувати можливі несприятливі наслідки.

Завдання в галузі інформаційної безпеки включають:

– гарантування права особи та суспільства на доступ до інформації;

– забезпечення об’єктивності інформації;

– боротьба з кримінальними загрозами в сфері інформаційних та телекомунікаційних систем;

– захист особистості, підприємств та держави від інформаційно-психологічних загроз;

– протидія дезінформації.

Інформація вважається безпечною, якщо вона у повному обсязі захищена від будь-яких видів загроз. Основну частину витоків інформації становлять події, пов'язані з розголошенням платіжних даних і особистої інформації, що становить близько 80% випадків [23]. Правильний підхід у забезпеченні захищеності – це здійснення запобіжних заходів, здатних зменшити вплив всередині та зовні системи.

В інформаційну систему входять такі елементи:

– суб'єкти – власники інформації та механізмів (інфраструктури);

– база – комп'ютерні приміщення, різноманітні системи.

До основних складових інформаційних даних відносять:

– доступність – це ознака, що дозволяє користувачам у певних випадках безперешкодно отримати інформацію, що їх цікавить. Винятком є дані, приховані від загального огляду, розголошення яких може завдати серйозної шкоди суб'єктам та інформації;

– цілісність – один із елементів інформації, що гарантує її стабільність при навмисному або ненавмисному перетворенні чи знищенні даних.

– конфіденційність – це ключовий аспект, який обмежує право доступу до інформації лише зацікавленим юридично повноваженим сторонам [24].

Цілісність даних – це властивість даних, що забезпечує їхню точність і не відтворюваність. Основна мета забезпечення цілісності даних полягає в тому, щоб гарантувати, що дані залишаються вірними протягом всього їхнього життєвого циклу [25].

Цілісність даних має велике значення, оскільки вони використовуються для важливих рішень у охороні здоров'я, фінансах, управлінні та безпеки. Якщо дані не є точними чи надійними, це може підірвати довіру до прийнятих рішень.

Цілісність даних становить ключовий компонент інформаційної безпеки. Системи інформаційної безпеки повинні не лише забезпечувати конфіденційність та доступність даних, а й гарантувати їхню цілісність. Забезпечення цілісності даних також важливе для відповідності нормативам і законам.

Склад цілісності даних – це збереження та зберігання даних з високим рівнем цілісності. Це означає, що дані залишаються непошкодженими, стійкими до помилок і несанкціонованого доступу протягом усього їх життєвого циклу.

Склад цілісності даних може включати в себе заходи безпеки, механізми перевірки цілісності даних, аудит та інші методи забезпечення надійності даних. Він відіграє важливу роль у забезпеченні точності та достовірності інформації.

Цілісність даних включає такі аспекти:

1) непошкодженість даних – гарантує відсутність будь-яких випадкових чи навмисних змін у вмісті даних;

2) автентичність – вимагає визначення істинного походження даних та перевірки їхньої правомірності та недоторканості;

3) узгодженість – забезпечує взаємо-узгодженість даних усередині системи та між різними компонентами, що гарантує їхню правильність та взаємну сумісність.

Основними вимогами до цілісності даних можуть включати:

1) перевірка контрольної суми – додавання контрольних сум або хеш-значень до даних для перевірки їхньої цілісності;

2) механізми виявлення та виправлення помилок – використання спеціальних кодів або алгоритмів для виявлення та виправлення помилок у даних;

3) автентифікація та авторизація – забезпечення, щоб тільки вповноважені користувачі мали доступ до даних і могли внесення змін;

4) резервне копіювання – регулярне створення резервних копій даних для запобігання втраті в разі аварій чи несправності обладнання [26].

Для створення системи інформаційної безпеки необхідно визначити джерела потенційних інформаційних небезпек і загроз. Існують чотири основні дії з інформацією, які можуть становити загрозу: збір, модифікація (спотворення), витік та знищення інформації. Загрози поділяються на внутрішні та зовнішні.

Внутрішніми джерелами загроз є:

– співробітники підприємства:

– програмне забезпечення;

– апаратні засоби.

Внутрішні загрози можуть виявитися у таких формах:

– неправильні дії користувачів та системних адміністраторів;

– порушення співробітниками установлених правил збору, обробки, передачі та знищення інформації;

– помилки у функціонуванні ПЗ;

– відмови або збої комп’ютерного обладнання.

Зовнішніми джерелами загроз є:

– комп'ютерні віруси та шкідливі програми;

– підприємства та окремі особи;

– стихійні лиха.

Формами прояву зовнішніх загроз є:

– зараження комп'ютерів вірусами чи шкідливими програмами;

– несанкціонований доступ (НСД) до корпоративної інформації;

– інформаційний моніторинг з боку конкуруючих структур, розвідувальних та спеціальних служб;

– дії державних структур та служб, що супроводжуються збором, модифікацією, вилученням та знищенням інформації;

– аварії, пожежі, техногенні катастрофи, стихійні лиха.

Усі перелічені вище види загроз (форми прояву) можна розділити на навмисні та ненавмисні.

За методами впливу на об'єкти інформаційної безпеки загрози можна класифікувати таким чином: інформаційні, програмні, фізичні, радіоелектронні та організаційно-правові.

До інформаційних загроз можна віднести:

– несанкціонований доступ до інформаційних ресурсів;

– незаконне копіювання даних в ІС;

– крадіжка інформації з бібліотек, архівів, банків та баз даних;

– порушення технології обробки даних;

– незаконний збір та використання інформації.

До програмних загроз відноситься:

– експлуатація помилок та вразливостей у ПЗ;

– комп’ютерні віруси;

– встановлення шкідливих пристроїв.

До фізичних загроз належать:

– знищення чи руйнування засобів обробки інформації та зв'язку;

– викрадення носіїв інформації;

– розкрадання програмних чи апаратних ключів та засобів криптографічного захисту даних;

– вплив на співробітників.

До радіоелектронних загроз належать:

– Впровадження електронних пристроїв перехоплення інформації в технічні засоби та приміщення;

– перехоплення, розшифрування, підміна та знищення інформації в каналах зв'язку.

До організаційно-правових загроз належать:

– порушення вимог законодавства та затримка у ухвалення необхідних нормативно-правових рішень в інформаційній сфері;

– закупівлі недосконалих чи застарілих інформаційних технологій та засобів інформатизації.

Для забезпечення безпеки інформаційних відносин важливо використовувати комплекс заходів:

1) законодавчий рівень є важливим для забезпечення інформаційної безпеки. До заходу цього рівня відноситься регламентація законом та нормативними актами дій з інформацією та обладнанням та настанням відповідальності за порушення правильності дій;

2) адміністративний рівень – головна мета даного рівня – сформувати програму робіт у галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси та контролюючи стан справ. Основою програми є безпекова політика, що відображає підхід організації до захисту своїх інформаційних активів. Керівництво кожної організації має усвідомити необхідність підтримання режиму безпеки та виділення з цією метою значних ресурсів.

3) процедурний рівень (конкретні заходи безпеки, орієнтовані людей). Заходи даного рівня включають:

– заходи, що здійснюються під час проектування,
будівництві та обладнанні обчислювальних центрів та інших об'єктів систем обробки даних;

– заходи щодо розробки правил доступу користувачів до ресурсів системи (розробка політики безпеки);

– заходи, що здійснюються при доборі та підготовці персоналу, який обслуговує систему;

– організацію охорони та режиму допуску до системи;

– організацію обліку, зберігання, використання та знищення документів та носіїв інформації;

– розподіл реквізитів розмежування доступу;

– організацію явного та прихованого контролю за роботою користувачів;

– заходи, що здійснюються при проектуванні, розробці, ремонті та модифікаціях обладнання та програмного забезпечення.

4) програмно-технічний рівень (технічні заходи). Заходи захисту цього рівня ґрунтуються на використанні спеціальних програм та апаратури та виконуючих функції захисту:

– ідентифікацію та аутентифікацію користувачів;

– розмежування доступу до ресурсів;

– реєстрацію подій;

– криптографічні перетворення;

– перевірку цілісності системи;

– перевірку відсутності шкідливих програм;

– програмний захист інформації, що передається, і каналів зв'язку;

– захист системи від наявності та появи небажаної інформації;

– створення фізичних перешкод на шляхах проникнення порушників;

– моніторинг та сигналізацію дотримання правильності роботи системи;

– створення резервних копій цінної інформації.

Ризик в інформаційній безпеці – це потенційна можливість виникнення загрози чи події, яка може призвести до втрати чи пошкодження інформації, а також порушення конфіденційності, цілісності або доступності даних. В іншій інформаційній безпеці ризик оцінює ймовірність виникнення події та можливі наслідки для організації чи системи, що обробляє інформацію. Управління ризиками включає в себе ідентифікацію, оцінку та контроль ризиків для забезпечення ефективного захисту інформації.

Оцінка ризиків в інформаційній безпеці зазвичай включає в себе аналіз потенційних загроз, визначення вразливостей у системі та оцінку можливих втрат чи негативних наслідків. Після ідентифікації ризиків розробляються стратегії та заходи для їх зменшення, переведення, прийняття чи уникнення. Ефективне управління ризиками в інформаційній безпеці дозволяє забезпечити адекватний рівень захисту, уникаючи або пом'якшуючи можливі негативні наслідки для системи та інформації.

У контексті інформаційної безпеки важливо постійно оновлювати оцінку ризиків, оскільки технології розвиваються, з'являються нові загрози, а

інфраструктура змінюється. Забезпечення безпеки вимагає постійного моніторингу, аналізу та вдосконалення заходів безпеки для пристосування до змін в середовищі. Підходи до ризиків систематично та стратегічно допомагає підтримувати стійкий захист інформації та забезпечити надійність у ділових процесах.

Цілісність даних є критично важливою складовою інформаційної безпеки, спрямованою на забезпечення непорушності та надійності даних протягом їхнього життєвого циклу. Зазначені загрози, такі як збої обладнання, помилки в програмному коді, хакерські атаки та невірне користувацьке втручання, підкреслюють необхідність вжиття ефективних заходів для захисту цілісності даних [27].

## 2.2 Засоби підтримки цілісності даних

Цілісність даних є однією з важливих характеристик інформаційних систем, яка визначає точність, невід'ємність та стійкість даних протягом їхнього життєвого циклу. Для забезпечення цілісності даних інформаційні системи використовують різноманітні засоби, які гарантують недоторканність та достовірність інформації.

Під цілісністю розуміється як правильність даних у будь-який момент часу. Але ця мета може бути досягнуто тільки в певних межах. СУБД не може контролювати правильність кожного окремого значення, що вводиться до бази даних [28].

Для забезпечення цілісності даних в базі даних у контексті інформаційної безпеки необхідно вирішити такі задачі:

– розуміння того, які конкретно дані містяться в базі та які дані не повинні потрапляти туди;

– дотримання визначених правил обробки інформації з метою уникнення несанкціонованого доступу.

Основними принципами є:

– СУБД та її додаткові інструменти можуть надавати контроль за збереження цілісності даних;

– достовірність інформації може бути забезпечена людиною, яка розуміє формат даних.

Підтримка цілісності бази даних означає гарантування захисту від неправомірного доступу, неправильних модифікацій та пошкоджень даних у базі. Сучасні бази даних мають ряд засобів для забезпечення підтримки цілісності даних.

Підтримка цілісності в реляційній моделі даних включає три ключові аспекти:

1) Першим аспектом є структурна цілісність, яка визначає обмеження для роботи СУБД. Вона передбачає відсутність дублікатів кортежів та обов'язковість первинного ключа.

2) Другим аспектом є підтримка мовної цілісності в реляційних базах даних. Це означає, що реляційна система повинна гарантувати належний рівень мов для опису та операцій над даними, не нижче стандарту SQL. Це сприяє стандартизації взаємодії з базою даних, полегшуючи розробку та обслуговування.

3) Третій аспект означає забезпечення одного із заданих принципів взаємозв'язку між екземплярами кортежів взаємопов'язаних відносин [29].

Всі обмеження цілісності даних можна розділити на такі категорії як:

1) прикладна цілісність – це обмеження, що стосується клієнтського додатку, який передбачає, що розробники повинні впроваджувати заходи для того, щоб помилки, виникнення яких пов'язано з порушеннями цілісності, були оброблені та виведені в клієнтському додатку.

2) доменна цілісність – це цілісність якою доручено гарантувати, що відповідне поле бази даних містить лише припустимі значення.

3) істотна цілісність – це цілісність метою якої є запобігти подвійному введенню даних про одну сутність в базу даних. Ця цілісність забезпечується шляхом встановлення обмежень на унікальність записів та визначення первинного ключа.

4) посилальна цілісність – здійснюється за допомогою визначення первинних та зовнішніх ключів в системі.

5) транзакційна цілісність – цілісність бази даних забезпечується за допомогою транзакційного механізму, який гарантує непорушність даних при обмеженнях, застосованих до бази даних, а не окремих операцій [30].

Сутнісна цілісність управляється за допомогою інструментів системи керування базою даних. Це досягається за допомогою таких обмежень:

– при додаванні записів до таблиці перевіряється унікальність їх первинних ключів;

– заборонено змінювати значення атрибутів, що входять до первинного ключа.

Цілісність БД може піддаватися внутрішнім та зовнішнім загрозам. Поза цілеспрямованими спробами модифікації або знищення інформації, часто їй завдає шкоди через аварії або помилки в програмному забезпеченні. На другому місці за важливістю є загроза зараження інформаційної системи вірусами, які можуть завдати шкоди, змінити чи знищити дані [46].

Загрози цілісності бази даних можуть виникати з різних причин, таких як:

– збої обладнання;

– помилки в програмному коді системи управління базою даних;

– SQL-ін'єкції, коли вводяться запити з наміром завдати шкоди;

– вразливості операційної системи;

– хакерські атаки;

– помилки користувачів.

Для забезпечення цілісності даних важливо встановлювати обмеження на рівні бази даних, використовувати ефективні механізми контролю доступу та виявлення інцидентів. Розвиток стійких методів виявлення та відновлення від випадків порушення цілісності також є невід'ємною частиною стратегії інформаційної безпеки [31].

Загальний підхід до забезпечення цілісності даних передбачає поєднання технічних, організаційних та людських ресурсів для ефективного управління та

реагування на потенційні загрози. Це стає ключовим елементом підтримки інформаційної безпеки та відображає визнання того, що цілісність даних є невід'ємною частиною стійкої та надійної інформаційної інфраструктури [47].

## 2.3 Хешування

Одним із видів криптографічних методів є хешування, яке використовується для перетворення великої кількості даних у фіксований хеш-код за допомогою спеціальної хеш-функції. Цей процес дозволяє ефективно захищати дані, забезпечуючи при цьому однозначність та неперевершеність, і широко використовується для зберігання паролів, перевірки цілісності даних та інших криптографічних завдань.

Хешування представляє собою захисний механізм, який перетворює вхідні дані в унікальний зашифрований код. Цей метод використовується не лише для шифрування, але і для вирішення інших завдань, що можуть мати певний зв'язок із захистом і обробкою інформації.

Основне призначення хешування – перевірка інформації. Це завдання важливе у величезній кількості випадків: від перевірки паролів на сайті до складних обчислень у блокчейні. Оскільки хеш – це унікальний код певного набору даних, можна зрозуміти, чи відповідає інформація очікуваної. Тому програма може зберігати хеш замість зразка даних для порівняння. Це може бути потрібне для захисту чутливих відомостей або економії місця.

Суть хешування полягає в тому, щоб перетворити вихідні дані будь-якої довжини в унікальний фіксованої довжини хеш-коду за допомогою спеціальних математичних алгоритмів, який може служити для ідентифікації вхідних даних. Усі криптографічні захищені хеш-процеси виводять однаковий результат для тих самих вхідних даних, залишаючи їх незмінними [32]. Цей характеристичний аспект відомий як детермінованість хеш-функції (рис. 2.2).

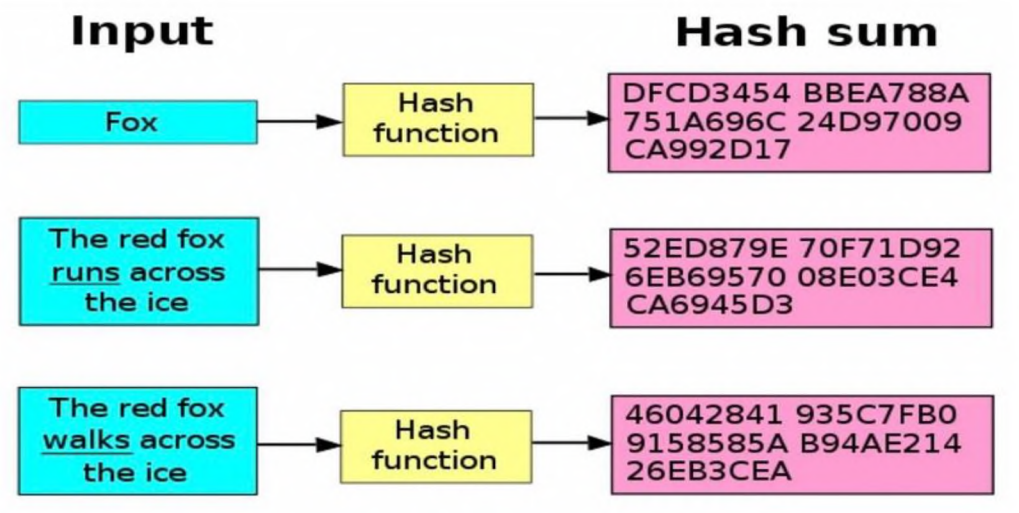


Рисунок 2.2 – Сутність хешування

Алгоритми хешування володіють унікальною особливістю: отримані хеш-рядки інформації неможливо зворотно перетворити у вихідні дані без значних витрат часу і ресурсів. Це пов'язано з тим, що процеси, що відбуваються на криптовалютних платформах, відбуваються лише в односторонньому напрямку . Приклад хеш функції показаний на рис. 2.3 та 2.4.

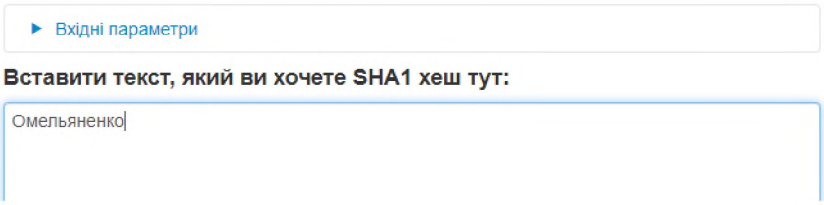


Рисунок 2.3 – Введення даних


Рисунок 2.4 – Результат хеш функції

Головними характеристиками криптографічних хеш-функцій є:

– безповоротність – отримати вихідні дані після застосування хешування майже неможливо, оскільки більшість інформації втрачається в процесі перетворення в унікальний код;

– обумовленість – при застосуванні хеш-функції до однакових вхідних даних завжди отримується однакове значення, що дозволяє використовувати хеш для перевірки автентичності наявних даних;

– унікальність – завжди може генерувати унікальний код для потенційно будь-яких вхідних даних;

– різноманітність – навіть за невеликої різниці між двома наборами даних, хешування може виробити абсолютно різні коди;

– швидкість перетворення – якщо порівняти із стандартним шифруванням файлів, процес хешування генерує значення значно швидше, незалежно від обсягу вихідних даних;

– стійкість до колізій – означає виникнення однакових хеш-кодів для двох різних вхідних наборів даних. Іноді при хешуванні можуть виникати помилки, що призводять до появи "дублікатів" у хеш-кодах.

– захист від відновлення інформації – це та сама не відновлюваність [33]. Теоретично можна використовувати метод підбору для відтворення вихідних даних, але повний захист означає, що навіть при тривалій спробі зловмисника відновити первинні дані шансі на це відсутні.

Перевагами хешування є:

– швидкість – процес генерації хеш коду відбувається швидко, що робить його ефективним для великих обсягів даних;

– унікальність – набір вхідних даних генерує унікальний хеш-код, що дозволяє ефективно визначати ідентичність даних;

– безпека паролів – використовується для захисту паролів, забезпечуючи безпеку в разі витоку інформації;

– перевірка цілісності даних – використовується для перевірки, чи були дані змінені або пошкоджені;

– застосування в криптографії – використовується для створення цифрових підписів та інших криптографічних застосувань.

Недоліками хешування є:

– вразливість до колізій – алгоритми хешування можуть мати колізії, коли два різних набори даних генерують однаковий хеш-код.

– без зворотність – неможливість відновлення оригінальних даних з хеш коду

– залежність від якості алгоритму – в безпекових застосуваннях важливо вибирати стійкі до атак алгоритми хешування.

– односторонній процес – оскільки хешування є одностороннім процесом, важко визначити вихідні дані, якщо не використовувати атаки методом перебору.

– стійкість до атак – старі алгоритми, такі як MD5 та SHA-1, стають менш стійкими до сучасних обчислювальних атак [34].

Стандарти хешування – це визначені норми і правила, які визначають, які конкретні методи та алгоритми використовуються для генерації хеш-кодів в різних областях і застосунках [35]. Це важливо для того, щоб різні системи та програми могли взаємодіяти із загальноприйнятими методами хешування. Також, стандарти допомагають забезпечити безпеку та стійкість алгоритмів хешування, уникнути ситуацій, коли різні вхідні дані генерують однаковий хеш, та забезпечити їхню ефективність у різних застосунках. Алгоритми хешування вказані в таблиці 2.1.

Таблиця 2.1 – Алгоритми хешування

| Алгоритм | Довжина виходу | Використання | Опис |
|---|---|---|---|
| MD5 | 128 бітів | Застарілий, вразливий до колізій | Швидкий, але вразливий до атак, не рекомендується |
| SHA-1 | 160 бітів | Застарілий, вразливий до колізій | Використовувався раніше, але також вразливий |
| SHA-256 | 256 бітів | Широко використовується для безпеки | Безпечний, використовується у багатьох протоколах |
| SHA-3 | Залежить від вибору версії (наприклад, SHA3-256) | Остання версія, рекомендована для використання | Стійкий до атак |

З таблиці видно, що алгоритми MD5 та SHA-1 вже застарілі та вразливі до колізій, тому їх використання в криптографічних задачах не рекомендується.

SHA-256 є поточним стандартом безпеки і широко використовується в різних протоколах та системах. SHA-3 є останньою версією, що володіє стійкістю до атак і представляє сучасний стандарт у галузі хеш-функцій. Отже, для оптимального забезпечення безпеки рекомендується використовувати SHA-256 або SHA-3.

Хешування виявляється потужним інструментом у сферах безпеки, цілісності даних та ідентифікації. Його швидкість та унікальність зробили його невід'ємною

частиною багатьох криптографічних інструментів та протоколів. Проте, важливо обирати стійкі до атак алгоритми, оскільки вразливість до колізій та інші проблеми можуть вплинути на безпеку системи. Хоча хешування є важливим елементом в багатьох аспектах інформаційної безпеки, важливо також усвідомлювати його обмеження та використовувати його відповідно до конкретних вимог і контексту.

## Висновки до розділу 2

В другому розділі розглянуто цілісність даних склад та вимоги до складової інформаційної безпеки підприємства. Розглянуто загальний підхід до забезпечення цілісності даних який передбачає поєднання технічних, організаційних та людських ресурсів для ефективного управління та реагування на потенційні загрози. Для забезпечення цілісності даних важливо встановлювати обмеження на рівні бази даних, використовувати ефективні механізми контролю доступу.

Також розглянуто що таке хешування та яка його суть у сфері цілісності даних та ідентифікації. Суть хешування полягає в тому, щоб перетворити вихідні дані будь-якої довжини в унікальний фіксованої довжини хеш-коду за допомогою спеціальних математичних алгоритмів, який може служити для ідентифікації вхідних даних. Стандарти хешування – це визначені норми і правила, які визначають, які конкретні методи та алгоритми використовуються для генерації хеш-кодів в різних областях і застосунках.

# РОЗДІЛ 3
# МОДЕЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

## 3.1 Обґрунтування математичного апарату

Щоб оцінити стійкість та доступність інформаційного ресурсу, враховуючи можливі відмови та відновлення апаратного та програмного забезпечення, застосовується метод аналізу на основі процесів Маркова.

Марковський аналіз – це головним чином індуктивний метод аналізу, що використовується для оцінки систем і стратегій технічного обслуговування та ремонту, ґрунтуючись на теорії марковських процесів. Він дозволяє розглядати складні функціональні системи, враховуючи ймовірні переходи між різними станами та оптимізувати їхню продуктивність [36].

Марковський процес характеризується тим, що його простір станів є постійним, а розподіл ймовірностей $P_k(i)$ залежить лише від результату попереднього кроку. Іншими словами, події в марковському процесі визначаються лише ймовірністю переходу з одного стану в інший на попередньому етапі, що в математичному формулюванні можна описати так:

$$P\left\{x^{(i+1)} = x_k^{(i+1)}\Big|_{x^{(0)}\dots x^{(i)}}\right\} = P\left\{x^{(i+1)} = x_k^{(i+1)}\Big|_{x^{(i)}}\right\}. \quad (3.1)$$

Для цього типу завдань використання марковських процесів передбачає моделювання простих потоків подій, таких як відмови і відновлення апаратного та програмного забезпечення. Це вимагає припущень про постійність параметрів цих потоків протягом усього періоду експлуатації системи. Однак такі припущення можуть не відповідати реальним умовам функціонування програмного забезпечення інформаційного ресурсу, таких як накопичення дефектів, внесення корекцій у код та оновлення програмних функцій. У такому випадку застосовується метод багатофрагментного моделювання.

Метод моделювання систем з відмовами і відновленням, використовуючи марковський апарат включає такі етапи:

1. Створення діаграми станів та переходів, що базується на структурній схемі надійності системи. Це може бути граф станів або орієнтований граф позначений в залежності від конкретних умов.

2. Визначення вхідних параметрів для моделі надійності системи, ураховуючи відмови та відновлення як апаратного, так і програмного забезпечення. Це охоплює параметри частоти відмов та відновлення для програмного забезпечення, а також частоти подій, що впливають на програмне забезпечення.

3. Визначення готовності інформаційної системи. Це вимагає введення відповідних вхідних параметрів у граф станів системи [37]. За графом складається система диференційних рівнянь наступного вигляду:

$$dP_i(t)/dt = -\sum_{j=0}^{k} \nu_{ij} P_i(t) + \sum_{q=0}^{m} \nu_{qi} P_q(t), \quad i = 0,\ldots,n \,, \tag{3.2}$$

де $j$ – це індекс стану, в який система переходить із стану $i$;

$q$ – це індекс стану, з якого система переходить у стан $i$;

$k$ – кількість станів, в які система переходить із стану $i$;

$m$ – кількість станів, з яких система переходить у стан $i$;

$\nu_{ij}$ – щільність ймовірності переходу системи зі стану $i$ в стан $j$;

$P_i(t)$ – ймовірність того, що система перебуває в стані $i$ в момент часу $t$.

Система рівнянь додається виразом нормалізації, який має вигляд:

$$\sum_{i=0}^{n} P_i(t) = 1 \,, \tag{3.3}$$

де $n$ – сумарна кількість можливих станів, які може займати система.

Після вирішення системи лінійних диференціальних рівнянь чисельним методом і знаходження значень $P_i(t)$, показник надійності визначається як сума ймовірності перебування системи в функціональних станах за формулою:

$$K\ (t) = \sum P_j(t);\ \ j : S_j \in S_P;\ S_P \in M\{S_P, S_I\} \,. \tag{3.4}$$

Отже марковський процес є потужним інструментом для моделювання та аналізу систем з відмовами та відновленням. Його основні принципи ґрунтуються на ідеї, що майбутній стан системи залежить лише від її поточного стану, а не від її попередньої історії. Це дозволяє ефективно вирішувати задачі оцінки ймовірностей, готовності та надійності систем.

Застосування його в моделюванні дозволяє здійснювати прогнози та оптимізувати стратегії обслуговування та ремонту систем. Врахування ймовірностей переходів між станами дозволяє реалістично відобразити динаміку систем з врахуванням відмов та відновлення.

Однак важливо враховувати обмеження та припущення Марковського процесу, зокрема, постійність параметрів і відсутність пам'яті. У деяких сценаріях ці припущення можуть не відповідати реальним умовам, і тоді можуть застосовуватися більш складні методи моделювання.

## 3.2 Модель функціонування інформаційної системи в умовах атак на цілісність даних

Інформаційні системи в сучасному світі стають все більш важливим елементом діяльності організацій та суспільства загалом. Збільшення залежності від інформаційних технологій вносить нові виклики, серед яких особливе значення має забезпечення цілісності даних в умовах можливих атак. Модель функціонування інформаційної системи в умовах атак на цілісність даних вимагає комплексного підходу та впровадження заходів забезпечення безпеки.

Інформаційні системи базуються на кількох основних принципах: конфіденційності, цілісності та доступності.

Цілісність даних є одним із ключових аспектів, що забезпечують надійність інформаційної системи [48].

Атаки на цілісність даних можуть призводити до неправильного змінення, видалення або введення фальшивої інформації в інформаційну систему. Такі

загрози можуть виникати як ззовні, так і зсередини системи внаслідок дії несанкціонованих користувачів чи програм.

Марківські процеси використовуються для моделювання стохастичних систем, де майбутній стан залежить тільки від поточного стану і не залежить від історії проходження системи. В контексті інформаційних систем, модель функціонування станів може бути подана як марківський процес для вивчення ймовірностей переходів між різними станами системи [38].

Загальна модель станів інформаційної системи підприємства зображено на рисунку 3.1.

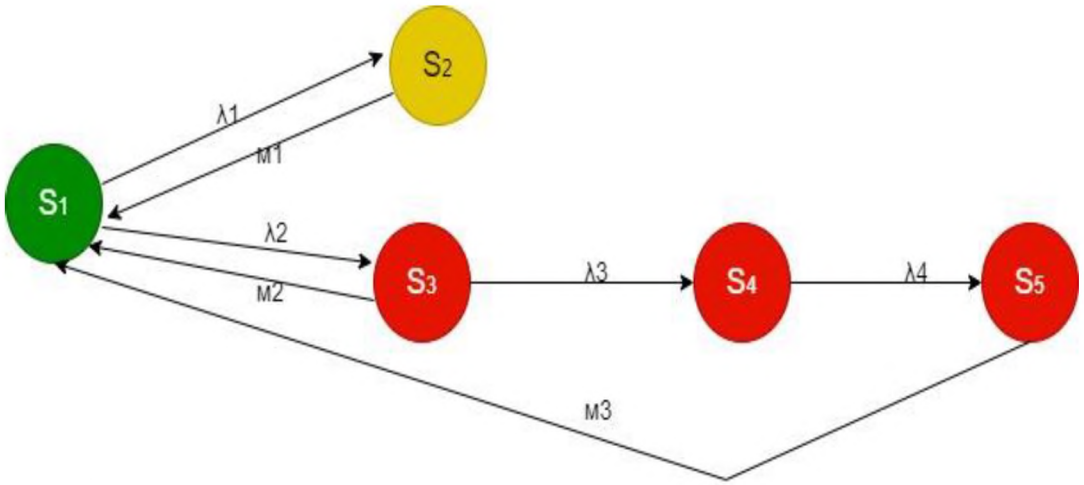


Рисунок 3.1 – Загальна модель станів інформаційної системи підприємства

Ця модель зображує загальний вміст станів інформаційної системи на підприємстві де:

1) $S_1$ – працездатний стан інформаційної системи – означає, що вона працює так, як повинна, і виконує свої функції без проблем чи збоїв.

2) $S_2$ – працездатний стан інформаційної системи, коли на її компоненту починає здійснюватися кібератака (тобто стан «система під атакою).

3) $S_3$ – непрацездатний стан інформаційної системи, обумовлений відмовами її компонент через ненавмисні впливи (фізичні дефекти, програмні помилки та збої).

4) $S_4$ – непрацездатний стан інформаційної системи, обумовлений успіхом кібератаки на її компоненту.

5) $S_5$ – непрацездатний стан інформаційної системи у якому усуваються наслідки проведення кібератаки на її компоненту (відновлення даних, оновлення програмного забезпечення чи встановлення патчів безпеки).

Починаючи зі стану $S_1$, що представляє собою працездатний стан інформаційної системи. У цьому стані система працює без проблем, виконуючи свої завдання відповідно до очікувань. Усі компоненти системи взаємодіють узгоджено, та не мають ознак неполадок.

Зі стану $S_1$ система може перейти до стану $S_2$, коли на її компоненту починає здійснюватися кібератака. У цьому випадку система виявляє можливі аномалії або невизначені дії через можливу кібератаку. Заходи безпеки активуються для виявлення та зупинки атаки, що допомагає зберегти працездатність системи.

Зі стану $S_1$ також може виникнути перехід до стану $S_3$, якщо система стикається з випадковими впливами, такими як фізичні дефекти чи програмні помилки. У стані $S_3$ система перебуває в непрацездатному стані, і може вимагати технічного обслуговування чи виправлення помилок для відновлення працездатності.

У випадку успішної атаки, система перейде до $S_4$, що представляє непрацездатний стан, обумовлений успіхом атаки. Тут необхідні заходи для припинення атаки і відновлення працездатності системи.

У кінці може знадобитися перехід до $S_5$, де система перебуває в непрацездатному стані, але усуваються наслідки кібератаки. Це включає відновлення втрачених даних, оновлення програмного забезпечення та встановлення патчів безпеки для попередження подібних проблем у майбутньому.

Після успішного усунення наслідків кібератаки в стані $S_5$, система може ефективно відновити свою функціональність. У цьому випадку, після термінового втручання та відновлення працездатності, система знову переходить до $S_1$. Цей перехід вказує на те, що система успішно відновила свою нормальну роботу після виправлення критичних помилок та готова до подальших завдань.

Інформаційна система в працездатному стані це стабільна та ефективна система, яка забезпечує неперервну доступність та оптимальну продуктивність. В працездатному стані інформаційна система може виконувати всі свої функції,

надаючи користувачам можливість ефективно працювати, а підприємству управляти ресурсами та виконувати бізнес-процеси без перебоїв чи проблем. основні компоненти інформаційної системи на підприємстві взаємодіють, щоб забезпечити ефективне управління ресурсами та виконання бізнес-процесів.

Інформаційна система підприємства в працездатному стані використовує такі компоненти:

– операційна система (Linux Ubuntu 20.04) – забезпечує основні функції та взаємодію з апаратним забезпеченням, забезпечуючи стабільність та ефективність системи;

– система управління базами даних (MySQL 8.0) – гарантує ефективне зберігання, організацію та доступ до інформації, що використовується в рамках підприємства;

– веб-сервер (Apache 2.4) – забезпечує зовнішній доступ та обмін даними через мережу, полегшуючи комунікацію та взаємодію;

– додатки (PHP 8.2) – різноманітні програмні засоби, розроблені для оптимізації конкретних робочих процесів та підтримки функціональних потреб підприємства.

Ці компоненти взаємодіють між собою, створюючи комплексну інформаційну систему, яка дозволяє підприємству ефективно управляти своїми ресурсами та виконувати бізнес-процеси (рис 3.2).

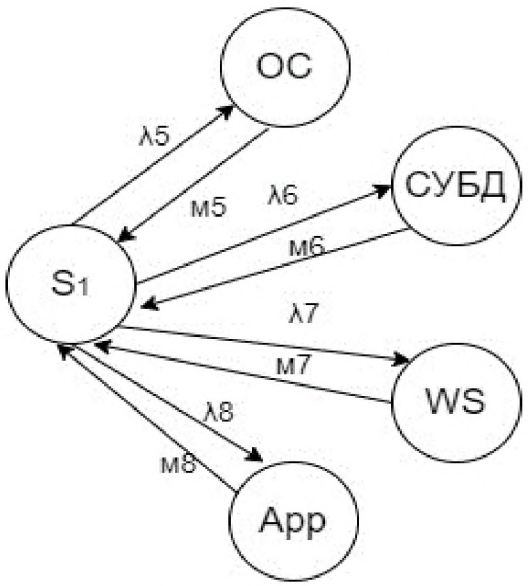


Рисунок 3.2 – Взаємодія компонентів в інформаційної системі

Недоліки або неправильна експлуатація апаратного забезпечення можуть призвести до потенційного непрацездатного стану інформаційної системи підприємства [39]. Неправильності в роботі обладнання можуть викликати перебої в роботі операційної системи, збої в роботі баз даних та інших компонентів, що може призвести до втрати доступу до важливої інформації та суттєвого зниження продуктивності бізнес-процесів.

До апаратного забезпечення можна віднести:

– процесор – основний обчислювальний блок системи, який виконує інструкції програми;

– постійна пам'ять (SSD, жорсткий диск) – місце для зберігання постійної інформації та програм;

– материнська плата – основна плата, на якій розташовані різні компоненти включаючи процесор, пам'ять, інтерфейси;

– відеокарта – відповідає за обробку графічної інформації та виведення зображення на екран;

– блок живлення – забезпечує постачання для всіх компонентів системи.

Атака на інформаційну безпеку підприємства представляє серйозну загрозу в сучасному цифровому світі. Зловмисники постійно розвивають та вдосконалюють свої методи для вторгнень, спрямованих на конфіденційні дані, фінансові ресурси та репутацію компанії [40].

Також можуть використовувати вразливості у програмному забезпеченні або використовувати техніки для отримання несанкційованого доступу до системи. Ця загроза може включати в себе різні форми атак, такі як віруси, троянські коні, фішингові атаки та інші шкідливі програми, які спрямовані на операційні системи, СУБД, веб-сервери та додатки.

На рисунку 3.3 зображено модель станів інформаційної системи підприємства під час атаки.

В таблиці 3.1 надані ключові характеристики безпеки та стійкості інформаційної системи підприємства. Ці характеристики визначаються різними показниками, які враховують інтенсивність прояву дефектів, відновлення після виникнення проблем, атаки на цілісність системи та інші аспекти безпеки.

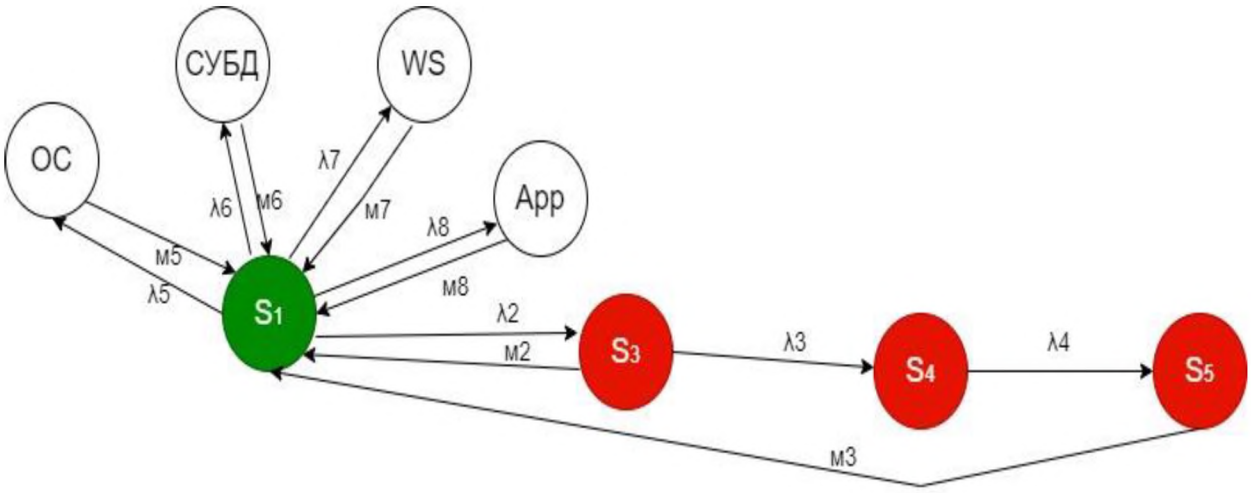


Рисунок 3.3 – Модель станів інформаційної системи підприємства під час атаки.

Таблиця 3.1 – Характеристики безпеки та стійкості інформаційної системи

| №п/п | Name | Matlab-name | Часовий період | Значення | Од.вим. |
|---|---|---|---|---|---|
| 1. | Інтенсивність прояву дефектів ОС | laos | 3,9 років | 3e-5 | 1/год |
| 2. | Інтенсивність прояву дефектів ПЗ служби СУБД | Lасубд | 8,6 років | 1.5e-5 | 1/год |
| 3. | Інтенсивність прояву дефектів WS | Laws | 3,5 місяця | 5e-4 | 1/год |
| 4. | Інтенсивність прояву дефектів App | Laapp | 5,5 місяців | 2.5e-4 | 1/год |
| 5. | Інтенсивність відновлення служби ОС | Muos | 1,5 години | 0.67 | 1/год |
| 6. | Інтенсивність відновлення служби СУБД | Mucубд | 1 година | 1 | 1/год |
| 7. | Інтенсивність відновлення служби WS | Muws | 3 години | 0.33 | 1/год |
| 8. | Інтенсивність відновлення служби App | Mufapp | 1 година | 1 | 1/год |
| 9. | Інтенсивність атак на цілісність СУБД | Laatcубд | 4,02 місяця | 3.46e-4 | 1/год |
| 10. | Критичність атак на цілісність СУБД | Q | | 0.52 | |
| 11. | Інтенсивність розробки оновлень в яких усуваються уразливості ціілсності | lapath | 4 дня | 0.0106 | 1/ год |
| 12. | Інтенсивність відновлення служби після установки патча | mupath | 2 години | 0.6 | 1/ год |

Перші чотири характеристики (laos, Lасубд, Laws, Laapp) вказують на інтенсивність прояву дефектів у операційних системах, службах СУБД, вебсервісах та додатках відповідно. Ці дані можуть слугувати основою для визначення рівня вразливостей та розробки стратегій з їх усунення.

Інші характеристики (Muos, Mucубд, Muws, Mufapp) вказують на інтенсивність відновлення роботи системи після виникнення проблем. Це важливий аспект, оскільки визначає час, необхідний для відновлення нормальної роботи системи та підтримання її стійкості.

Характеристики, пов'язані із забезпеченням цілісності СУБД (Laatcубд, Q) та інтенсивність розробки оновлень (lapath, mupath), свідчать про заходи, спрямовані на усунення вразливостей та підвищення цілісності системи.

Структура даної таблиці дозволяє комплексно оцінити стан безпеки та стійкості інформаційної системи підприємства, що є ключовим елементом у забезпеченні надійності її функціонування та захисту від потенційних кіберзагроз.

Дані для цілісності даних були взяті із сайту NVD. Параметрами пошуку були:

– тип результатів: огляд;

– ключове слово: mysql;

– тип пошуку: пошук у всіх;

– пошук імені CPE: false;

– постачальник CPE: cpe:/:mysql;

– версія CVSS: 2;

– метрики CVSS V2: I:P (рис.3.4).


Рисунок 3.4 – Параметри пошуку даних

На рисунку 3.5 представлена статистика вразливостей за роками, що надає можливість аналізувати динаміку змін на рівні вразливостей та оцінювати ефективність заходів з безпеки протягом років. За цією інформацією можна визначити ключові періоди, такі як періоди зростання чи зменшення кількості вразливостей, а також виявити етапи успішної боротьби з загрозами [41].

Інформація за роками дозволяє провести глибокий аналіз тенденцій у сфері вразливостей. Виявлення періодів зростання чи зменшення може вказувати на ефективність заходів з безпеки та слабкі моменти, які потребують додаткової уваги.

Розглядання статистики в контексті впроваджених заходів забезпечення безпеки дозволяє визначити, наскільки успішно були реалізовані попередні стратегії та чи потребують вони змін.

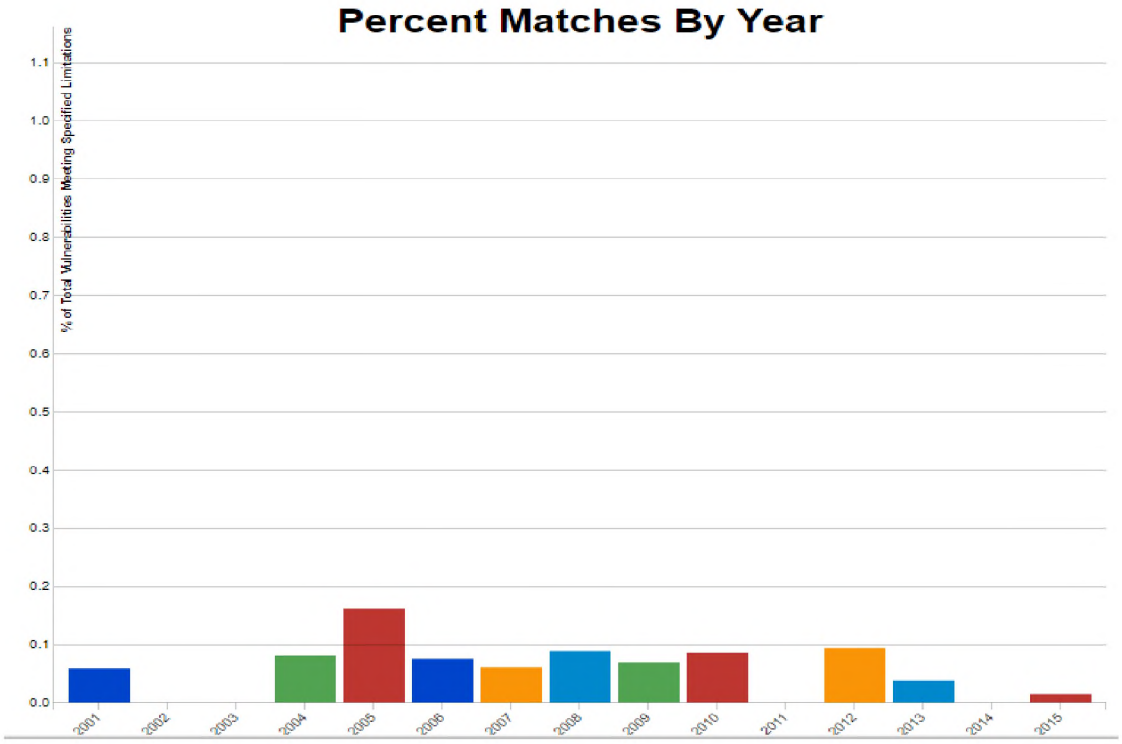


Рисунок 3.5 – Статистика вразливостей за роками

Отже по даній статистиці можна сказати, що зростання кількості вразливостей до 2012 року вказує на постійну загрозу інформаційним системам та їхню вразливість перед новими технологіями та загрозами. Значний спад в 2013 та 2014 роках свідчить про можливий перелом у стратегіях з безпеки чи успішні заходи, спрямовані на виявлення та усунення вразливостей. Це може бути

результатом впровадження нових технологій, поліпшення стандартів безпеки чи активних заходів із забезпечення безпеки. Відновлення в 2015 році та низький рівень вразливостей може вказувати на сталість заходів з кібербезпеки, або на те, що інформаційні системи стали менш схильними до нових загроз.

Загальний контекст виявлення вразливостей в порівнянні з загальною кількістю допомагає зрозуміти, наскільки ефективно виявляються потенційні проблеми в інформаційних системах. Це може бути важливим показником ефективності стратегій та призначення ресурсів для їх запобігання.

На рисунку 3.6 зображено модель інформаційної системи підприємства під час атаки.

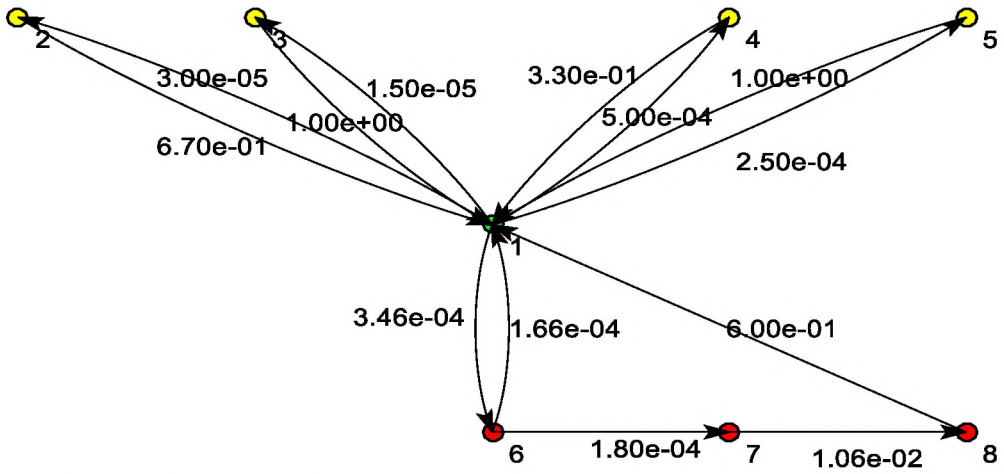


Рисунок 3.6 – Модель інформаційної системи підприємства під час атаки

Дана модель інформаційної системи підприємства під час атаки визначається комплексом факторів та параметрів, які враховуються для аналізу та забезпечення стійкості системи в умовах загроз.

На рисунку 3.7 зображено дві лінії: зелена лінія, яка відображає значення 0.998 та червона лінія зі значенням 0.99. Ці значення представляють рівні стану інформаційної безпеки підприємства. Зелена лінія вказує на конкретний рівень безпеки, який є прийнятним. У той час як червона лінія визначає критичний поріг безпеки, який не повинен бути перевищений. Такі порогові значення дозволяють визначити критичні моменти та ефективно контролювати стан інформаційної безпеки.

У разі будь-яких відхилень від прийнятних стандартів безпеки, можуть вживатися негайні заходи для усунення виявлених проблем та запобігання можливим атакам чи витокам інформації. Ці порогові значення є важливою складовою стратегії інформаційної безпеки, надаючи підприємствам чіткі орієнтири для забезпечення надійного та стабільного захисту їхніх інформаційних ресурсів.

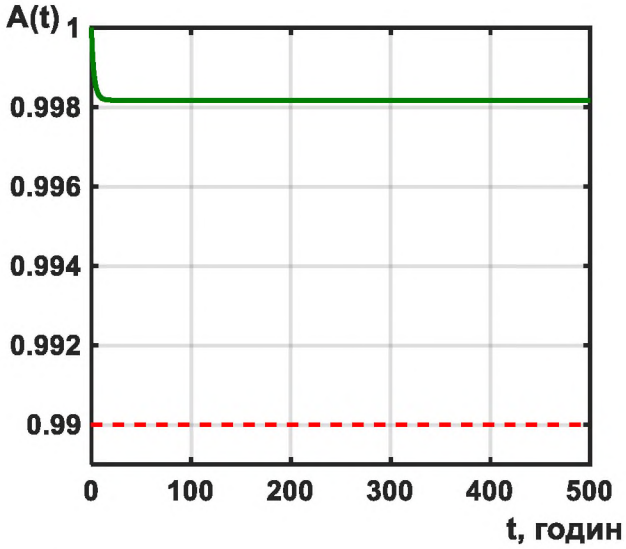


Рисунок 3.7 – Модель без атаки

На рисунку 3.8 зображений графік який показує, як атаки впливають на рівень інформаційної безпеки підприємства та чи перевищують цей рівень певні критичні значення.

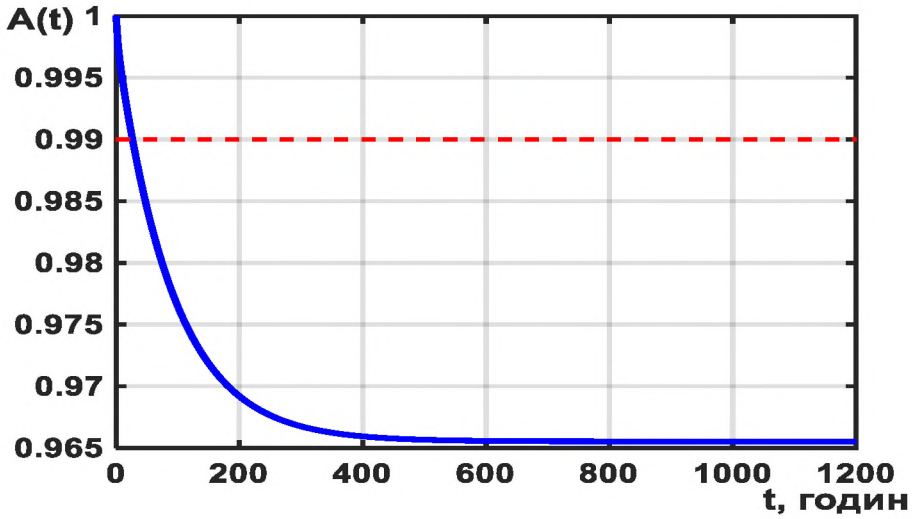


Рисунок 3.8 – Модель з атакою

На даній моделі зображено як синя лінія (від 0.995 до 0.965) представляє динаміку якості чи стану інформаційної безпеки підприємства під впливом атак чи інших вторгнень. Початкове значення 0.995 може вказувати на високий рівень безпеки, а закінчення на 0.965 може сигналізувати про зниження цього рівня внаслідок атак.

Червона лінія з показником визначає критичний поріг безпеки, який, якщо досягнуто, вказує на необхідність реагування чи вжиття заходів для відновлення стану безпеки.

### 3.3 Дослідження моделі безпеки та аналіз результатів

У світі високих технологій важливо забезпечити максимальний рівень безпеки для захисту інформації, ресурсів та інфраструктури [42]. Ключову роль в цьому відіграють моделі безпеки, які встановлюють основні принципи та стратегії захисту. Дослідження цих моделей та подальший аналіз результатів стають важливим етапом для забезпечення ефективної функціональності систем безпеки. Моделі безпеки встановлюють основні принципи, на яких ґрунтується захист інформації та ресурсів. Ці принципи можуть включати конфіденційність, цілісність, доступність та аутентифікацію. Дослідження їх взаємодії визначає загальні стратегії захисту. Вивчення та аналіз моделей безпеки визначає основні напрямки для створення надійних та ефективних заходів забезпечення безпеки в умовах високих технологій.

Було проведено докладний аналіз критичності атак на цілісність системи управління базами даних (СУБД). Дослідження включає в себе аналіз залежності критичності від параметра Q, який представлений на графіку (рис 3.9).

Графік демонструє критичність атак при різних значеннях Q, визначених як критичність атак на цілісність СУБД. Чотири лінії на графіку відповідають різним значенням параметра Q: 0.3, 0.4, 0.5 і 0.6.

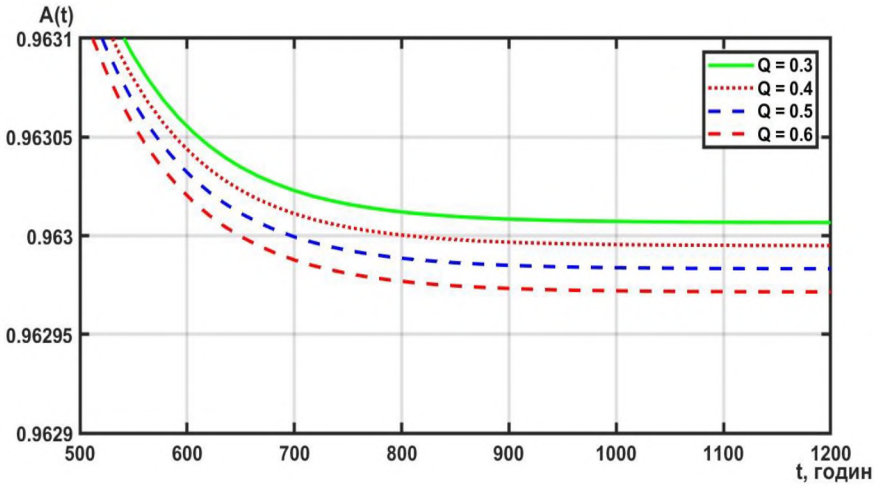


Рисунок 3.9 – Вплив параметра Q на критичність атак на інформаційну безпеку

Зелена лінія (Q = 0.3) починається з високого рівня критичності (0.963007), що може вказувати на меншу вразливість до атак при даному рівні параметра Q. Це може вказувати на те, що при менших значеннях Q система має високий рівень захисту від атак.

Червоний пунктир (Q = 0.4) вказує на динаміку критичності, яка зростає до визначеного пункту (0.962905). Це може вказувати на загострення ситуації при атаках зі значенням Q = 0.4, і це значення стає критичним для цілісності СУБД.

Синій пунктир (Q = 0.5) представляє рівень критичності при іншому значенні параметра Q (0.962983), що може вказувати на варіацію в інтенсивності атак. Високий рівень критичності залишається значущим при цьому значенні Q.

Червоний пунктир (Q = 0.6) ілюструє критичність атак при значенні Q = 0.6, призводячи до значення 0.962972. Це свідчить про те, що при більших значеннях Q критичність атак може залишатись на високому рівні.

На рисунку 3.10 проведено аналіз інтенсивності відновлення служби системи після установки патча з урахуванням різних значень параметра mu_path. Графік ілюструє залежність інтенсивності відновлення від величини mu_path для чотирьох різних сценаріїв.

Зелений пунктир (Mu = 0.3) графік цієї лінії демонструє ефективність відновлення служби при низькій інтенсивності mu_path (0.3). Кінцеве значення 0.963159 свідчить про високий рівень відновлення при цьому параметрі.

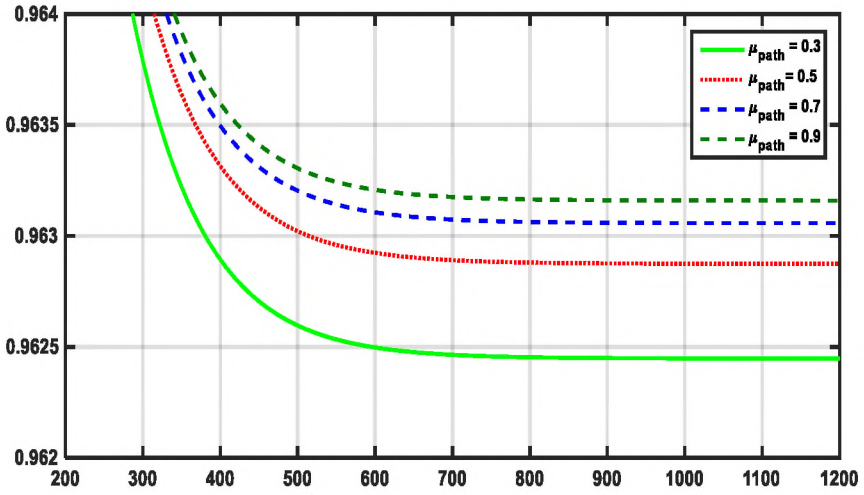


Рисунок 3.10 – Інтенсивності відновлення служби після патча

Синій пунктир (Mu = 0.5) лінія представляє динаміку інтенсивності відновлення для mu_path = 0.5. Завершальне значення 0.963057 вказує на можливі зміни у швидкості відновлення в порівнянні з Mu = 0.3.

Червоний пунктир (Mu = 0.7) графік відображає інтенсивність відновлення при mu_path рівному 0.7. Завершальне значення 0.962874 може вказувати на можливий спад ефективності відновлення при високому значенні mu_path.

Зелена лінія (Mu = 0.9) ця лінія ілюструє інтенсивність відновлення для величини mu_path = 0.9. Закінчення графіку значенням 0.962447 вказує на можливе зниження ефективності відновлення при великому mu_path.

Аналіз графіка дозволяє визначити, як різні рівні mu_path впливають на інтенсивність відновлення служби та може слугувати основою для оптимізації параметрів відновлення у системі.

## 3.4 Техніко-економічне обґрунтування запропонованих рішень

У сучасному цифровому світі, де обробка та передача інформації відіграють ключову роль в функціонуванні підприємств, забезпечення безпеки інформаційної системи є критично важливим завданням.

Розробка та впровадження ефективних стратегій моделювання цілісності даних та забезпечення безпеки інформаційної системи є невід'ємною частиною стратегічного управління на сучасних підприємствах. У зв'язку з великим ростом обсягів даних та зростанням кількості кіберзагроз, ці аспекти стають ключовими для забезпечення конфіденційності, цілісності та доступності інформації.

На технічному рівні однією з ключових складових є застосування передових технологій шифрування для забезпечення конфіденційності даних, які передаються та зберігаються в інформаційній системі. Важливим елементом також є системи автентифікації, які включають в себе різноманітні методи визначення і підтвердження ідентичності користувачів. Технічні аспекти також охоплюють використання мережевих та системних засобів захисту, що включають брандмауери, антивіруси та системи виявлення вторгнень.

Організаційні заходи безпеки включають в себе розробку та впровадження ефективних політик та процедур безпеки, спрямованих на правильну обробку та зберігання інформації. Регулярний моніторинг інформаційної системи стають ключовими елементами для виявлення потенційних загроз.

Людські ресурси грають важливу роль у забезпеченні безпеки, оскільки навчання та свідомість персоналу стають першочерговими заходами. Програми навчання мають охоплювати не тільки технічні аспекти безпеки, але й етичні питання та взаємодію персоналу з технічними засобами захисту.

Фізичні заходи безпеки включають у себе захист фізичного доступу до ключових точок доступу та серверних приміщень. Резервне копіювання та відновлення даних є важливою складовою для забезпечення доступності інформації в разі аварій.

На соціальному рівні, навчання персоналу виявляти та запобігати атакам, пов'язаним із соціальною інженерією, стає важливим завданням. Розробка політик інформаційної безпеки, які враховують аспекти соціальної взаємодії та залучають спільноту працівників, також є необхідною для впровадження комплексного підходу до забезпечення безпеки інформаційної системи.

Усі ці аспекти узгоджені та взаємодіють у комплексній системі забезпечення безпеки інформаційної системи, що враховує технічні, організаційні, людські, фізичні та соціальні вимоги та аспекти. Оновлення та вдосконалення цих заходів у відповідь на зміни у кіберзагрозах та технологічному середовищі стають важливою складовою для забезпечення ефективності та стійкості інформаційної системи.

Щоб гарантувати безпеку інформаційного середовища підприємства, треба систематично виконувати такі етапи:

1) оцінка можливих небезпек для ІБ;

– ідентифікація загроз – розпізнавання потенційних загроз безпеці, таких як хакерські атаки, віруси, соціальний інжиніринг тощо;

– оцінка вразливостей – аналіз існуючих вразливостей в інформаційній інфраструктурі та програмному забезпеченні;

– визначення ризиків – оцінка можливих наслідків та ймовірності виникнення загроз для прийняття рішень щодо пріоритетів захисту.

2) створення заходів для гарантування ІБ;

– розробка політик безпеки – визначення правил і процедур, які забезпечують безпеку інформаційного середовища;

– впровадження технічних заходів – встановлення захисних технологій, таких як антивірусне програмне забезпечення, брандмауери, системи виявлення вторгнень;

– навчання персоналу – проведення навчань з питань безпеки для працівників, щоб зменшити ризик людського фактору.

3) виконання запланованих заходів у реальному часі (рис. 3.10).

– моніторинг та реагування – моніторинг інформаційного середовища для виявлення проблем та швидка реакція на можливі інциденти;

– аудит та оновлення – регулярне проведення аудитів безпеки для перевірки ефективності заходів та вдосконалення їх у відповідності з новими загрозами [43].

Для визначення рівня інформаційної безпеки підприємства рекомендується провести діагностику у трьох напрямках:

– програмно-технічний захист інформації;

– оцінка компетентності персоналу в питаннях забезпечення інформаційної безпеки;

– оцінка інформаційної якості, яку отримують особи, що приймають рішення від інформаційної служби підприємства.

– оцінка інформаційної якості, яку отримують особи, що приймають рішення, від інформаційної служби підприємства.


Рисунок 3.10 – Етапи функціонування інформаційної безпеки підприємства

Для визначення рівня інформаційної надійності персоналу пропонується розраховувати кілька коефіцієнтів, таких як правова захищеність інформації, рівень досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, загальна надійність цього персоналу у справах інформаційної безпеки та рівень підготовленості персоналу до виявлення можливих загроз [44].

Для оцінки інформації, яку отримують особи, що приймають рішення від інформаційної служби підприємства, рекомендується використовувати такі показники:

– ступінь повноти інформації;

– точність інформації;

– рівень суперечливості в ній.

Наведена нижче система показників оцінки рівня інформаційної безпеки підприємства включає розрахункові формули та максимально допустимі значення для кожного з визначених напрямків [45].

Технічний захист інформації визначається коефіцієнтом захисту. $К_{Т.З.}$ за формулою:

$$К_{Т.З.} = IA_{Н.В} \tag{3.5}$$

де $IA_{Н.В.}$ – позначає кількість інформаційних атак, які не були відвернуті.

Програмний захист інформації визначається за допомогою коефіцієнта програмної захищеності $К_{П.З.}$ за формулою:

$$К_{П.З} = \frac{Чб.ф}{Ч_{н.ф}}, \tag{3.6}$$

де $Ч_{б.ф.}$ – період безперебійної роботи інформаційної системи яка вимірюється в годинах.

$Ч_{н.ф.}$ – стандартний час роботи інформаційної системи, який вимірюється в годинах.

Фінансовий захист інформації визначається за допомогою коефіцієнта фінансової безпеки $К_{ф.з}$ за формулою:

$$К_{ф.з} = \frac{Вз.ін}{В_{пр.ін}}, \tag{3.7}$$

де $В_{з.ін.}$ – фінансові витрати на захист інформаційних ресурсів, виражені в гривнях;

$В_{пр.ін.}$ – фінансові витрати на придбання інформаційних ресурсів, виражені в гривнях.

Рівень фінансування служб, що забезпечують інформаційні потреби підприємства, визначається за допомогою коефіцієнта фінансування інформаційних служб за формулою:

$$К_{фін} = \frac{В_{фін}}{R}, \tag{3.8}$$

де $В_{фін}$ – фінансові витрати на забезпечення фінансування інформаційних служб підприємства, виражені в гривнях.

Коефіцієнт правової захищеності інформації $К_{пр.з}$ обчислюють за формулою:

$$К_{пр.з} = \frac{I}{I_{юр.з}}, \quad (3.9)$$

де $I$ – обсяг інформації, викриття якої може призвести до негативних наслідків для підприємства, визначається в процентному співвідношенні.

$I_{юр.з.}$ – сумарний обсяг інформації, що підпадає під правовий захист.

Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства $К_{д.р.}$, обчислюють за формулою:

$$К_{Д.Р} = ЧП_1 / ЧП_З, \quad (3.10)$$

де $ЧП_1$ – кількість працівників, які працюють на підприємстві понад рік;

$ЧП_з$ – сумарна кількість осіб, які мають право доступу.

Ступінь надійності персоналу, який забезпечує безпеку інформації на підприємстві $К_{н.п.}$ обчислюють за формулою:

$$К_{н.п} = \frac{ЧП_{з.зв.} - Ч_{вип}}{ЧП_{з.зв.}}, \quad (3.11)$$

де $ЧП_{вип}$ – кількість осіб, які були звільнені у зв'язку з витоком інформації;

$ЧП_{З.зв.}$ – сукупна кількість осіб, які були звільнені.

Коефіцієнт рівеня готовності персоналу до виявлення потенційних небезпек або загроз обчислюється за формулою:

$$К_{н.п} = \frac{ЧП_{з.} - Ч_{п}}{ЧП_{з}}, \quad (3.12)$$

де $ЧП_п$ – кількість співробітників, які нечітко діяли, що веде до витоку інформації через низький рівень підготовки персоналу у виявленні загроз безпеки;

$ЧП_З$ – кількість працівників з правом доступу до конфіденційної інформації.

Коефіцієнт повноти інформації $К_{п.ін.}$ обчислюється за формулою:

$$К_{п.ін} = \frac{І_н}{І_{необ}}., \quad (3.13)$$

де $І_Н$ – обсяг інформації, яка знаходиться у володінні ОПР;

$І_{необ.}$ – процент необхідної інформації для прийняття обгрунтованого рішення.

Коефіцієнт точності інформації $К_{т.ін.}$ обчислюється за формулою:

$$К_{т.ін} = \frac{І_р}{І_н}, \quad (3.14)$$

де $І_р$ – відсоток інформації, яка є відповідною або актуальною;

$І_н$ – процент загального обсягу інформації, що знаходиться у володінні ОПР.

Коефіцієнт надійності інформації $К_{н.ін.}$ визначається за формулою:

$$К_{т.ін} = \frac{І_{н.д}}{І_{з.н}} \quad (3.15)$$

де $І_{н.д.}$– відсоток обсягу інформації, який надійшов до ОПР з достовірних джерел;

$І_{з.н.}$– відсоток всього обсягу інформації.

Кожне підприємство повинно встановити свої вимоги до забезпечення безпеки. У процесі оцінки цих вимог використовуються такі показники як:

– перший показник охоплює  показник охоплює оцінку ризиків, з якими підприємство зіштовхується. Це включає визначення потенційних загроз для інформації, її вразливостей, ймовірності виникнення ризикових ситуацій та можливих втрат;

– другий показник охоплює вимоги законодавства, які повинні бути виконанні підприємством та її партнерами, підрядниками та постачальниками послуг;

– третій показник включає конкретний комплекс принципів, цілей і вимог щодо обробки інформації, які розроблені підприємством для забезпечення підтримки її діяльності.

Методи опису і класифікації є важливими інструментами для аналізу стану забезпечення інформаційної безпеки. Для ефективного захисту системи управління інформаційною безпекою рекомендується спочатку детально описати різні види загроз а потім провести їх класифікацію. На основі цього аналізу можна розробити систему заходів з управління цими аспектами для забезпечення ефективного захисту.

Заходи безпеки організації включають витрати на різні компоненти, які спрямовані на забезпечення інформаційної безпеки підприємства:

1. Технічні засоби:

– антивірусне програмне забезпечення;

– фаєрволи та інші засоби захисту мережі;

– шифрування даних та з'єднань;

– системи виявлення вторгнень;

– засоби безпеки для апаратного забезпечення.

2. Організаційні заходи:

– розробка та впровадження політик безпеки;

– управління доступом до інформації;

– проведення аудитів безпеки;

3. Навчання персоналу:

– інструктажі з правил користування інформаційними ресурсами;

– тренінги для працівників з безпеки.

4. Фізичне забезпечення:

– контроль доступу до фізичних приміщень;

– відеоспостереження та системи безпеки будівлі;

– захисні пристрої для обладнання та серверних приміщень.

5. Соціальні заходи:

– соціальні кампанії з підвищення освітленості щодо кібербезпеки;

– психологічна підтримка для працівників у випадках інцидентів щодо безпеки.

У таблиці 3.2 вказані компоненти заходів безпеки та ціна.

Таблиця 3.2 – Компоненти заходів безпеки

| Компоненти заходів безпеки | Витрати (грн.) |
|---|---|
| Технічні засоби | 8000 |
| Організаційні заходи | 5000 |
| Навчання персоналу | 1000 |
| Фізичне забезпечення | 6000 |
| Соціальні заходи | 1000 |
| Загальні витрати | 21000 |

Отже загальна сума 21000 грн. це значні ресурси в заході безпеки, охоплюючи технічні, організаційні, освітні, фізичні та соціальні аспекти. Це свідчить про серйозний підхід до забезпечення комплексної безпеки, що включає в себе не лише технічні заходи, але й звернення уваги до організаційних та людських аспектів безпеки.

## Висновки до розділу 3

В даному розділі було розглянуто, що марковський процес – це процес який характеризується тим, що його простір станів є постійним, а розподіл ймовірностей Pk(i) залежить лише від результату попереднього кроку. Іншими словами, події в марковському процесі визначаються лише ймовірністю переходу з одного стану в інший на попередньому етапі.

Була наведена загальна модель станів інформаційної системи підприємства яка мала 5 станів де:

1) $S_1$ – працездатний стан інформаційної системи – означає, що вона працює так, як повинна, і виконує свої функції без проблем чи збоїв.

2) $S_2$ – працездатний стан інформаційної системи, коли на її компоненту починає здійснюватися кібератака (тобто стан «система під атакою).

3) $S_3$ – непрацездатний стан інформаційної системи, обумовлений відмовами її компонент через ненавмисні впливи (фізичні дефекти, програмні помилки та збої).

4) $S_4$ – непрацездатний стан інформаційної системи, обумовлений успіхом кібератаки на її компоненту.

5) $S_5$ – непрацездатний стан інформаційної системи у якому усуваються наслідки проведення кібератаки на її компоненту (відновлення даних, оновлення програмного забезпечення чи встановлення патчів безпеки).

Отже, у роботі було проведено детальний аналіз стану інформаційної безпеки підприємства. Встановлені порогові значення (0.998 та 0.99) дозволяють ефективно визначати прийнятний та критичний рівні безпеки відповідно. Порогове значення 0.965 представляє динаміку стану безпеки інформаційної безпеки при впливі атак, що можна вважати важливим індикатором для можливих загроз.

При дослідженні виявлено, що параметр Q має великий вплив на критичність атак на цілісність СУБД. Високі значення критичності можуть вказувати на загрози безпеці, особливо при певних значеннях параметра Q. Система виявляється менш вразливою до атак, і критичність залишається на високому рівні. Це може бути знаком того, що при низьких значеннях Q система має ефективний рівень захисту. При збільшенні значень параметра Q (представлене червоним пунктиром), критичність атак зростає, що може свідчити про загострення ситуації і вказує на критичний момент для цілісності СУБД.

Також при дослідженні виявлено, що різні параметри mu_path впливають на інтенсивність відновлення служби та може слугувати основою для оптимізації параметрів відновлення у системі. При збільшенні значень mu_path може відбуватися зниження ефективності відновлення служби системи. Результати вказують на важливість оптимального вибору значення mu_path для забезпечення максимальної ефективності відновлення служби після встановлення патча.

# ВИСНОВКИ

У процесі виконання роботи її мета була досягнута, а завдання вирішені. Робота включала в себе розробку комплексного підходу до гарантування цілісності даних та захисту інформаційної системи. Цей підхід призначений для надання підприємствам ефективних засобів протистояння сучасним викликам і загрозам в галузі інформаційної безпеки.

В першому розділі було розглянуто перехід від локальних до хмарних інформаційних систем, який визначає етап в розвитку технологій. Досліджено склад та завдання сучасної інформаційної системи та її роль в продуктивності діяльності підприємства. В останньому пункті розглянуто стандарти інформаційної безпеки та які завдання вони виконують.

В другому розділі розглянуто загальний підхід до забезпечення цілісності даних який передбачає поєднання технічних, організаційних та людських ресурсів для ефективного управління та реагування на потенційні загрози. Розглянуто що таке хешування та яка його суть у сфері цілісності даних та ідентифікації.

В третьому розділі було проведено детальний аналіз стану інформаційної безпеки підприємства. Встановлені порогові значення дозволяють ефективно визначати прийнятний та критичний рівні безпеки відповідно. Порогове значення при впливі атак представляє динаміку стану безпеки інформаційної безпеки, що можна вважати важливим індикатором для можливих загроз. параметр Q має великий вплив на критичність атак на цілісність СУБД. Високі значення критичності можуть вказувати на загрози безпеці, особливо при певних значеннях параметра Q. Параметри mu_path впливають на інтенсивність відновлення служби та може слугувати основою для оптимізації параметрів відновлення у системі.

Напрямком подальших досліджень є проведення аналізу впливу різних значень параметрів на цілісність інформаційної безпеки. Ці значення повинні не лише забезпечувати цілісність СУБД, але й забезпечувати оптимальний баланс між безпекою та ефективністю системи.