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

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ВИБІР ЗАСОБІВ РЕЗЕРВНОГО ЗБЕРЕЖЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Виконала: студентка групи 2К-21
Спеціальності 123 Комп’ютерна інженерія
Дар’я КОСТОЛОМОВА
Керівник:
Маргарита МЕДОЛИЗ

Черкаси 2025

АНОТАЦІЯ

У роботі розглянуті теоретичні аспекти стосовно виборів засобів резервного збереження інформаційних систем.

Метою роботи є отримання знань і навичок з вибору та реалізації засобів резервного збереження інформаційних систем.

Для досягнення мети було проведено аналіз сучасних засобів резервного збереження інформаційних систем, моделювання інформаційних систем та застосування на ці моделі засоби резервного збереження. В якості засобу моделювання була застосована програма моделювання інформаційних систем Modelio.

Ключові слова: MODELIO, РЕЗЕРВНА КОПІЯ, ХМАРНІ СЕРВІСИ, RAID-МАСИВ, ТІНЬОВА КОПІЯ.

ANNOTATION

The paper considers theoretical aspects regarding the selection of backup storage facilities for information systems.

The purpose of the paper is to obtain knowledge and skills in the selection and implementation of backup storage facilities for information systems.

To achieve the goal, an analysis of modern backup storage facilities for information systems, modeling of information systems and application of backup storage facilities to these models was conducted. The Modelio information systems modeling program was used as a modeling tool.

Keywords: MODELIO, BACKUP, CLOUD SERVICES, RAID ARRAY, SHADOW COPY.

ЗМІСТ

ВСТУП

Різні системи оточують людину скрізь. Достатньо глянути на цей аркуш паперу, що є результатом роботи багатьох систем, і не тільки інформаційних. Мова, чорнила, папір, засоби друку, інформаційні технології – все це результати окремих систем, які в XXI столітті дозволяють людині створювати необмежену кількість засобів реалізації власних потреб. Сукупність оточуючих людину систем і є для неї світ.

Варто зауважити, що певні системи мають надзвичайно цінні дані, втрата яких може призвести до катастрофи в своїх масштабах. Сюди входять системи міжнародних організацій, держав, банків, закладів освіти. Для гарантії збереження даних і використовуються засоби резервного збереження.

У сучасному світі ми вже не уявляємо життя без інформаційних технологій. Вони супроводжують нас на кожному кроці – від банківських операцій до зберігання медичних даних, від систем освітнього процесу до великих міжнародних корпорацій. Інформаційні системи стали невід'ємною частиною всієї інфраструктури сучасного суспільства. Зі збільшенням обсягів даних та зростанням залежності від їх постійної доступності постає критично важливе завдання – забезпечити їх збереження, доступність та цілісність у будь-яких умовах

Резервне збереження даних дозволяє мінімізувати наслідки технічних збоїв, помилок користувачів, атак шкідливого програмного забезпечення або природних катастроф. Наявність актуальних резервних копій забезпечує можливість швидкого відновлення інформації та зменшує ризики втрати критичних даних.

У зв'язку з широким розмаїттям доступних засобів резервного копіювання від локальних апаратних рішень до хмарних сервісів і гібридних моделей виникає проблема оптимального вибору такого інструменту для конкретної інформаційної системи. Цей вибір має базуватися на технічних, економічних та організаційних критеріях, а також враховувати особливості функціонування

самої системи.

Одним з найефективніших механізмів захисту від втрати інформації є впровадження систем резервного копіювання. Саме резервне збереження дозволяє гарантувати відновлення даних після збою та мінімізувати простої інформаційної системи. Проте вибір конкретного засобу резервного збереження має здійснюватися з урахуванням технічних можливостей, потреб користувача, рівня критичності даних, бюджету та безпекових вимог.

Об’єктом дослідження є інформаційні системи, які потребують резервного збереження даних.

Предметом засоби, методи та технології, які забезпечують таке збереження. Метою роботи є аналіз існуючих рішень у сфері резервного копіювання та обґрунтований вибір найоптимальнішого з них для конкретних умов функціонування інформаційної системи.

Метою роботи є дослідження сучасних засобів резервного збереження та обґрунтований вибір оптимального рішення для конкретних інформаційних систем.

Для досягнення мети будуть виконані наступні завдання:

- проведення аналізу сучасних засобів резервного збереження інформаційних систем,
- моделювання інформаційних систем,
- застосування засобів резервного збереження на змодельовані інформаційні системи,
- оцінка застосованих засобів.

Основна мета резервного копіювання – це відновлення роботи інформаційних систем після збоїв, спричинених апаратними поломками, програмними помилками, кібератаками, стихійними лихами або людським фактором. Робота дозволяє обрати оптимальні засоби, що мінімізують час простою та втрати даних, а отже, забезпечують безперервність бізнес-процесів. Основна мета резервного копіювання – це відновлення роботи інформаційних систем після збоїв, спричинених апаратними поломками, програмними

помилками, кібератаками, стихійними лихами або людським фактором. Робота дозволяє обрати оптимальні засоби, що мінімізують час простою та втрати даних, а отже, забезпечують безперервність бізнес-процесів.

Практичне значення роботи полягає у наданні методологічної основи для обґрунтованого вибору та ефективного впровадження рішень з резервного копіювання, що є критично важливим для забезпечення стабільності та успіху будь-якої сучасної організації. Впровадження добре продуманої стратегії резервного копіювання та відновлення, заснованої на висновках роботи, підвищує загальну надійність та стійкість інформаційних систем до різних видів загроз.

Ні для кого не є секретом, що ризики втрати даних зростають пропорційно до їх кількості. Збої обладнання, помилки користувачів, вірусні атаки, стихійні лиха чи навіть банальна людська неуважність – усе це може призвести до непоправних наслідків, якщо організація не має надійної системи резервного збереження. У сучасних умовах навіть кілька годин простою можуть призвести до фінансових збитків, втрати клієнтів або репутаційних ризиків. Саме тому резервне копіювання стало не просто корисною практикою, а життєво необхідною умовою безперебійної роботи інформаційної системи.

У межах дослідження буде проведено теоретичний аналіз поняття резервного копіювання, вивчено сучасні підходи, змодельовано типову інформаційну систему та випробувано на ній різні варіанти резервного збереження з подальшою оцінкою ефективності. Практичне значення роботи полягає в тому, що її результати можуть бути застосовані для створення або вдосконалення політик резервного копіювання в організаціях, що працюють з критичними даними.

РОЗДІЛ І
ОГЛЯД ПОНЯТТЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА ЗАСОБІВ РЕЗЕРВНОГО ЗБЕРЕЖЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

У сучасному інформаційному суспільстві термін "інформаційна система" став загальновживаним, хоча його зміст є значно ширшим, ніж здається на перший погляд. Інформаційна система – це сукупність взаємопов’язаних елементів, яка забезпечує збір, обробку, зберігання, передачу та представлення інформації з метою підтримки процесів прийняття рішень, управління та контролю. Ці системи можуть мати різне призначення: від простих баз даних до складних багаторівневих архітектур підприємств, банківських установ, державних організацій тощо.

Загалом, структура типової інформаційної системи включає апаратне забезпечення (сервери, комп’ютери, мережеве обладнання), програмне забезпечення (операційні системи, прикладні програми, бази даних), інформаційні ресурси (дані, документи, файли), а також персонал, який забезпечує функціонування системи. Усі ці компоненти взаємодіють у межах визначених правил та процедур, формуючи єдиний механізм для ефективного управління інформацією.

З розвитком цифрових технологій зростає і значення інформаційних систем. У багатьох сферах діяльності саме інформація стала основним ресурсом, від якого залежить успішність і конкурентоспроможність. Втрата доступу до критично важливих даних, навіть на короткий період, може мати катастрофічні наслідки – від фінансових втрат до повної зупинки бізнес-процесів. У зв’язку з цим зростає роль засобів резервного збереження, які дають змогу захистити інформацію від втрати та швидко відновити її у разі необхідності.

Під засобами резервного збереження слід розуміти сукупність технічних і програмних рішень, що дозволяють створювати копії даних з метою їх подальшого відновлення. Залежно від типу інформаційної системи, обсягів даних, вимог до безпеки та часу відновлення, засоби резервного копіювання

можуть значно відрізнятися. Найбільш поширеними сьогодні є локальні засоби (зовнішні носії, мережеві накопичувачі), віддалені сервери, хмарні сервіси та гібридні моделі, які поєднують декілька підходів.

Резервне збереження є частиною загальної стратегії управління ризиками в інформаційних системах. Воно виконує дві основні функції: запобігання втраті даних і забезпечення швидкого відновлення системи після інциденту. Завдяки цьому зберігається цілісність, доступність і конфіденційність інформації – три основоположні принципи інформаційної безпеки.

Не менш важливо зазначити, що вибір засобу резервного копіювання не є універсальним. Те, що є ефективним для малого підприємства, може виявитися недостатнім для великої корпорації з розподіленою інфраструктурою. Тому в процесі проектування систем резервного збереження враховуються такі чинники, як масштаб інформаційної системи, її критичність для бізнесу, наявні ресурси, а також технічна кваліфікація персоналу.

У цьому розділі буде розглянуто базові поняття, пов’язані з інформаційними системами, їхньою структурою, функціями та класифікацією. Крім того, детально проаналізовано різновиди засобів резервного копіювання, принципи їхньої роботи, переваги та обмеження кожного з підходів, а також загальні вимоги до сучасних систем резервного збереження, що дає змогу зрозуміти, чому саме ця тема є критично важливою для стабільного функціонування цифрової інфраструктури.

1.1 Аналіз поняття інформаційної системи

Інформаційна система – сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

Спершу під інформацією розуміли відомості, що передаються усним, письмовим чи іншим способом (за допомогою певних сигналів, технічних

засобів тощо). Тепер прийнято, що інформаційні взаємодії складають основу всіх процесів керування у системах будь-якої природи. Тобто, кожну систему можна представити у вигляді інформаційної системи.

Структура інформаційних систем складається з:

– Засобів фіксації і збору інформації;
– Засобів передачі відповідних даних та повідомлень;
– Засоби збереження інформації;
– Засоби аналізу, обробки і представлення інформації

Також, існує класифікація інформаційних систем за різними ознаками. Так за ступенем автоматизації виділяють ручні інформаційні системи – всі операції з обробки інформації виконуються людиною. Автоматизовані інформаційні системи – частина операцій керування або опрацювання даних здійснюється без участі людини, а інша – людиною. Автоматичні інформаційні системи – всі функції керування й опрацювання даних здійснюється без участі людини.

За сферою призначення є економічні інформаційні системи – призначені для виконання фінансових функцій на підприємстві, медичні, географічні, адміністративні, виборчі, навчальні інформаційні системи тощо.

За місцем діяльності інформаційних систем розділяють наукові – створені для автоматизації діяльності науковців, аналізу статистичної інформації, керування експериментом; інформаційні системи автоматизованого керування – призначені для автоматизації праці інженерів-проєктувальників і розробників нових технічних засобів. Такі інформаційні системи допомагають здійснювати: розробку нових виробів, інженерні розрахунки, графічну документацію, моделювання спроєктованих об’єктів, створення керуючих програм для верстатів. Ще існують інформаційні системи організаційного керування – призначені для автоматизації функцій адміністративного персоналу, інформаційні системи керування технологічними процесами – призначені для автоматизації технологічних процесів (металургія, енергетика тощо).

Існує класифікація за функціональним призначенням: керувальні, проєктувальні, наукогового пошуку, діагностичні, моделювальні, системи

підготовки прийняття рішень [1] – система, що через збирання і аналіз великого обсягу інформації може впливати на керівничі рішення в бізнесі та підприємстві.

1.2 Аналіз поняття засобів резервного збереження інформаційних систем

Засоби резервного збереження інформаційних систем – це сукупність технічних, програмних і організаційних засобів, що призначені для створення копій даних (резервних копій), їхнього зберігання і подальшого відновлення у випадку втрати даних.

Вони є ключовим елементом у забезпеченні захисту інформаційних систем і гарантією надійності, безперервності роботи за збереження цілісності даних. При цьому варто розуміти, що під втратою даних розуміється певна подія, що призвела до зміни даних, після чого вони втратили цінність або були видалені. Наприклад, умисне видалення важливої для підприємства інформації, що призвело до надлишкових витрат або втрати прибутку.

Першочерговою метою резервного збереження даних є їх відновлення, що передбачає можливість повернення до попереднього, працездатного стану інформації та систем після непередбачених подій. Цей процес тісно пов'язаний із запобіганням втраті даних, мінімізуючи обсяг втраченої інформації між моментом збою та останнім успішним резервним копіюванням. Зрештою, це все спрямовано на забезпечення безперервності бізнесу, дозволяючи швидко відновити критичні бізнес-процеси та функції після аварії, тим самим скорочуючи час простою.

Крім того, резервне копіювання допомагає дотримуватися нормативних вимог (Compliance), задовольняючи законодавчі та регуляторні вимоги щодо зберігання, доступності та цілісності даних, як-от Загальний регламент про захист даних (General Data Protection Regulation), Стандарт безпеки даних індустрії платіжних карток (PCI DSS) [18] тощо. Це також є життєво важливим інструментом для захисту від кібератак та вірусів-шифрувальників, оскільки

наявність чистих копій даних, не вражених шкідливим програмним забезпеченням, дозволяє відновити роботу без сплати викупу. Не менш важливим є й відновлення після людської помилки, що дає змогу виправити випадкові видалення, перезаписи або неправильні конфігурації, здійснені користувачами чи адміністраторами.

Об’єктом цих засобів є дані або сукупність даних, з яких можна створити резервну копію. Це можуть бути файли, дані прикладних програм, дані операційної системи, сама операційна система тощо.

1.3 Основні характеристики засобів резервного збереження інформації

Для об’єктивного оцінювання засобів резервного збереження інформаційних систем встановлено конкретні критерії. Варто зауважити, що в певні системи можна вводити лише певні засоби резервного збереження інформації. Тобто, сенс порівнювати засоби резервного збереження інформаційних систем з’являється лише для засобів, які можна інтегрувати в одну і ту саму інформаційну систему. Цими критеріями є: Recovery Point Objective (PRO) – цільова точка відновлення – визначає періодичність створення резервних копій. Тобто, це певна точка, яка зберігає дані у тому стані, коли ця копія була створена; Recovery Time Objecitve (RTO), цільовий час відновлення – визначає необхідний час відновлення даних з початку і до кінця.

Окремо виділяють характеристики у разі катастрофи: Disaster Recovery Point Objective (DRPO) – RPO у разі настання катастрофи. Це точка відновлення, яка гарантовано дозволить повернути працездатність системи у випадку катастрофи; Disaster Recovery Time Objective (DRTO) – RTO у разі настання катастрофи, тобто необхідний час для повернення на точку відновлення у разі катастрофи.

Також виділяються різні рівні резервного копіювання:

Повне резервне копіювання (L0) – повна копія даних. Рівень, який

забезпечує створення повної копії об’єкта резервування. Зберігає файли незалежно від того, чи були вони змінені з часу останнього резервного копіювання. Є базовою точкою для подальших рівнів резервних копій. Є найпростішим та самим надійним варіантом резервування, час відновлення з ним стає самим швидким (адже необхідна лише одна копія, і нічого більше). Проте, потребує великого простору в зв’язку з великим об’ємом інформації, і відповідно вимагає найбільше часу для створення копії в порівнянні з наступними рівнями;

Диференційне резервне копіювання (L1) – копіювання змін, що були зроблені після створення останньої повної копії. Такий спосіб зменшує об’єм даних, що резервуються. Це дозволяє швидше проводити процес резервування даних, але збільшує час відновлення даних (адже спочатку відновлюється повністю система, а потім всі внесені зміни). Є альтернативою між повним резервуванням і додатковим;

Додаткове резервне копіювання (L2) – копіювання змін, що відбулись після повного, диференційного або додаткового копіювання. На такому рівні резервування відбувається швидше за попередні, але процес відновлення даних займає найбільше часу (оскільки спочатку відновлюються дані повної копії й після цього – всі резервні копії подій у системі). З використанням цього рівня значно збільшується складність відновлення, оскільки спочатку необхідно відновити дані в інкрементальному порядку від L0 до L2 в правильному порядку. Якщо L2-копія пошкоджена, то при відновленні наступних копій можуть ставатись помилки. Проте, все-таки є найефективнішим методом резервування в системах з великою кількістю змін, де часто доводиться зберігати дані;

Level X (Lx) – це один із стандартів описання методів резервного копіювання, де наступний рівень Lx завжди залежить від попереднього. Наприклад, у разі наступної послідовності резервних копій L0, L5, L3, L2, L4, процедура відновлення на останню резервну копію буде відбуватись у такій послідовності: L0, L2, L4. Дозволяє більш гнучко налаштовувати резервну політику, але більш складне у керуванні. Добре підходить для великих корпоративних систем з багаторівневим захистом.

1.4 Принципи створення резервної копії інформаційної системи

Окрім цього, резервування даних також має гарантувати цілісність резервних копій даних – відповідність даних резервної копії та оригіналу на момент створення копії (мають зберігатись контрольні суми або криптографічні хеші для порівнянна з оригіналом, що точно дозволяє впевнитись в цілісності копії). Якщо було обрано неправильний метод створення резервної копії, неможливо буде відновити дані у разі потреби. Для забезпечення цілісності резервних копій використовують різні методи, в залежності від об'єкта резервного копіювання. Серед них: забезпечити незмінність даних під час створення копії: контрольні суми збереженої копії та оригіналу мають бути відповідними, розблокувати дані для можливості читання – програмна частина інформаційної системи не має створювати перешкод у разі створення резервних копій; зміни, які були зроблені поки ще в оперативній пам'яті, записати на накопичувач. Інакше деякі частини об'єкта можуть не відповідати змінам, які вже були виконані.

Наприклад, при створенні резервної копії файлів в операційній системі Windows, неможливо отримати доступ до деяких системних файлів, які використовуються в системі, але, завдяки технології Volume Shadow Copy Services, перед початком копіювання може бути виконана процедура тіньової копії тому. Таким чином, для копіювання буде використовуватись не оригінальний том, а його тіньова копія.

В разі неправильного підходу до резервування можуть виникнути наступні проблеми: пошкоджені дані копії, втрата критичних даних, неможливість застосування резервної копії в зв'язку з відсутності цілісності.

1.5 Методи передачі даних і створення резервних копій, та засоби зберігання резервних копій

Необхідно виділити три ключових елемента створення резервної копії: метод передачі резервних копій, метод створення резервної копії та засоби зберігання резервної копії. Правильний вибір цих компонентів при налаштуванні політики резервного збереження є ключовим.

Існують різні методи передачі резервних копій. Перший це метод передачі резервних копій з використанням агента – копіювання здійснюється за допомогою частини програмного забезпечення, що встановлюється з боку системи, резервну копію якої необхідно провести. Дозволяє налаштовувати детальний контроль та прямо інтегрувати в клієнтські додатки, але буде мати додаткове навантаження на клієнтську систему.

Off-host – цей метод дозволяє створювати резервну копію без значного навантаження на клієнтську систему. Дані безпосередньо передаються зі сховища даних на сервер резервного копіювання. Дозволяє зменшити навантаження на клієнтську систему, але потребує необхідних підтримок технологій з боку сховища.

Serverless – метод, що дозволяє передавати дані від клієнта у сховище резервних копій без участі сервера резервного копіювання. Цей метод використовується для зменшення навантаження на сервер резервного копіювання. Самий ефективний за ресурсами варіант, але більш складний в налаштуванні.

Також, варто виділити загальні методи створення резервних копій: Тіньова копія – створення миттєвої копії з дискового розділу операційної системи, в операційній системі Windows таку можливість дозволяє реалізувати Volume Shadow Copy Services; Snapshot дисків – замороження змін на основному диску та перенаправлення цих змін в окремий файл під час створення резервної копії, дозволяє отримати точну копію стану без зупинки роботи системи; Snapshot дискового розділу – створення миттєвої копії даних безпосередньо на масиві

накопичувачів. Використовуються RAID-контролери або NAS/SAN-системи, що забезпечує майже миттєве створення копій, мінімізує вплив на роботу системи і не зменшує її продуктивність.

Засоби зберігання резервної копії:

Апаратні засоби: жорсткі диски – класичний і самий доступний варіант для локального зберігання даних; SSD – швидші за HDD та мають більшу вартість, використовуються у разі потреби в більшій швидкості доступу [4]; NAS-системи – мережеві сховища, які дозволяють централізоване збереження, якщо клієнтів більше ніж один [5]; RAID-масиви – поєднання декількох незалежних дисків, що дублюють інформацію та дозволяє зберегти дані у разі виходу одного диску з ладу [6]; інші накопичувачі та масиви накопичувачів;

Програмні засоби: Windows Backup (вбудована в операційну систему Windows), Time Machine (вбудована в macOS), Acronis True Image (прикладна програма для резервування даних);

Загальні характеристику цих зособів можна відобразити у таблиці 1.5.1

Таблиця 1.5.1 – Порівняльна таблиця програмних засобів

Засіб	Тип	OS	Рівень користувача	Основні переваги	Основні обмеження
Windows Backup	Вбудований	Windows	Початковий	Простота, безкоштовність	Обмежена функціональність
Time Machine	Вбудований	macOS	Початковий	Інкрементне копіювання, інтеграція	Працює лише на macOS
Acronis True Image	Стороннє ПЗ	Windows/ macOS	Середній/профі	Шифрування, кіберзахист, хмара	Платне, складніше налаштування

Хмарні сервіси: Google Drive, OneDrive, Dropbox, Mega (дані резервуються на сторонніх сервісах);

Virtual Tape Library (VTL) – технологія резервного збереження даних, що імітує традиційну стрічкову бібліотеку, але використовує сучасні накопичувачі. Працює на програмному рівні, дозволяє значно збільшити кількість одночасних операцій і забезпечує велику швидкість доступу до даних. [3]

РОЗДІЛ ІІ
МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Перш ніж розробляти ефективну стратегію резервного збереження, важливо детально дослідити структуру та логіку побудови сучасних інформаційних систем. Їхнє моделювання дозволяє зрозуміти, як саме працює система, з яких компонентів вона складається, як ці елементи взаємодіють між собою, і які з них є критичними з точки зору збереження та безперебійного функціонування.

Типова інформаційна система може мати найрізноманітнішу архітектуру – від традиційних монолітних рішень і клієнт-серверних конфігурацій до сучасних багаторівневих, мікросервісних або повністю хмарних платформ. У контексті резервного копіювання важливо не лише класифікувати систему за її структурою чи масштабом, а й розуміти, наскільки критичними є її дані, які залежності існують між сервісами, та наскільки швидко система має відновитися у разі збою.

До найпоширеніших елементів ІС належать системи управління базами даних – як реляційні (MySQL, PostgreSQL, Oracle, MS SQL), так і нереляційні NoSQL-системи (MongoDB, Cassandra), що зберігають величезні масиви структурованої інформації. Сюди ж відносяться файлові сервери, мережеві сховища (NAS, SAN), що забезпечують зберігання документації, мультимедіа, резервних архівів. Важливу роль відіграють поштові сервери (наприклад, Exchange), веб-сервери (Apache, Nginx), а також прикладні системи – CRM, ERP, HRM. Зростання популярності віртуалізації (VMware, Hyper-V) і контейнеризації (Docker, Kubernetes) також вплинуло на підхід до копіювання, оскільки ці технології вимагають специфічного підходу до збереження стану віртуальних машин, контейнерів та конфігураційних файлів.

Моделювання ІС дозволяє визначити, які компоненти є критичними. Це можуть бути не тільки бази даних або користувацькі файли, а й конфігурації, налаштування операційних систем, журнали доступу, ключі шифрування,

ліцензії та інше. У складних системах відновлення лише одного елемента – наприклад, бази даних без конфігурацій застосунку – не забезпечить повноцінної працездатності. Тому важливо оцінювати ІС як цілісний живий механізм, де всі частини взаємозалежні.

Після моделювання настає етап формалізації вимог до резервного копіювання. Основні показники, які тут враховуються, – це RPO (Recovery Point Objective), що визначає допустимий обсяг втрати даних, і RTO (Recovery Time Objective), який показує, за який час система повинна бути повністю відновлена після збою. Ці параметри напряму залежать від важливості ІС для бізнес-процесів. Наприклад, для банківських систем RPO і RTO можуть вимірюватися хвилинами, тоді як для архівів документів – годинами або навіть днями.

Окрім RPO та RTO, визначаються строки зберігання копій, їхня періодичність, масштабованість системи, обсяги даних у перспективі, а також вимоги до безпеки – включаючи шифрування, контроль доступу, захист від несанкціонованих змін (наприклад, використання технологій immutability).

Сучасні підходи до резервного копіювання включають як повне (Full), так і диференційне (Differential) та інкрементне (Incremental) копіювання. Все частіше застосовуються блокові копії, знімки (snapshots), а також системи безперервного захисту даних (CDP), що дозволяють звести втрати до нуля. Вибір підходу залежить від структури ІС, її навантаження та обсягу даних.

Інструменти резервного збереження також обираються індивідуально. Наприклад, для віртуальних середовищ ефективними є рішення на кшталт Veeam, для комплексного резервування гібридної інфраструктури – Acronis або Commvault. Важливими функціями є дедуплікація, компресія, централізоване управління та верифікація цілісності копій.

Що стосується фізичного зберігання, то можливі різні варіанти: від стрічкових накопичувачів для довготривалого архівування, до високошвидкісних масивів HDD/SSD для швидкого відновлення, і аж до хмарних платформ (AWS, Azure, Google Cloud), які забезпечують надійність, масштабованість і географічну рознесеність.

Усі ці елементи повинні поєднуватися в єдиний документований план аварійного відновлення – Disaster Recovery Plan, який передбачає чіткі сценарії для кожної змодельованої ІС. План повинен регулярно тестуватися та оновлюватися, аби гарантувати готовність системи до відновлення в будь-якій кризовій ситуації.

Окрему увагу сьогодні привертають новітні технології, що поступово змінюють уявлення про збереження даних. Наприклад, використання блокчейн-рішень (Storj, Filecoin) для децентралізованого зберігання резервних копій з мінімальною довірою до централізованих провайдерів, або технології квантового шифрування (QKD), що унеможливлюють перехоплення критичної інформації.

Нарешті, ШІ та машинне навчання стали невід'ємною частиною «розумних» систем резервного копіювання. Завдяки ним, системи можуть адаптувати частоту копіювання, самостійно виявляти потенційні загрози та навіть формувати звіти про ризики втрати даних. Ці функції особливо важливі для великих корпоративних мереж, де обсяг даних щоденно змінюється.

Таким чином, моделювання інформаційних систем є необхідним етапом для розуміння їхньої структури та визначення оптимальних рішень резервного збереження. Без глибокого аналізу та правильної моделі неможливо створити ефективну, безпечну та стійку до загроз систему захисту даних. Саме детальне моделювання дозволяє підготуватися до найгірших сценаріїв і гарантувати відновлення інформаційної інфраструктури незалежно від характеру збою.

2.1 Методологія дослідження та вибір інструментів моделювання

В якості методології дослідження теми роботи, було обрано моделювання з використанням мови моделювання UML, адже лише таким методом можна досконало дослідити зміни, які вводять засоби резервного збереження інформаційних систем.

В якості інструменту побудови UML-діаграм було обрано Modelio –

сучасне середовище моделювання з відкритим кодом. Цей інструмент підтримує можливість створення логічних та фізичних моделей, підтримує велику кількість розширень та має безкоштовну ліцензію з відкритим кодом.

2.2 Пояснення формату відображення змодельованих інформаційних систем

Кожний елемент (вузол) інформаційної системи позначається прямокутником та підписується. Зв’язки між вузлами відображаються за допомогою ліній проведених між ними і стрілками, що показують напрям куди прямує інформація та для чого саме вона передається (див. рис. 2.2.1).

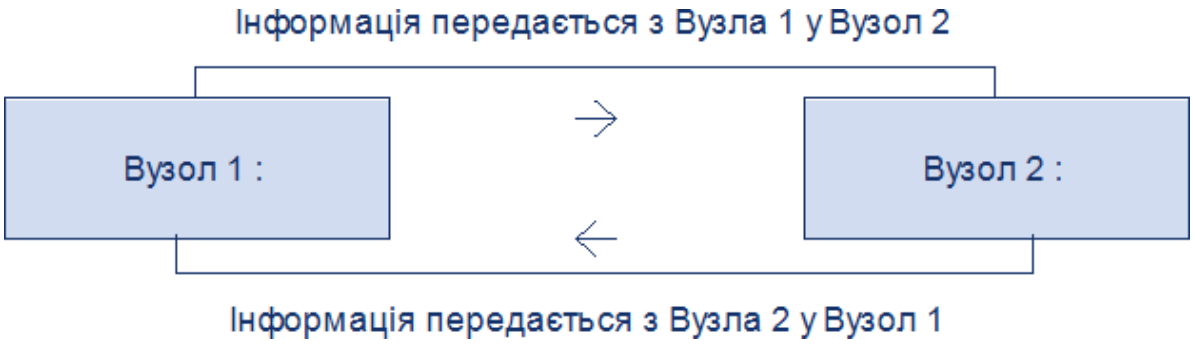

Рисунок 2.2.1 – Демонстрація інформаційної взаємодії вузлів інформаційної системи.

Опціонально до вузлів можуть додаватись описи, які дадуть більше інформації про вузол та матимуть значення при застосуванні засобів резервного збереження інформації (див. рис. 2.2.2).

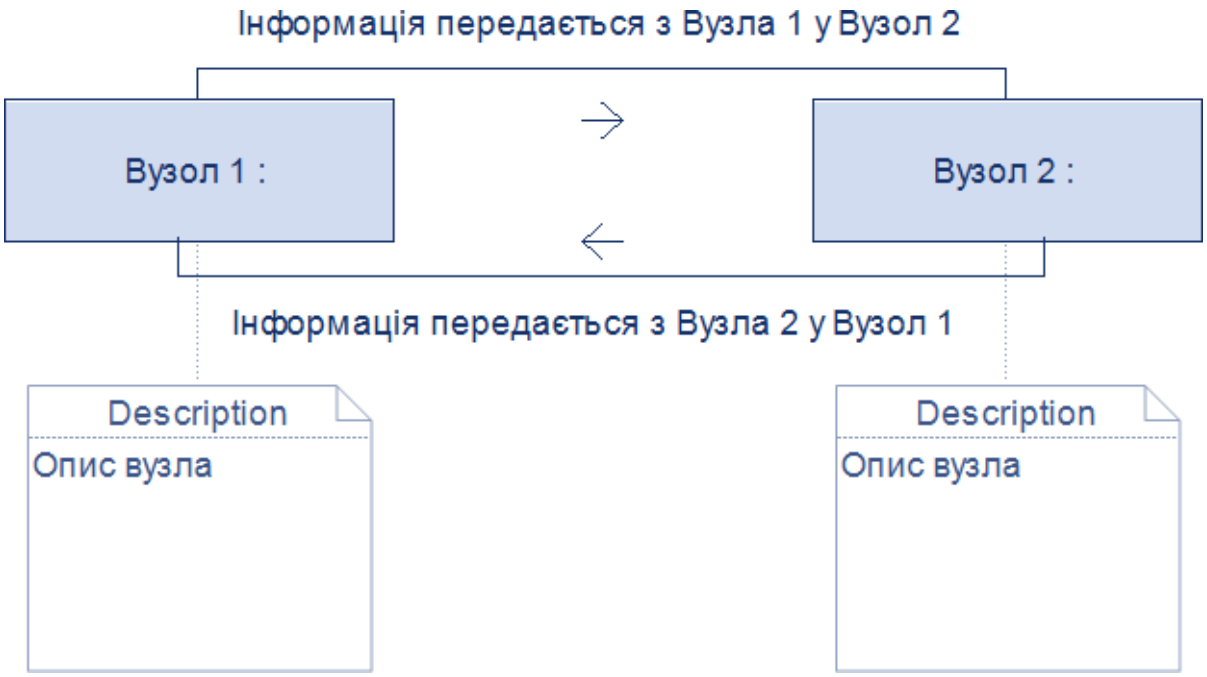

Рисунок 2.2.2 – Демонстрація як відображається опис вузлів інформаційної системи.

У разі рівноправного обміну інформації та відсутності необхідності в контексті передачі даних, зв’язки між вузлами можуть підписуватись як «взаємний інформаційний обмін» (див. рис. 2.2.3).

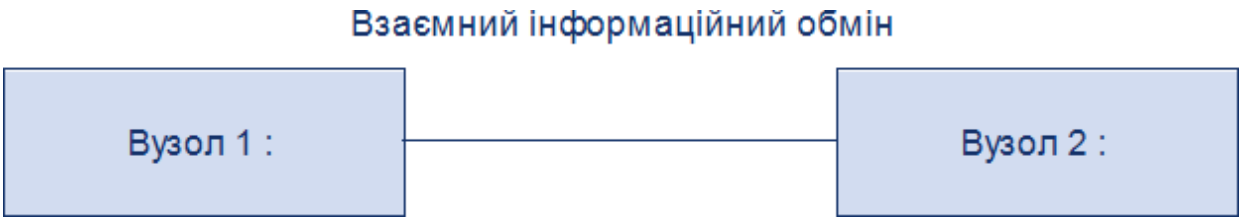

Рисунок 2.2.3 – Демонстрація взаємного інформаційного обміну вузлів інформаційної системи.

Варто зауважити, що представлені далі моделі інформаційних систем відображають лише необхідні для розуміння вузли та зв’язки, що дозволить не перенасичувати моделі непотрібними для роботи речами та дадуть змогу зосередитись на важливих деталях, що стосуються теми роботи.

2.3 Створення типових інформаційних систем та їх аналіз

Кожне дослідження має в свою чергу також мати практичне значення. Саме тому були побудовані типові інформаційні моделі, які можна буде зустріти в реальному житті.

Перша модель, що була створена, представляє типову організацію накопичувачів на сучасному домашньому ПК (див. рис. 2.3.1). Жорсткий диск та SSD-накопичувач представляють собою ключовими зберігачами інформації, які в контексті резервного збереження можуть потребувати засобів резервування для забезпечення надійності збереження інформації.

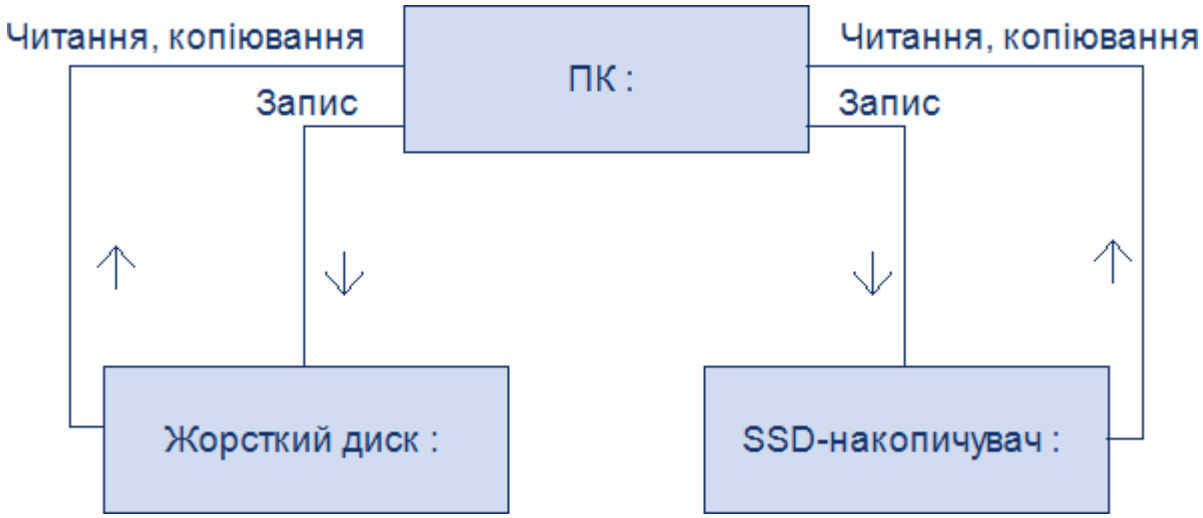

Рисунок 2.3.1 – Модель організації накопичувачів на домашньому ПК.

Друга модель представляє собою невелику локальну мережу (див. рис. 2.3.2). В ній використовується клієнт-серверна архітектура, в центрі якої стоїть сервер, до якого під’єднані клієнти. В контексті цієї роботи немає різниці які клієнти підключені до серверу, а інтерес представляє лише сервер, адже це найважливіший вузол системи, несправність якого призведе до зупинки роботи всієї мережі.

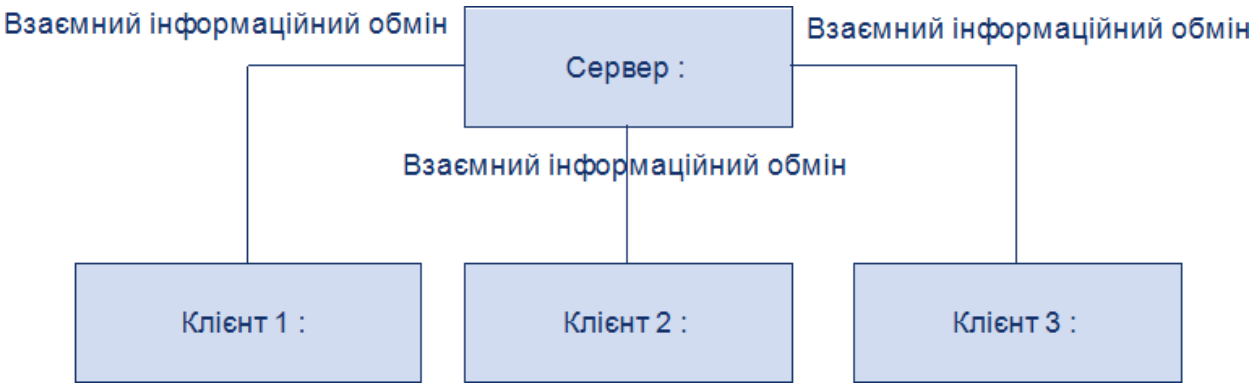

Рисунок 2.3.2 – Модель локальної клієнт-серверної мережі.

Створених моделей має бути достатньо для демонстрації засобів резервного збереження. Змодельовані приклади представляють більшу частину інформаційний систем, з яким може мати справу сучасний комп’ютерний інженер. Різниця буде виключно в масштабах та потребах для конкретних систем.

РОЗДІЛ ІІІ
ЗАСТОСУВАННЯ ЗАСОБІВ РЕЗЕРВНОГО ЗБЕРЕЖЕННЯ НА ЗМОДЕЛЬОВАНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Після аналізу теоретичних основ та моделювання інформаційних систем настає етап практичного впровадження рішень резервного збереження. Саме на цьому рівні перевіряється ефективність обраної архітектури та стратегій, а також виявляються можливі «вузькі місця», які могли бути непомітними у теоретичних схемах.

Резервне копіювання – це не просто технічна опція, а невід'ємна складова життєвого циклу інформаційної системи. Його мета – не лише створення копій, а забезпечення безперервності бізнес-процесів навіть у випадках аварій, втрати доступу чи кібератак. Для досягнення цього результату важливо коректно підібрати методи і засоби з урахуванням реальних характеристик системи.

Нижче наведено конкретні практичні рекомендації щодо вибору підходів до резервного копіювання в межах змодельованих ІС:

По-перше, визначається рівень критичності даних. Якщо мова йде про облікові, фінансові або конфіденційні дані, доцільно застосовувати багаторівневу схему: локальне резервування на зашифрованих носіях у поєднанні з хмарним копіюванням, що забезпечує географічну рознесеність та додатковий рівень безпеки. Для менш критичних файлів достатньо використання стандартних програмних рішень, наприклад Windows Backup або Time Machine.

По-друге, важливо обрати оптимальну періодичність копіювання. Якщо система зазнає частих змін – варто впроваджувати інкрементальне резервування, що дозволяє економити ресурси та зменшує навантаження на мережу. Якщо ж інформація оновлюється рідко, підійде повне або диференційне копіювання, яке спрощує відновлення.

Третім фактором є доступність копій. Для мобільних команд або розподілених офісів найбільш ефективним є використання хмарних рішень (Google Drive, OneDrive, AWS S3). У випадках, коли критично важливо

обмежити доступ сторонніх осіб, перевагу слід віддати автономним шифрованим накопичувачам, ізоляції мережевих сегментів і багаторівневій автентифікації.

Захист від кіберзагроз – окремий аспект. Сучасні атаки, зокрема програми-вимагачі, здатні не лише зашифровувати дані, а й знищувати резервні копії. Тому все частіше впроваджуються технології незмінних резервних копій (immutable backups), які фізично унеможливлюють редагування чи видалення копії без проходження визначених процедур авторизації.

Значну роль у виборі рішень відіграє бюджет. Для приватних осіб або малих підприємств достатнім може бути безкоштовне або маловартісне програмне копіювання. У середовищах з обмеженим фінансуванням вигідним варіантом є NAS-сервери з RAID-масивами. Водночас великі компанії повинні впроваджувати складні гібридні рішення – з дублюванням у кількох середовищах, автоматизацією перевірок та цілісності.

Особливу увагу слід приділяти автоматизації процесу резервування. Людський фактор часто стає джерелом помилок: забули зробити копію, не протестували відновлення тощо. Використання сценаріїв (скриптів) та спеціального ПЗ, яке самостійно виконує копіювання за розкладом, перевіряє контрольні суми і сповіщає про помилки, дозволяє уникнути більшості ризиків.

У результаті, під час застосування методів резервного копіювання на змодельовані інформаційні системи важливо не лише враховувати технічні характеристики середовища, а й інтегрувати інструменти резервування у повсякденну операційну діяльність. Ефективна стратегія включає: багаторівневе збереження, шифрування, облік RPO та RTO, автоматичне тестування відновлення та дотримання політик безпеки.

Таким чином, вибір засобів резервного збереження – це не питання лише технологій, а продумане рішення, що враховує як характеристики самої ІС, так і людський, економічний та організаційний контекст. Саме завдяки такому цілісному підходу можна забезпечити стабільність і стійкість інформаційної інфраструктури в реальних умовах.

3.1 Структура виконання роботи стосовнот застосування засобів резервного збереження інформаційних систем

В минулому розділі були створені моделі інформаційних систем. Саме ці моделі будуть застосовуватись для демонстрації засобів резервного збереження інформаційних систем. Проте, при застосуванні цих засобів велике значення має контекст та потреби в резервуванні. Тобто, навіть в структурно однакових інформаційних систем можуть бути різні потреби в резервуванні. Тому спочатку буде вказуватись, яка модель розглядається, і яка задача поставлена стосовно резервування. Після цього буде представлено пояснення з моделлю, що створена для виконання поставленої задачі.

Такий формат представлення виконаного дослідження має забезпечити достатнє уявлення про практичне застосування засобів резервного збереження й забезпечити ясну їх демонстрацію.

3.2 Застосування засобів резервного збереження на інформаційні системи

Задача 1: представлена модель організації накопичувачів на домашньому ПК (див. рис. 2.3.1). Підібрати засіб або сукупність засобів резервного збереження при умові, що цінна інформація зберігається лише на SSD-диску, і ця інформація має бути доступною поза межами цього ПК. ПК підключений до інтернету.

Виконання задачі 1: для поставленої задачі в якості засобу резервування було застосовано синхронізація даних з хмарою (див. рис. 3.2.1), на якій зберігається вся важлива інформація. Хмара синхронізується з даними на ПК і у разі потреби здатна надати дані для їх відновлення. Оскільки до хмари відбувається підключення через інтернет, це дає потенційну змогу підключитись до неї з будь-якої точки світу, де є

підключення до глобальної мережі.

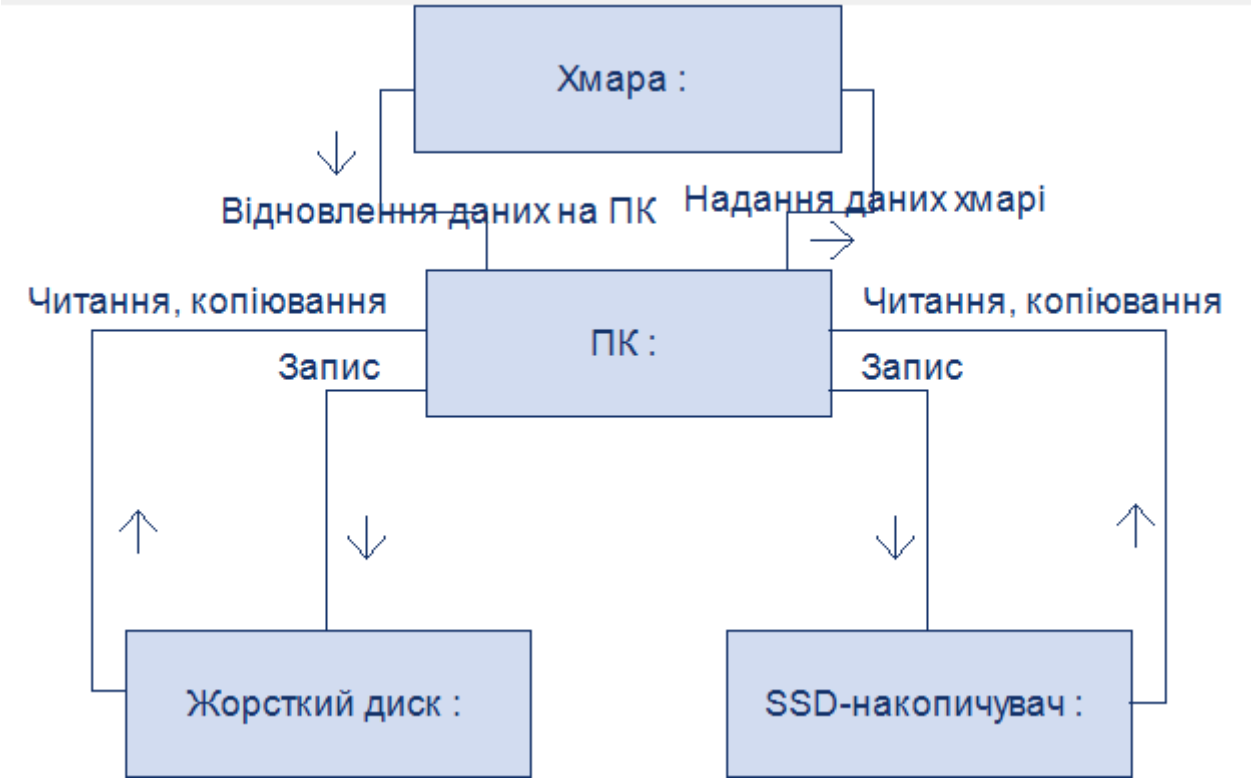

Рисунок 3.2.1 – Модель ПК з використанням хмари як засіб резервного збереження системи.

Задача 2: Представлена локальна мережа охоронної організації (див рис. 2.3.2). Вона потребує резервного збереження інформації на сервері та підвищення безвідмовності його роботи. З міркувань безпеки сервер не має підключення до глобальної мережі.

Виконання задачі 2: для поставленої задачі був застосований апаратний спосіб резервування – інформація з основного серверу дублюється на резервний (див. рис. 3.2.2), що дозволяє підвищити безвідмовність системи. Виходячи з опису завдання, цей засіб має бути оптимальним в зв’язку з високою необхідністю в підвищенні надійності систем та забезпечення безвідмовності в кризових ситуаціях. Хмарні засоби не підійдуть в зв’язку з відсутністю підключення до інтернету, а програмні засоби, у разі виникнення проблем, будуть потребувати більшого часу відновлення здатності роботи системи, чим пряме підключення до резервного серверу.

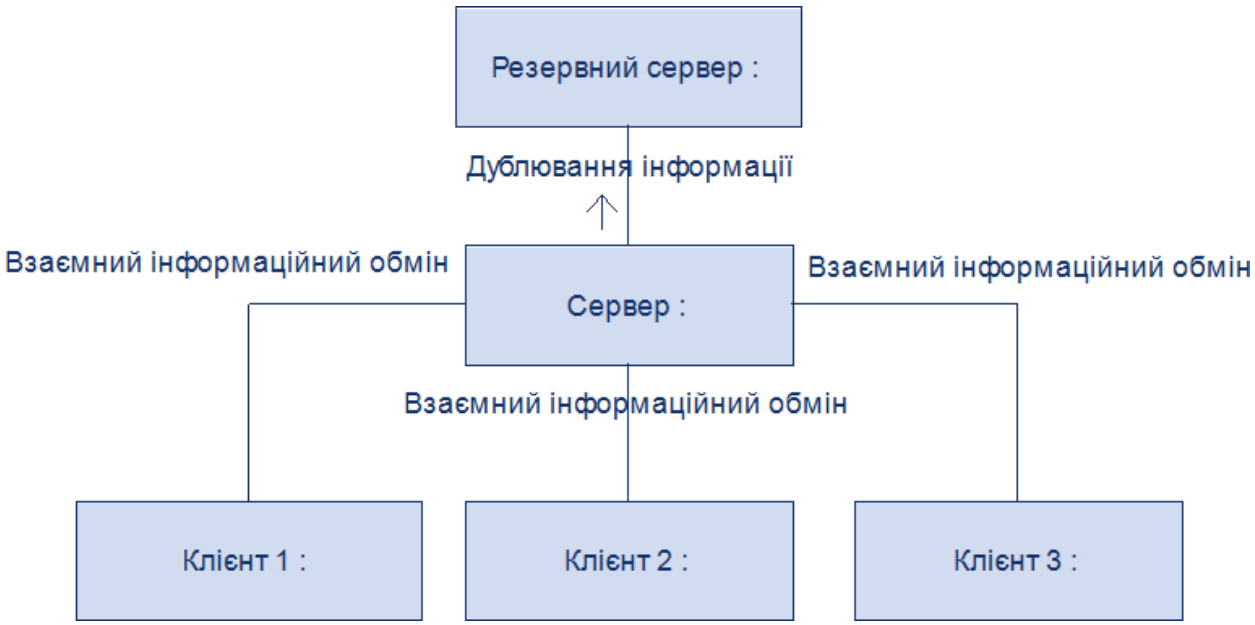

Рисунок 3.2.2 – Модель мережі з використанням апаратного засобу резервування.

Задача 3: представлена організація збереження даних на побутовому ПК (див. рис. 2.3.1). Необхідно виконати резервування ПК самим бюджетним засобом.

Виконання задачі 3: оскільки апаратні та хмарні сервіси потребують додаткових, іноді регулярних, витрат, в такому випадку доведеться обмежитись програмним резервуванням в межах цього ПК. Саме просте – застосування Windows Backup для операційної системи Windows, утиліти tar і dd для систем на базі ядра Linux, Time Machine якщо застосовується MacOS. Більш бюджетних рішень не знайти. Апаратні та хмарні рішення потребують все-таки більше фінансових вкладів, ніж програмні. (див. рис. 3.2.3)

Рисунок 3.2.3 – Модель ПК з використанням програмних засобів резервування.

Задача 4: представлена локальна мережі організації (див рис. 2.3.2). Для неї ввести засоби резервного збереження для серверу, який має високий пріоритет збереження даних, та локальний для кожного клієнта мережі, при умові, що організація готова вкластись лише в резервування серверу, а для клієнтів просить встановити самий доступний варіант по вартості. Дані, що зберігаються, мають цінність лише для самої організації, та мають бути доступними в усіх можливих кризових ситуаціях.

Виконання задачі 4: по-перше варто визначити які засоби будуть застосовуватись для серверу та для клієнтів. Оскільки для клієнтів необхідно обрати самий бюджетний варіант, тому застосовуватись будуть лише програмні засоби резервного збереження. А саме на сервері зберігаються важливі дані організації, тому її надійність є критичною. В задачі не вказані критичні ситуації, тому будемо відходити від наступних: відсутність енергопостачання, вихід з ладу апаратної складової сервера, помилки програмного забезпечення,

відсутність підключення до інтернету. Несанкціоноване проникнення розглядатись не буде, адже в задачі вказано, що дані несуть цінність лише для самої організації. Можна було б додати стихійні лиха, але це може стати лише причиною виходу з ладу апаратної частини, тому окремо подібну ситуація не розглядатимемо. Отже, беручи до уваги обставини, було застосовано наступні засоби резервного збереження інформаційних систем: дублювання інформації на хмару (у разі апаратної поломки всі дані все-одно будуть збережені, і у разі відсутності енергопостачання на мережеву складову організації, доступ до даних можна буде отримати ззовні), додавання резервного серверу та організація RAID-масиву (такий варіант дозволить максимально забезпечити безвідмовність в апаратній частині – якщо вийде з ладу один вузол, його можна буде замінити за рахунок працюючих інших вузлів) (див. рис. 3.2.4).

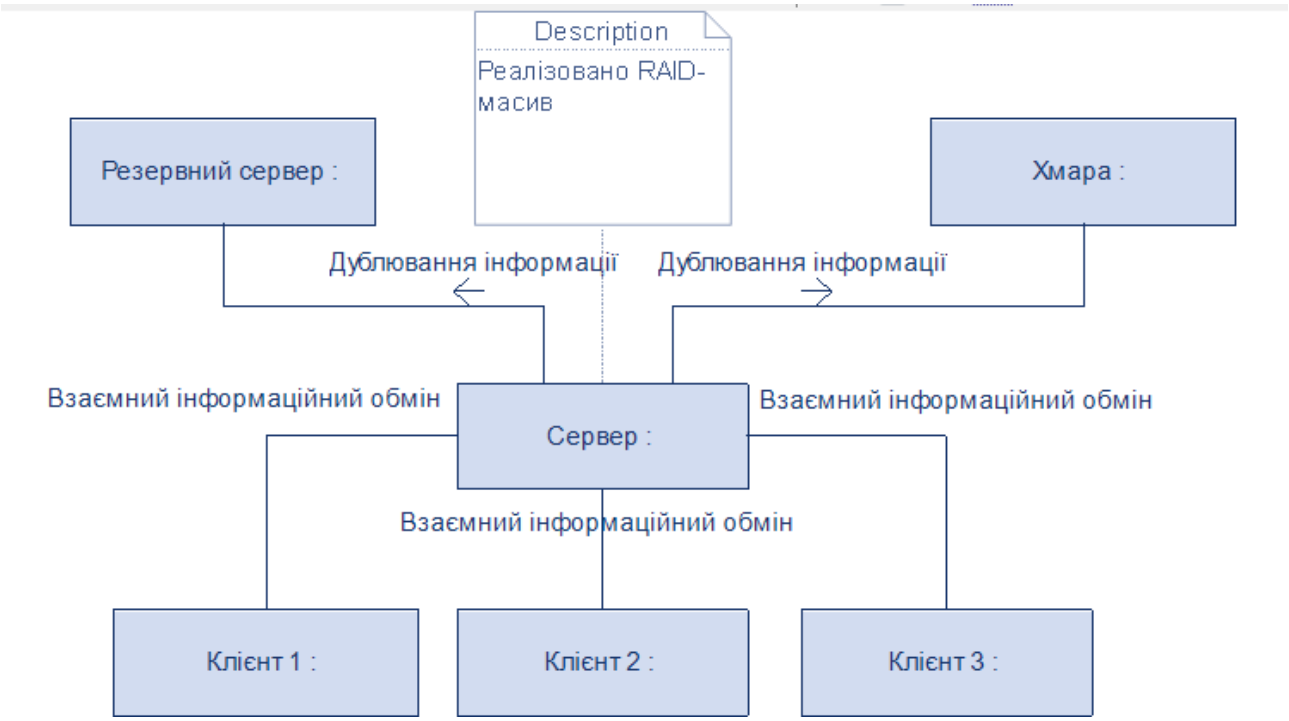

Рисунок 3.2.4 - Модель локального серверу з апаратних, програмних та хмарних засобів резервного збереження інформації.

Задача 5: представлена локальна мережа (див. рис. 2.3.2). Необхідно реалізувати централізоване незалежне середовище для зберігання резервних копій індивідуальним клієнтам мережі, що не буде виходити за межі локальної

мережі.

Виконання задачі 5: Оскільки постановка задачі схиляє до застосування апаратного резервування (адже прямо вказано «централізоване незалежне середовище»), було прийнято рішення щодо встановлення окремого серверу, який буде зберігати резервні копії клієнтів мережі. Він підключається паралельно основному серверу і не залежить від посторонніх факторів мережі (див рис. 3.2.5).

Рисунок 3.2.5 – Модель локальної мережі з незалежним сервером резервного збереження.

3.3 Оцінка актуальності сучасних практичних можливостей щодо резервного збереження інформаційних систем

Оцінка актуальності проводиться за єдиним критерієм: чи достатньо на сьогодні засобів для забезпечення сучасних потреб в резервуванні. Це охоплює: локальне програмне резервування (вбудоване у Windows, macOS, Linux); хмарні сервіси (Google Drive, Dropbox, OneDrive, iCloud); спеціалізоване ПЗ для

резервного копіювання (Acronis, Veeam, Cobian, Bacula, Duplicati); апаратні рішення (NAS-сервери, резервні дата-центри, SAN-системи).

Відповідно до сучасних вимог, засоби резервного копіювання повинні підтримувати такі функціональні характеристики:

– автоматизацію процесу копіювання та перевірку цілісності копій;

– можливість налаштування розкладу резервування та обсягу збережуваних даних;

– гнучке керування політиками збереження (наприклад, політики "Grandfather-Father-Son", ротація, інкрементальні копії);

– підтримку шифрування та аутентифікації доступу до резервів.

Таблиця 3.3.1 - Основні засоби та сховища резервного збереження

Засіб/Сховище	Опис та особливості	Переваги	Недоліки
Знімні носії	Зовнішні HDD, SSD, USB-флешки, оптичні диски	Простота, портативність, незалежність від мережі	Фізична вразливість, обмежена ємність
Стрічкові бібліотеки	Магнітні стрічки для зберігання великих обсягів даних	Дешева вартість зберігання, можливість offline зберігання	Повільний доступ, складність організації
Дискові сховища	RAID-масиви, NAS, SAN	Висока швидкість доступу, масштабованість, централізоване керування	Вища вартість, потреба в обслуговуванні
Центри обробки даних	Серверні приміщення з професійним захистом і адмініструванням	Високий рівень безпеки, масштабування, професійне управління	Залежність від зовнішніх постачальників
Хмарні сховища	Зберігання даних у хмарі (Google Drive, AWS, Azure, Dropbox тощо)	Доступність із будь-якої точки, масштабування, автоматичне резервування	Залежність від інтернету, можливі ризики безпеки

–

Таблиця 3.3.1 відображає порівняння різних засобів резервного збереження інформації

Варто зазначити, що більшість сучасних операційних систем (Windows

10/11, macOS, Linux-дистрибутиви) мають вбудовані або легко інтегровані засоби резервування, які часто активуються за замовчуванням або доступні в кілька кліків. Ці інструменти забезпечують зручну автоматизацію, не потребуючи від користувача глибоких технічних знань. Це робить резервування доступним практично для кожного користувача, навіть якщо він сам цього не усвідомлює.

Таким чином, на сучасному етапі розвитку інформаційних технологій можна стверджувати, що практичні засоби резервного збереження інформаційних систем є не лише актуальним, а цілком достатнім для більшої частини існуючих інформаційних систем.

Проте, варто звернути увагу на необхідність в грамотному налаштуванні всіх політик: людський фактор, неправильно налаштовані політики резервування та політики безпеки, недбалість кінцевого користувача – все це фактори, які можуть забезпечити виключно неправильну роботу резервних засобів, які зведуть нанівець всю суть резервного копіювання.

3.4 Перспективи розвитку засобів резервного збереження в умовах зростання кіберзагроз

У сучасних умовах зростаючих кіберзагроз пріоритетним напрямом розвитку інформаційних систем стає підвищення рівня їх захищеності. Особливого значення набуває забезпечення безпеки не лише основних обчислювальних систем, а й засобів резервного збереження, які дедалі частіше стають об’єктами атак. Уразливі резервні копії можуть бути використані зловмисниками для відновлення доступу до критичних даних або поширення шкідливого програмного забезпечення [16]. Тому резервні засоби збереження повинні відповідати таким самим, а в окремих випадках – і підвищеним, стандартам безпеки, як і основна IT-інфраструктура. Йдеться передусім про застосування сучасних методів шифрування, автентифікації, контролю доступу, ізоляції та моніторингу.

Одним із ключових підходів, що активно розвивається в цьому контексті, є модель нульової довіри (Zero Trust Model), яка передбачає відсутність апріорної довіри до будь-якого користувача чи компонента системи – незалежно від його статусу, рівня авторизації чи розташування в мережі. Кожен запит до інформаційних ресурсів, зокрема до резервних копій, має проходити багаторівневу перевірку, що включає автентифікацію, авторизацію та контроль доступу на основі політик безпеки. Запровадження цієї концепції на державному рівні було офіційно закріплене виконавчим указом Президента США Дж. Байдена у 2021 році, що започаткував перехід федеральних інформаційних систем до архітектури з нульовою довірою [7]. Її застосування в середовищі резервного збереження даних дає змогу знизити ризики внутрішніх загроз, несанкціонованого доступу та шкідливих впливів.

Подальший розвиток систем резервного копіювання пов’язаний із впровадженням функцій незмінності резервних копій (immutability), що унеможливлює їх зміну або видалення навіть у разі компрометації адміністративного доступу. Така властивість забезпечується застосуванням спеціалізованих файлових систем, обмежень на рівні апаратного забезпечення або політик збереження даних у хмарних середовищах [16]. Одночасно з цим широко використовується наскрізне шифрування (end-to-end encryption), що захищає дані як під час передавання, так і в стані зберігання. Додатково підвищується рівень безпеки за рахунок багатофакторної автентифікації (MFA), яка унеможливлює доступ до резервних копій при втраті облікових даних [7].

Важливим напрямом модернізації є впровадження принципів логічної сегментації та фізичної ізоляції сховищ. Поділ сховищ на ізольовані сегменти унеможливлює масове поширення атак, зокрема шкідливого ПЗ або програм-вимагачів, а зберігання копій на носіях, що фізично від’єднані від основної мережі, знижує ризик зовнішнього втручання .

З метою забезпечення оперативного реагування на потенційні загрози, резервні рішення активно інтегруються з системами виявлення та запобігання вторгненням (IDS/IPS), а також з платформами обробки інцидентів безпеки

(SIEM). Завдяки цьому стає можливим своєчасне виявлення аномальної активності та автоматизоване реагування на інциденти. Крім того, впровадження регулярного тестування процедур відновлення даних забезпечує постійну перевірку готовності до надзвичайних ситуацій.

Ще одним важливим фактором безпеки є географічна надлишковість – розміщення резервних копій у різних фізичних або віртуальних локаціях, що підвищує відмовостійкість та дає змогу дотримуватись міжнародних нормативних вимог, зокрема щодо територіального розміщення персональних даних (GDPR, HIPAA та ін.).

На завершальному етапі розвитку перебуває використання технологій штучного інтелекту та машинного навчання для оптимізації процесів резервного збереження. Ці технології дозволяють автоматизувати моніторинг резервних копій, виявляти аномалії в роботі системи, прогнозувати потенційні загрози, а також адаптувати частоту й обсяг копіювання до змін у структурі даних. Інтеграція таких рішень підвищує ефективність, надійність і гнучкість сучасних систем резервного збереження.

Таким чином, у відповідь на стрімке зростання рівня кіберзагроз, розвиток засобів резервного збереження інформаційних систем зосереджується не лише на збереженні даних, а й на створенні комплексного, стійкого та інтелектуального захисного середовища, що інтегрує новітні технології шифрування, контролю доступу, автоматизації та аналітики.

ВИСНОВКИ

Важливо розуміти, що питання резервного збереження – це не лише технічна чи організаційна задача. Це стратегічне рішення, яке визначає майбутню стійкість бізнесу, безперервність процесів і здатність компанії чи установи оперативно реагувати на загрози. У світі, де дані стали новою валютою, а час – найціннішим ресурсом, від правильного вибору засобів резервного копіювання може залежати не лише стабільність, а й саме виживання інформаційної системи.

За результатом роботи була проведена оцінка сучасних засобів резервного збереження інформаційних систем, із подальшим формуванням чітких практичних рекомендацій щодо їх застосування в різних умовах. Основною метою дослідження стало не просто ознайомлення з існуючими технологіями резервного копіювання, а побудова цілісного підходу до забезпечення надійності інформаційних систем шляхом впровадження адаптивних та ефективних стратегій резервного збереження.

Першим кроком стало детальне вивчення загальних принципів побудови інформаційних систем, аналіз типових архітектур – від монолітних і клієнт-серверних до сучасних мікросервісних та хмарних рішень. Це дозволило краще зрозуміти логіку функціонування таких систем, виявити залежності між їхніми компонентами та визначити потенційні «вразливі точки», які особливо потребують резервного збереження. Було також проведено порівняння різних класів інформаційних систем (бази даних, файлові сервери, поштові та веб-сервери, віртуалізовані середовища, спеціалізовані бізнес-рішення типу ERP/CRM/HRM), що дозволило врахувати специфіку кожного з них при виборі методів резервного копіювання.

Наступним етапом стало моделювання таких інформаційних систем – створення логічних схем і умовних ситуацій, які максимально наближені до реальних умов експлуатації. На основі змодельованих ІС були підібрані відповідні методи резервного збереження, що враховували критичність даних,

частоту змін, вимоги до часу відновлення (RTO) та допустимого обсягу втрати (RPO). У результаті цього аналізу сформувались рекомендації, зокрема щодо використання повного, диференційного, інкрементального копіювання, знімків (snapshots), технологій CDP (безперервного захисту даних), а також щодо вибору типів сховищ – від локальних жорстких дисків до хмарних об’єктних сховищ (S3, Azure Blob).

Окрему увагу в дослідженні приділено сучасним технологіям, які доповнюють або суттєво змінюють підхід до резервного копіювання. Це, зокрема, блокчейн-рішення для незмінного збереження копій, інструменти постквантового шифрування, концепція Zero Trust для мінімізації ризиків несанкціонованого доступу, а також застосування штучного інтелекту для автоматичного моніторингу, адаптації частоти резервування і виявлення потенційних загроз. Ці інновації роблять системи резервного копіювання не просто пасивним способом збереження, а активною частиною кіберзахисту.

За підсумками практичної частини була сформована база моделей типових ситуацій, у яких резервне збереження відіграє критичну роль. Ця база може використовуватись як методичний матеріал у навчальному процесі, у розробці інструкцій для IT-відділів, а також як основа для побудови реальних систем резервного копіювання на підприємствах. Показано, що залежно від масштабу та цілей, резервне збереження можна організовувати як у простих домашніх умовах (за допомогою базового програмного забезпечення типу Windows Backup, Time Machine), так і в масштабах складних корпоративних мереж, де потрібна інтеграція з хмарними платформами, віртуалізація, шифрування, багаторівнева аутентифікація та централізоване управління.

Результати дослідження мають високу універсальність. Вони можуть бути адаптовані під широкий спектр сценаріїв: від особистого користування (резервування фото, документів, налаштувань системи) до стратегічних систем підприємств і державних установ (фінансові транзакції, база клієнтів, медичні записи тощо). Усі методи та рішення були підібрані з урахуванням можливості масштабування, бюджетних обмежень та нормативних вимог, що робить цю

роботу не просто академічною, а реально прикладною.

У підсумку можна стверджувати, що резервне збереження – це більше не технічна опція, а обов’язковий елемент кібергігієни. Його грамотне впровадження – це питання не лише збереження інформації, а й загальної безпеки бізнесу, приватної особи або державного органу. Системи резервного копіювання повинні проєктуватись як живі й адаптивні рішення, які постійно враховують зміни в інфраструктурі, обсягах даних і рівні загроз. Саме такий підхід був реалізований у межах цього дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методи моделювання інформаційних систем. Конспект лекцій. DSpace :: ELAKPI :: Репозитарій КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/handle/123456789/54107 (дата звернення: 17.11.2025).

2. Для чого потрібне резервне копіювання даних - Важливість та способи | Skeleton.ua. Skeleton. URL: https://skeleton.ua/uk/articles/dlya-chogo-potribne-rezervne-kopiyuvannya-danih/ (дата звернення: 20.10.2024).

3. Virtual Tape Libraries. Documentation. URL: https://documentation.commvault.com/11.20/virtual_tape_libraries.html (дата звернення: 5.12.2024).

4. Резервне копіювання даних: визначення та види - Netwave. Netwave. URL: https://netwave.ua/blog/rezervne-kopiyuvannya-danyh-vyznachennya-ta-vydy/ (дата звернення: 15.10.2024).

5. Система резервного копіювання та відновлення – запорука збереження даних - TechExpert. TechExpert. URL: https://techexpert.ua/backup-and-recovery-system-is-the-key-to-data-security/ (дата звернення: 10.11.2024).

6. Що таке система зберігання даних та як її використовувати. Secur.ua - товари для розумного дому, енергоживлення і безпеки. URL: https://secur.ua/news/shho-take-sistema-zberigannia-danix-ta-iak-yiyi-vikoristovuvati (дата звернення: 13.01.2025).

7. microsoft.com. URL: https://www.microsoft.com/uk-ua/security/business/zero-trust (дата звернення: 03.03.2025).

8. Ace. Способи резервного копіювання комп'ютерних файлів - Filemail. Filemail. URL: https://www.filemail.com/uk/blog/резервне-копіювання-файлів/способи-резервного-копіювання-комп-ютерних-файлів (дата звернення: 18.03.2025).

9. URL: https://www.sim-networks.com/ukr/blog/backup-full-increment-differential (дата звернення: 03.05.2025).

10. Резервне копіювання: види та методи бекапів | Netwave. Netwave. URL: https://netwave.ua/blog/metody-i-vidy-rezervnogo-kopirovaniya/ (дата

звернення: 11.11.2024).

11. Резервне копіювання. Повний довідник. Мегатрейд. URL: https://megatrade.ua/news/reviews/rezervne-kopiyuvannya-povniy-dovidnik/ (дата звернення: 03.04.2025).

12. Створення резервних копій для бізнесу: що необхідно знати | Kyivstar Business Hub. Kyivstar Business Hub – корпоративний блог для бізнесу. URL: https://hub.kyivstar.ua/articles/stvorennya-rezervnyh-kopij-dlya-biznesu-shho- neobhidno-znaty (дата звернення: 01.04.2025).

13. Юдкова К., Чернишина Г. Класифікація інформаційних систем. Інформація і право. 2015. С. 92-98.

14. Oteir N. Основні технології резервного копіювання даних. INTROSERV. URL: https://introserv.com/ua/blog/osnovni-texnologii-rezervnogo-kopiyuvannya-danix/ (дата звернення: 26.05.2025).

15. What is AWS Backup? - AWS Backup. URL: https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html (дата звернення: 20.05.2025).

16. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.

17. PCI DSS. Головна | GetPCI. URL: https://getpci.com/vidi-sertifikativ/pci-dss (дата звернення: 26.04.2025)