Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Бобошко Марини Анатоліївни*

академічної групи *125м-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Дослідження ефективності методів резервування даних приватного підприємства*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Начовний І.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту ***Бобошко Марині Анатоліївні*** **академічної групи** ***125м-19-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Дослідження ефективності методів резервування даних приватного підприємства***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Навести актуальність технології RAID, технології з'єднання систем зберігання даних з обчислювальними системами DAS, SAN, NAS, розглянути переваги та недоліки алгоритмів резервного копіювання даних.	10.10.2020
Розділ 2	Визначити інформаційні потоки на типовому підприємстві, виконати аналіз загроз, визначити профіль захищеності та методи його реалізації, обґрунтувати методи підвищення захищеності засобів резервування даних на комерційному підприємстві	20.11.2020
Розділ 3	Обґрунтування економічної доцільності застосування методів підвищення захищеності засобів резервування даних на приватному підприємстві	05.12.2020

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 01.09.2020р.

Дата подання до екзаменаційної комісії: 11.12.2020р.

Прийнято до виконання _____ Бобошко М.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., __ додатки, __ джерел.

Об’єкт досліджень: засоби резервування даних на комерційному підприємстві.

Метою дипломної роботи є: підвищення рівня захищеності засобів резервування даних на комерційному підприємстві.

Предмет досліджень: методи підвищення захищеності засобів резервування даних на комерційному підприємстві.

В першому розділі роботи магістра було розглянуто: актуальність технології RAID, технології з'єднання систем зберігання даних з обчислювальними системами DAS, SAN, NAS, розглянуті переваги та недоліки алгоритмів резервного копіювання даних.

В другому розділі роботи магістра визначена інформація яка циркулює на типовому підприємстві, виконано аналіз загроз, визначений профіль захищеності та методи його реалізації, обґрунтовані методи підвищення захищеності засобів резервування даних на комерційному підприємстві.

РЕЗЕРВНЕ КОПІЮВАННЯ, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, RAID, РІВЕНЬ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ, DAS, SAN, NAS.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., __ приложений, __ источников.

Объект исследований: средства резервирования данных на коммерческом предприятии.

Целью работы является повышение уровня защищенности средств резервирования данных на коммерческом предприятии.

Предмет исследований: методы повышения защищенности средств резервирования данных на коммерческом предприятии.

В первой разделе работы магистра были рассмотрены: актуальность технологии RAID, технологии соединения систем хранения данных с вычислительными системами DAS, SAN, NAS, рассмотрены преимущества и недостатки алгоритмов резервного копирования данных.

Во втором разделе работы магистра определена информация которая циркулирует на типовом предприятии, выполнен анализ угроз, определенный профиль защищенности и методы его реализации, обоснованные методы повышения защищенности средств резервирования данных на коммерческом предприятии.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ, ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СИСТЕМЫ, RAID, УРОВЕНЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ, DAS, SAN, NAS.

ABSTRACT

Explanatory note: ___ p., __ fig., __ tab., __ application, __ sources.

Object of research: means of data backup in a commercial enterprise.

The aim of the work is to increase the level of protection of data backup facilities in a commercial enterprise.

Subject of research: methods to improve the security of data backup at a commercial enterprise.

The first chapter of the master's thesis work considered: the relevance of RAID technology, the technology of connecting data storage systems with DAS, SAN, NAS computing systems, and the advantages and disadvantages of data backup algorithms.

In the second section of the master's thesis, information that circulates in a typical enterprise is defined, threats are analyzed, a certain security profile and methods for its implementation, and sound methods for improving the security of data backup facilities in a commercial enterprise.

BACKUP COPYING OF INFORMATION WITH LIMITED ACCESS, INFORMATION AND COMMUNICATION SYSTEM, RAID, LEVEL OF PROTECTION OF INFORMATION, DAS, SAN, NAS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

API	–	Application Programming Interface;
DAS	–	Direct Attached Storage;
RAID	–	Redundant Array of Independent / Inexpensive Disks;
RPO	–	Recovery Point Objective;
RTA	–	Recovery Time Actual;
RTO	–	Recovery Time Objective;
HVD	–	Holographic Versatile Disc;
MAID	–	Massive Array of Inactive Disks;
NAS	–	Network Attached Storage;
SAN	–	Storage Area Network;
АС	–	автоматизована система;
КЗЗ	–	комплекс засобів захисту;
КС	–	комп’ютерна система;
КСЗІ	–	комплексна система захисту інформації;
НД	–	нормативний документ;
ОС	–	операційна система;
ПЗ	–	програмне забезпечення;
ПЗП	–	постійний запам’ятовуючий пристрій.

ЗМІСТ

с.

ВСТУП

Інформації, що зберігається в комп'ютерних системах, загрожує безліч небезпек. Дані можуть бути загублені через помилки програмного забезпечення, невмілої роботи користувачів, збоїв фізичних носіїв і засобів зв'язку, зловмисного псування даних. Абсолютного захисту від усіх цих загроз не існує, ризик втрати даних існує завжди.

Як показує загальносвітова статистика, основними причинами втрат даних є несправна робота апаратних засобів (44%) і людські помилки (32%), в основному тих, хто має максимальний рівень доступу до систем зберігання даних компанії. 14% всіх випадків втрат даних відбуваються внаслідок помилок програмного забезпечення, інші 7% відбуваються через комп'ютерні віруси, а внаслідок стихійних лих – лише 3%.

Збої призводять до призупинення бізнес-процесів і втрати даних, тим самим ставлять під питання існування бізнесу в цілому. Мабуть, єдиний спосіб надійно зберегти потрібну інформацію – періодично створювати резервні копії.

Впроваджуючи системи зберігання даних і резервного копіювання, компанія стикається зі складними завданнями оцінки її поточних потреб, плануванні майбутніх обсягів даних, вибору технологій та архітектур, які повинні максимально відповідати вимогам безпеки, можливості подальшого масштабування, задовольняти технічним вимогам швидкості запису, читання, відновлення даних і багатьом іншим умовам. Виявити оптимальне рішення дуже непросто, особливо з огляду на широке різноманіття існуючих шляхів реалізації систем зберігання і резервного копіювання, а також досить високу динаміку зміни цін і появи нових технологій на IT ринку.

У клієнтів різні пріоритети, проте, існує загальна для всіх проблема – стрімке зростання обсягів збережених даних, що становить 50-100% на рік. Так за результатами дослідження компанії IDC – сукупний обсяг інформації, зберігається в електронному вигляді, в 2019 році склав понад 791 екзабайт.

Відповідно, все серйозніше стає проблема надійного зберігання даних і швидкості доступу до них.

Дійсно, побудова високоефективної системи зберігання даних, відповідають реальним вимогам організації, а також вибір найбільш підходящої системи резервного копіювання – процес досить складний і трудомісткий.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність проблеми

Актуальність резервування даних зростає з кожним роком, так само як зростає і цінність інормації. Часто втрата інформації може видатися дуже неприємною (наприклад при втраті музичного архіву улюбленого виконавця), а іноді й небезпечною (втрата бухгалтерської звітності). Встановлено, що більшість підприємств, які пережили велику незворотну втрату корпоративних даних, припиняють своє існування протягом трьох років після такого інциденту.

Але все ще багато компаній нехтують резервним копіюванням даних або виконують його на недостатньо якісному рівні. Виявлення недоліків системи ти усунення їх значно зменшить ризик втрати важливої інформації.

1.2 Сутність систем резервного копіювання

Розглянемо визначення поняття резервного копіювання за версією.

Резервна копія – дані, що зберігаються на енергонезалежних носіях, звичайно віддалено, призначені для відновлення, у разі якщо оригінал копії даних загублений або недоступний.

Резервне копіювання (англ. backup) – процес створення резервних копій.

1.2.1 Системи резервного копіювання даних за методом копіювання

Резервне копіювання (англ. backup) - процес створення резервних копій. Всі системи резервного копіювання даних можна розділити на три типи згідно використовуваному методом копіювання:

- блочне копіювання;
- пофайлове копіювання;
- копіювання даних на рівні додатків.

1.2.1.1 Система блочного резервного копіювання

Система блочного резервного копіювання працює безпосередньо з носієм, ігноруючи файлову структуру, і зберігаючи усі матеріали повністю – операційну систему, робочі дані, настройки та інше.

Перевагою виконання даного виду резервного копіювання є висока швидкість. Проте зазвичай при виконанні операцій копіювання потрібно призупинити роботу додатків, щоб копія була цілісною. Деякі системи виявляють невикористовувані блоки і виключають їх копіювання. При використанні блочного резервного копіювання, досить складним є відновлення приватних файлів.

1.2.1.2 Система резервного пофайлового копіювання

При виконанні операцій резервного копіювання на файловому рівні використовується файлова система. В цьому випадку відносно простий завданням є відновлення деяких конкретних файлів. В цілому ж операції резервного копіювання тривають довше, виникає додаткова загрузка операційної системи, а також з'являється проблема доступу до відкритих файлів.

1.2.1.3 Резервне копіювання даних на рівні додатків

Резервне копіювання може здійснюватися на рівні додатків. Операції копіювання і відновлення виробляються за допомогою використання спеціально передбаченого в резервованому додатку програмного інтерфейсу API.

Резервна копія являє собою набір файлів і можливо інших об'єктів, визначаються самим додатком, які разом є відображенням стану додатки на деякий момент часу. При даному способі резервного копіювання може мати місце проблема сумісності між різними версіями додатків і систем резервного копіювання, що реалізують відповідний інтерфейс.

1.2.2 Системи резервного копіювання даних за методом реалізації

Сучасні системи резервного копіювання реалізуються як програмно, так і апаратно, а також в поєднанні програмних і апаратних компонентів.

1.2.2.1 Резервне копіювання даних з використанням програмних засобів

Використання програмних засобів відносно дешеве і універсальне. Вони виконують свої завдання незалежно від того, де і як розташоване приміщення для серверів, або від того, як здійснюється доступ до корпоративних додатків з робочих станцій співробітників. Програмні рішення слабо залежать від прийнятої архітектури зберігання і захисту даних.

1.2.2.2 Резервне копіювання даних з використанням апаратних засобів

Виділені апаратні потужності для резервного копіювання дозволяють не завантажувати основні сервера компанії. Чисто апаратні методи резервного копіювання, а також інші апаратні способи запобігання збоїв, такі, як кластеризація серверів або використання RAID-масивів з гарячою заміною дисків, досить дорогі, і пред'являють особливі вимоги до використовуваного апаратного і програмного забезпечення. Подібні системи також досить вимогливі до кваліфікації обслуговуючого персоналу. Апаратні системи резервного копіювання зазвичай складають частину масштабних систем зберігання даних, розгортання великими компаніями.

1.2.2.3 Резервне копіювання даних з використанням програмно-апаратних засобів

Програмно-апаратна система резервного копіювання складається з апаратних і програмних компонентів. Вся логіка резервного копіювання, як правило, зосереджена в програмних компонентах і реалізується ними.

Вони управляють пристроями, процесом резервного копіювання і відновлення даних, підтримують розклад робіт і реалізують додаткові сервісні функції. Апаратні компоненти призначені для виконання операцій запису, зберігання резервних копій і відновлення даних.

1.2.3 Архівування. Відмінність від резервного копіювання

Більшість домашніх користувачів і малих компаній не розрізняють резервне копіювання та архівування, для них резервні копії і є архівом.

Розглянемо визначення поняття архівування за версією SNIA.

Архів – дані, що зберігаються протягом тривалого кількості часу, з метою ведення контролю, аналізу, довідкових цілей.

Архівування – процес створення архівів; копіювання або переміщення даних з метою зберігання.

Архівування відрізняється від резервного копіювання, перш за все тим, що направлено на тривале зберігання інформації і не передбачає вимог до швидкого доступу при необхідності.

Якщо до даних архіву доступ може бути отриманий відносно швидко, то архів називають «активним», а у випадку, коли доступ вимагає значної кількості часу – «не активним» або «холодним».

Найчастіше «активні» архіви використовуються спільно з «не активними», утворюючи ієрархічні структури. Наприклад, для частого використання можуть використовуватися масиви дискових накопичувачів, при цьому менш необхідні дані зберігаються на магнітних стрічках.

Для «не активних» архівів практично завжди використовуються накопичувачі на магнітних стрічках, насамперед через дуже тривалого терміну служби.

В дискових архівах зазвичай використовуються жорсткі SATA диски, як правило, їх об'єднують разом так, щоб більша частина перебувала у відключеному стані, і активізувалася при необхідності. Такі масиви жорстких дисків називають RAID.

Фактори, що враховуються при виборі носіїв, включають не тільки ціну на обсяг збережених даних, але і, звичайно ж, очікуваний термін придатності носіїв. Ставлячи задачу зберігання даних протягом ста років, і припускаючи термін корисної служби використовуваних носіїв рівний 8-10 років, потрібно

очікувати, що буде необхідно провести заміну устаткування як мінімум 10 разів.

1.2.4 Пріоритети, що враховуються при виборі систем резервного копіювання

При виборі систем резервного копіювання виставляється ряд вимог до характеристикам процесів резервування і зберігання, які описуються в контракті з постачальником і називаються, як правило, SLA (англ. Service Level Agreement) – угодою про рівень послуг. При постановці й аналізі загальних технічних вимог зазвичай оперують такими поняттями як RPO, RTO, Backup Window, RTA, Data security.

Backup Window (вікно резервного копіювання) - кількість часу, необхідне для виконання операцій резервного копіювання на цільовій системі.

RPO – момент часу до якого потрібно відновити дані. RPO визначає наскільки часто потрібно робити операції резервного копіювання і яка кількість резервних копій потрібно зберігати.

RTO – час протягом якого потрібно відновити систему в разі потреби. RTO буде низьким у випадку якщо існує локальна копія всіх необхідних даних.

RTA – дійсний час відновлення. Використовується в поєднанні з поставленим часом RTO. Визначається експериментально, при проведенні тестування.

Data security (безпека даних) – рівень захисту від неавторизованого доступу до інформації, що зберігається. Може матися на увазі як шифрування даних, так і захист від фізичного доступу до систем зберігання і т.п.

1.2.5 Обмежувальні фактори

Впроваджуючи, будь-яку систему резервного копіювання необхідно розуміти, що це позначиться тим чи іншим чином на продуктивності обслуговування системи, наприклад, вибираючи розподілене зберігання резервних копій потрібно припускати зростання трафіку в мережі.

Кожен підхід у побудові системи передбачає певне співвідношення між обсягом збережених даних, швидкістю створення копій, швидкістю відновлення, кількістю спеціально навченого персоналу, вартістю придбання та обслуговування. При цьому збільшення швидкості створення копій на 10% може збільшити витрати в два рази, тому при виборі систем потрібно ретельно вибирати вимоги до характеристик і планувати їх зміну в майбутньому, щоб передбачити можливість масштабування.

Всі технічні характеристики системи, а також вартість впровадження та володіння істотно залежать від застосовуваних технологій зберігання і резервного копіювання.

1.3 Сучасні технології в системах зберігання і резервного копіювання

Резервне копіювання, будучи складовою частиною єдиної системи зберігання даних компанії, цілком залежить від сукупності використовуваних технологій, тому будемо розглядати технології резервного копіювання спільно з технологіями зберігання.

1.3.1 Типи носіїв даних

Вибір носіїв даних безпосередньо впливає на головні характеристики процесів створення копій, зберігання і відновлення.

З плином часу, з'являється маса нових технологій, змінюються технічні характеристики носіїв, ціни за одиницю об'єму, вартість обслуговування, застарівають формати зберігання даних і інтерфейси пристроїв. Це обумовлює одну з проблем при зберіганні даних, адже найчастіше носії замінюються не тому, що закінчився їх термін служби, а тому, що з'являються нові технології з набагато кращими характеристиками або з меншими експлуатаційними витратами [9].

В системах зберігання і резервного копіювання частіше за інших використовуються три типи носіїв даних.

1.3.1.1 Магнітні стрічки

Спочатку магнітні стрічки почали використовуватися в 50-х роках, і практично з цього моменту цей тип носіїв даних є найбільш використовуваним для архівного зберігання даних і резервного копіювання.

Сучасні стрічкові накопичувачі можуть вміщати до терабайта неупакованих даних (наприклад, DLT-S4, LTO-4, SAIT-2 зберігають 800 Гб). Зазвичай бібліотеки магнітних стрічок використовуються 10-15 років до наступної заміни на більш нові.

1.3.1.2 Жорсткі диски

Співвідношення ємності і ціни з кожним роком стає все більш виграшним. В даний час використання масивів жорстких дисків в якості основних накопичувачів при зберіганні даних вже не рідкість. За прогнозами очікується, що найближчим часом буде спостерігатися поступовий перехід від використання жорстких дисків в якості основного носія до використання SSD.

За прогнозом IDC загальносвітовий ринок дискових систем зберігання буде продовжувати бурхливе зростання, загальний обсяг проданих накопичувачів даних буде збільшуватися на 40% щорічно [12, 15].

На сьогоднішній день капітальні вкладення для впровадження систем резервного копіювання з використанням жорстких дисків вище, ніж із застосуванням магнітних стрічок. У той же час, експлуатаційні витрати порівнянні, а в багатьох випадках нижче, при використанні рішень на базі жорстких дисків. Вважається, що термін служби масивів активних жорстких дисків дорівнює 5-7 рокам.

1.3.1.3 Оптичні накопичувачі

Оптичні диски першого, другого і третього покоління, такі як CD і DVD, BR використовуються повсюдно. Такі оптичні накопичувачі мають термін служби до 10 років при дотриманні спеціальних умов зберігання [9]. Широке поширення поступово отримує нове покоління оптичних дисків - Blu-ray Disc і HD DVD, мають багато разів більші ємності. Все ж можна з упевненістю

сказати, що на сьогодні оптичні диски досить погано підходять для створення масивних сховищ на їх основі. Все може змінитися з появою нових технологій. Вже існують прототипи дисків із застосуванням технології голографічного пам'яті (англ. holographic memory). Приміром, оптичні диски HVD (англ. Holographic Versatile Disc), створені HSD Forum можуть теоретично зберігати до 3.9 Тб.

Tapestry Media - оптичні диски, вже вироблені американською компанією InPhase Technologies, мають ємність 300 Гб при теоретично максимальної місткості в 1,6 Тб.

Розробляється технологія, при якій, теоретично, може бути збережено до 50 Тб даних на один оптичний диск PCD (англ. Protein-Coated Disc). Ідея полягає в покритті диска спеціальним, світлочутливим білком.

1.3.2 RAID-масив

Дискові масиви з надмірністю даних, які прийнято називати RAID (Англ.Redundant Array of Independent / Inexpensive Disks - надлишковий массив незалежних / недорогих дисків).

У Каліфорнійському університеті в Берклі RAID 1 було визначено як дзеркальний дисковий масив, RAID 2 як масив, в якому застосовується код Хеммінга. Рівні RAID 3, 4, 5 використовують парність для захисту даних від одиночних несправностей. RAID 0 був представлений індустрією як не відмовостійкий дисковий масив. Ця систематика RAID була фактично прийнята як стандарт [15].

Для стандартизації продуктів RAID в 1992 році був організований промисловий консорціум - RAID Advisory Board.

1.3.2.1 Реалізація RAID

Виділяють три основні варіанти реалізації RAID систем:

- програмну (англ. software-based);
- апаратну-шинно-орієнтовану;
- апаратну-автономну підсистему.

Відрізняються вони фактично тим, де виповнюється код: у центральному процесорі комп'ютера (програмна реалізація) або в спеціалізованому процесорі на RAID контролері (апаратна реалізація).

Головна перевага програмної реалізації - низька вартість. При цьому у неї досить багато недоліків: по-перше, низька продуктивність по-друге, додаткова загрузка центрального процесора, по-третє, збільшення шинного трафіку. Програмно реалізують прості рівні RAID 0 і 1, так як вони не вимагають значних обчислень. Враховуючи дані особливості, RAID системи з програмної реалізацією використовуються в серверах початкового рівня. Рисунки 1.1 зображено схему побудови RAID 0 і 1.

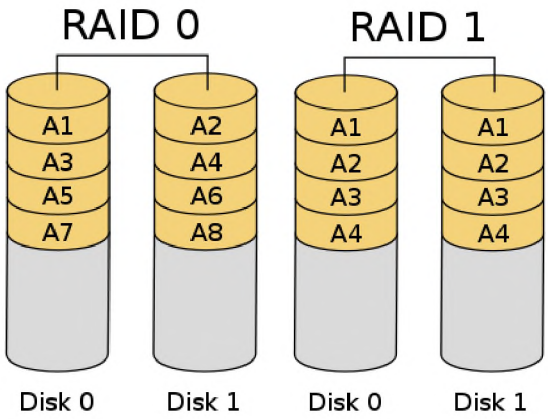

Рисунок 1.1 – RAID 1 та RAID 0

Апаратні реалізації коштують дорожче, ніж програмні, бо використовують додаткову апаратуру для виконання операцій введення-виведення, при цьому вони розвантажують системну шину і ЦП, збільшуючи тим самим швидкодію.

1.3.2.2 Комбіновані рівні

Різноманітність користувацьких сценаріїв породило безліч рівнів RAID, список модифікацій яких продовжує поповнюватися. У літературі пропонується більше десятка рівнів, широке практичне застосування має в кращому випадку

половина з них, а найчастіше використовуються RAID 1, почасти RAID 10 (з розподілом віддзеркалювати даних) і RAID 5.

Структуру RAID 5 представлено на рисунку 1.2.

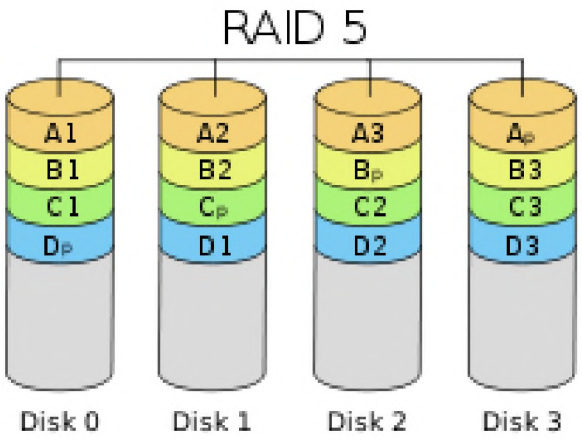

Рисунок 1.2 – RAID 5

В останні роки набули поширення комбіновані рівні RAID. Загальна їхня ідея – збереження максимально високої доступності даних і продуктивності після відмови одного з дисків. На відміну від спочатку створених рівнів, які описують алгоритми обробки одиночних помилок, в комбінованих основна увага приділяється скороченню часу відновлення та зниження ризиків втрати даних від повторних збоїв.

Комбіновані рівні RAID 1+0, RAID 3+0, RAID 5+0, RAID 1+5, різні виробники інтерпретують кожен по-своєму. Суть таких комбінацій коротко полягає в наступному. RAID 1+0 (або RAID 1E) – це комбінація розподілу інформації по дискам від RAID 0 і віддзеркалення – від RAID 1. Нинішні контролери використовують цей режим за замовчуванням для RAID 1. Тобто, 1 диск основний, 2-й диск – дзеркало, причому читання проводиться з них по черзі, як для RAID 0. Власне, зараз можна вважати що RAID 1 і RAID 1+0 – це просто різне назва одного й того ж методу апаратного зеркалирования дисків.

RAID 5+0 – це чергування томів 5-го рівня. RAID 1+5 – віддзеркалення RAID 5.

Комбіновані рівні успадковують як переваги, так і недоліки своїх «Батьків»: поява чергування в рівні RAID 5+0 анітрохи не додає йому надійності, але зате позитивно відбивається на продуктивності.

Рівень RAID 1+5, більш надійний, але не найшвидший і, до того ж, вкрай неекономічний: корисна ємність тому менше половини сумарної ємності дисків.

1.3.2.3 Matrix RAID

Matrix RAID – це технологія, реалізована фірмою Intel в своїх чіпсетах. Строго кажучи, ця технологія не є новим рівнем RAID, вона просто дозволяє, використовуючи лише 2 диски, організувати одночасно один або кілька масивів рівня RAID 1 і один або кілька масивів рівня RAID 0. Це дозволяє за порівняно невеликі кошти забезпечити для одних даних підвищену надійність, а для інших високу швидкість доступу.

Таким чином, власники SATA-контролерів з підтримкою Matrix RAID можуть скористатися перевагами масивів RAID-0 і RAID-1, маючи всього два диски.

1.3.3 Технології з'єднання систем зберігання з обчислювальними системами

DAS, SAN, NAS – основні типи з'єднання систем зберігання з обчислювальними системами.

1.3.3.1 DAS

DAS – пристрій зовнішньої пам'яті, безпосередньо підключений до основного комп'ютера і використовується тільки ним. Найпростіший приклад DAS – вбудований жорсткий диск. Для зв'язку хоста із зовнішньою пам'яттю в типової конфігурації DAS зазвичай використовується SCSI (англ. Small Computer Systems Interface). На рисунку 1.3 зображена архітектура DAS.

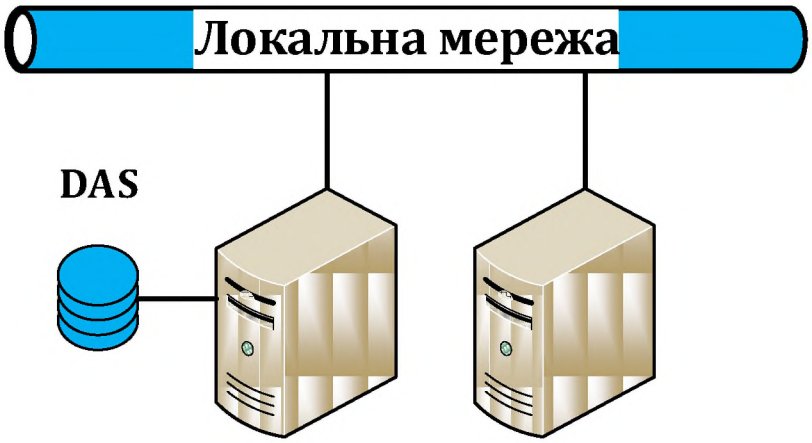

Рисунок 1.3 – Архітектура DAS

Конфігурація DAS прийнятна для застосувань, невимогливих до обсягів, продуктивності і надійності систем зберігання. Багато DAS-пристроїв в масштабі підприємства означають розрізнені сховища, при цьому надлишки пам'яті на одному хост-комп'ютері не можуть використовуватися іншими. Це призводить до неефективної трати ємності зберігання в цілому, а в результаті загальна вартість володіння може виявитися значно вище, ніж для спочатку більш дорогої, більш складної мережевої системи.

1.3.3.2 SAN

Говорячи про системи зберігання корпоративного рівня, мають на увазі, перш все, мережеве зберігання, або іншими словами - мережі зберігання SAN. SAN являє собою виділену мережу пристроїв зберігання, яка дозволяє безлічі серверів використовувати сукупний ресурс зовнішньої пам'яті без навантаження на локальну мережу. На рисунку 1.4 зображена архітектура SAN.

На даний момент фактичним стандартом передачі даних для середовища SAN є технологія Fibre Channel (FC), що забезпечує швидкість 1-2 Гбіт / с. Fibre Channel дозволяє працювати на відстані до 100 км. У мережу зберігання можуть бути підключені дискові масиви RAID, прості масиви дисків JBOD, стрічкові або магнітооптичні бібліотеки для резервування та архівування даних. Основними компонентами для організації мережі SAN є самі пристрої

зберігання, адаптери HBA для підключення серверів до мережі Fibre Channel, мережеві пристрої для підтримки тієї чи іншої топології FC-мережі та спеціалізований програмний інструментарій.

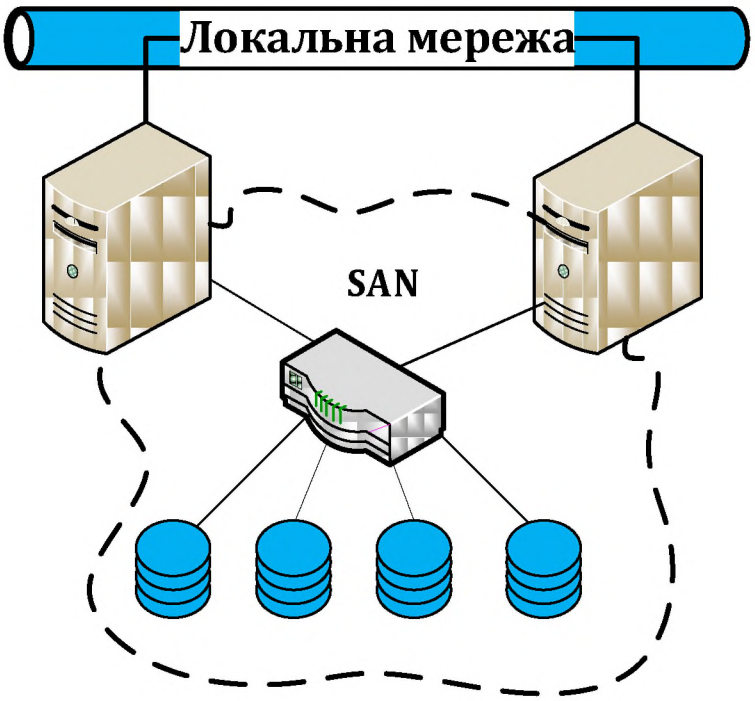

Рисунок 1.4 – Архітектура SAN

Завдання програмного забезпечення для SAN - централізоване управління мережею зберігання, включаючи конфігурування, моніторинг, контроль і аналіз компонентів мережі. Іноді частина функцій ПЗ керування мережею SAN, виноситься на спеціалізований тонкий сервер для управління мережею зберігання.

Виділена мережа зберігання розвантажує основну мережу. Цей фактор, а також високошвидкісне середовище передачі, використовуване в мережі зберігання SAN, забезпечуэ високу продуктивність процесів обміну даними із зовнішніми системами берігання.

Єдиний пул ресурсів, консолідований в SAN, розділяється всіма обчислювальними потужностями, і в результаті необхідна ємність забезпечується меншим числом підсистем.

1.3.3.3 NAS

NAS позначає мережевий пристрій зберігання, точніше виділений файловий сервер, з приєднаної до нього дисковою підсистемою. У конфігурацію NAS може входити і стрічкова бібліотека. NAS-пристрій безпосередньо підключається до мережі і надає хостам доступ до даними на своїй інтегрованій підсистемі зовнішньої пам'яті на рівні файлів (а не блоків даних). На рисунку 1.5 зображена архітектура NAS.

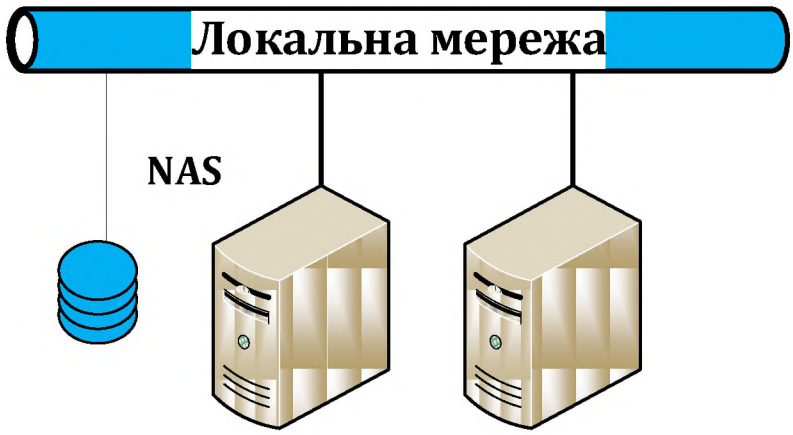

Рисунок 1.5 – Архітектура NAS

На відміну від мереж зберігання, NAS простий в установці та управлінні. При підключенні NAS-пристроїв не потрібно спеціального планування та витрат на додаткове керуюче ПЗ.

Обмін даними з NAS-пристроями йде по локальній мережі загального призначення та їх підключення збільшує трафік. Кілька NAS-пристроїв не можна об'єднати в єдиний ресурс зберігання, а тому збільшення числа NAS-сайтів ускладнює завдання управління.

1.3.3.4 Об'єднання NAS і SAN

NAS і SAN часто співіснують в розподіленої IT-інфраструктурі компанії. Це неминуче породжує проблеми управління та оптимального використання ресурсів зберігання.

Конвергенція NAS і SAN - одна з найважливіших тенденцій останнього часу. Виробники шукають шляхи об'єднання обох технологій в єдину мережеву інфраструктуру зберігання, яка забезпечить консолідацію даних, централізацію резервного копіювання, спростить адміністрування, збільшить масштабованість і захист даних.

Для того щоб додати в мережу зберігання можливість розділення логічної структури файлових систем, необхідний проміжний керуючий сервер для реалізації всіх функцій мережевих протоколів обробки запитів на рівні файлів.

Загальний підхід до об'єднання SAN і NAS - використання NAS-пристрою без інтегрованої дискової підсистеми, але з можливістю підключення компонентів мережі зберігання. Ці пристрої є своєрідним буфером між локальною мережею і SAN, забезпечуючи розділення інформації в мережі зберігання і доступ до даних на рівні файлів. Такі пристрої, у одних виробників називаються NAS-шлюзами, в інших головними NAS-пристроями.

1.3.4 Віртуалізація систем зберігання

Провідні представники ринку систем зберігання не просто об'єднують свої продукти, а формулюють власні стратегії створення консолідованих, мережевих інфраструктур зберігання і захисту корпоративних даних. Ключову роль в цих стратегіях грає ідея віртуалізації, підтримана головним чином на рівні потужних програмних рішень централізованого управління розподіленими сховищами [15].

Віртуалізація систем зберігання зазвичай визначається як комплекс заходів для подання ресурсів різних систем зберігання у вигляді об'єднаного віртуального сховища. Фактично віртуалізація поділяє логічний та фізичний рівні доступу до даних, дозволяючи поєднувати фізичні пристрої зберігання у віртуальні пули. Процеси взаємодії з фізичними носіями і розподілу ємності стають прозорими для серверів і додатків і не вимагають їх участі. При цьому сервер безпосередньо працює не з системою зберігання, а з абстрактною віртуальної системою введення-виведення.

1.3.5 Шифрування резервних копій

Раніше захист сховищ даних с застосуванням шифрування вважався зайвим, бо сховища як такі були-приховані. З появою нових технологій зберігання даних все змінилося, мережі зберігання SAN стали управлятися за допомогою IP-з'єднань.

Магнітні стрічки більше за інших носіїв схильні до небезпеки крадіжок і втрат. Наприклад, відомий випадок з вкраденої магнітною стрічкою з незашифрованими даними, що належить Bank of America, а також випадки з іншими великими компаніями такими, як Time Warner, Ameritrade, DSW Shoe Warehouse [10].

Однак багато компаній як і раніше не шифрують резервні копії на магнітних стрічках. Відповідно з дослідженнями ESG (Enterprise Strategy Group) [14] 60% опитаних компаній ніколи не шифрували створювані резервні копії, причому щодо компаній фінансового сектора цей показник становить 65%, для урядових - 77%, охорони здоров'я - 67%.

Шифруванням нехтують, насамперед, через сильну завантаження ресурсів, а також через досить важке завдання управління ключами доступу [15]. Захист даних непросте завдання, однак не може бути проігнорована. Системи зберігання, зазвичай забезпечені пристроями апаратного стиснення даних. Важливо відзначити, що попередньо зашифровані дані погано піддаються подальшому стисненню. Користувач може відключити практично марне апаратне стиснення шифрованих даних, тим самим багаторазово збільшивши необхідний обсяг для зберігання.

Не самим простим рішенням є початкове стиснення даних, а потім подальше їх шифрування. Можливо, найбільш практичним в загальному випадку рішенням є вибір для шифрування тільки найбільш важливих в сенсі безпеки даних [12].

1.3.6 Технологія виключення дублювання даних

За даними Seagate [13], за останні два десятки років продуктивність процесорів збільшилася більш ніж у два мільйони разів, в той же час продуктивність жорстких дисків – тільки в одинадцять. В даний час продуктивність наростає шляхом збільшення кількості ядер в процесорах. Очевидно, що розробники систем резервного копіювання намагаються тепер більшою мірою використовувати ресурси процесорів, ніж прив'язувати продуктивність роботи систем до характеристик пристроїв накопичувачів [7].

Дедублікація – процес визначення ідентичних елементів в багатьох різних версіях і копіях даних, і подальшого видалення надлишкових копій.

Основна ідея впровадження дедублікації – зменшення обсягів збережених даних, не погіршуючи при цьому інші характеристики. Однак, дедублікація – складний процес, який досить важко реалізувати, так що б він не знижував продуктивність. Використання дедублікації може істотно погіршити показники швидкості відновлення даних.

Безпосередньо процес дедублікації може відбуватися до того як дані будуть записані в цільове сховище або вже після запису. Рішення, які виконують процес дедублікації після запису, вимагають більшого об'єму сховищ, бо дані спочатку зберігаються повністю.

Головною перевагою впровадження дедублікації є істотна економія дискового простору. За даними досліджень компаній ESG Lab і Excillio Group Inc. [4, 15], в ході тестування технології дедублікації різних виробників, включаючи Avamar (EMC), Data Domain, Diligent, було виявлено, що в середньому обсяг даних для зберігання знижується в 10-20 разів, при цьому іноді вдається досягти зниження в 40 разів.

В результаті недавніх досліджень ESG [3] було виявлено, що 33% респондентів вважають, що технологія дедублікації є важливою складовою частиною впроваджених систем резервного копіювання на базі жорстких дисків (D2D - Disk-to-disk). Це особливо високий показник, враховуючи, що дана технологія з'явилася відносно недавно.

1.3.7 Технологія тіньового резервного копіювання

1.3.7.1 Проблема відкритих файлів. Традиційні шляхи вирішення

Для більшості компаній не представляється можливим зупинити роботу систем, щоб виконати цілісну копію всіх даних. Тобто операції резервного копіювання повинні проводитися, коли всі системи запущені і працюють.

Відкриті файли були завжди проблемою для процесу резервування.

Найчастіше системи резервного копіювання пропускають такі файли, або зберігають копію непридатну для використання після відновлення.

Одним з існуючих підходів є примусове закриття файлів або видача повідомлення користувачеві з проханням закрити використовувані програми.

При створенні резервних копій також можуть виникнути проблеми синхронізації. Приміром, компанія використовує систему управління взаємовідносинами з клієнтами CRM (англ. Customer Relationship Management), яка працює безпосередньо з бухгалтерськими системами. Може так статися, що під час створення резервних копій баз даних CRM були зроблені зміни в пов'язаних базах даних бухгалтерії, які будуть копійовані пізніше. При відновлення виявиться, що сукупність всіх даних не є цілісною.

Існує два традиційних шляхи вирішення проблеми відкритих файлів.

По-перше, деякі компанії виробники систем резервного копіювання надають інструменти, інтегровані в цільові програми, для забезпечення можливості створення цілісних резервних копій по необхідному розкладом [13].

По-друге, розробники систем резервного копіювання створюють специфічні для їх продуктів, в деякому роді універсальні системи, що дозволяють працювати з будь-якими відкритими файлами в системі. Більшість універсальних систем обмежені у своїх можливостях створювати синхронізовані копії в масштабі всієї системи. Проблема в даному випадку пов'язана з даними, розподіленими на різних фізичних носіях.

1.3.7.2 Microsoft Volume Shadow-Copy Service

Microsoft Volume Shadow-Copy Service (VSS) - це інфраструктура операційних систем Microsoft для роботи систем резервного копіювання з відкритими в системі файлами.

Спочатку подібна технологія була реалізована в ОС Windows XP, і носила назву Volume Snapshot Service, яка працювала тільки з програмою резервного копіювання що поставлялася в комплекті з ОС. Починаючи з операційної системи Windows Server 2003 функціональність даної технології була значно розширена.

VSS звертається до додатків, щоб визначити чи може бути виконана копія, іншими словами - знімок даних. Знімок даних - це копія даних на певний момент часу. Далі VSS звертається до ОС і до працюючого з даними з додатком, щоб «заморозити» виконання завдань і скопіювати необхідні дані. Якщо не призупинити виконання, копійовані дані можуть стати непридатними для роботи після відновлення, тому що копіювання може відбутися в процесі роботи програми з даними. Після цього VSS дає можливість працювати програмі резервного копіювання зі знятою копією.

Для роботи описаного процесу резервного копіювання, необхідно, щоб додаток, що працює з даними, і система резервного копіювання були «VSS сумісними». VSS сумісність означає що компонент, що бере участь в процесі резервного копіювання, спеціально спроектований відповідно до наданої Microsoft документацією описаної в SDK (англ. Software Development Kit) [10].

Не всі програми можуть бути, і будуть інтегровані в інфраструктуру VSS. Існує ряд додатків, які принципово не можуть підтримувати VSS. Наприклад, клієнт-серверні додатки, які зберігають свої дані на одній системі, а виконуються на інший.

В деякі програми розробники можуть взагалі ніколи не впроваджувати підтримку VSS просто на свій розсуд. VSS не є простим рішенням для впровадження, бо додатки повинні реалізовувати певні інтерфейси і протоколи.

В силу вище згаданих складнощів рівень адаптації технології VSS невисокий [10].

1.3.8 Сервіси віддаленого резервного копіювання

Сервіси віддаленого резервного копіювання дозволяють створювати копії даних і зберігати їх віддалено, при цьому доступ до файлів можна отримати в будь-якому місці, де є підключення до мережі Інтернет (іноді потрібна установка відповідного ПЗ).

Сьогодні більшість провайдерів online-сервісів резервного копіювання позиціонують свої послуги використовуючи модель SaaS (Software as a Service - програмне забезпечення як послуга). SaaS – це така форма пропозиції програмного забезпечення споживачеві, при якій постачальник розробляє веб-додаток, розміщує його і управляє ним для того, щоб надавати можливість його використання замовниками через Інтернет. Замовники платять не за володіння програмним забезпеченням як таким, а за можливість його використання через Інтернет. Оплата стягується зазвичай як щорічна або щомісячна абонентська плата з урахуванням обсягів збережених даних.

Безсумнівною перевагою сервісів віддаленого резервного копіювання є те, що їх використання огороджує користувача від необхідності встановлювати і підтримувати власні системи зберігання, а віддалене розміщення збільшує їхню безпеку.

Однак швидкість створення резервних копій і відновлення значно обмежена пропускною здатністю підключення до Інтернету. Також інформація у цьому випадку буде передаватися через незахищений канал.

1.4 Алгоритми резервного копіювання

Разом с швидким зростанням обсягів збережених даних зростає складність їх захисту, використовуючи стандартні традиційні алгоритми резервного копіювання.

Кожен алгоритм резервного копіювання робить компроміс між основними характеристиками процесів створення копій та операцій

відновлення даних. Найважливішими з них є швидкість реплікації, необхідний обсяг пам'яті для зберігання резервних копій, швидкість відновлення.

1.4.1 Повне резервне копіювання

Повне резервне копіювання є традиційним підходом у резервному копіюванні. Процес резервування включає копіювання всіх даних, вибраних для резервного копіювання, незалежно змінилися вони чи ні, в кожний момент резервування $t_j \in t_k$, як показано на рисунку 1.6.

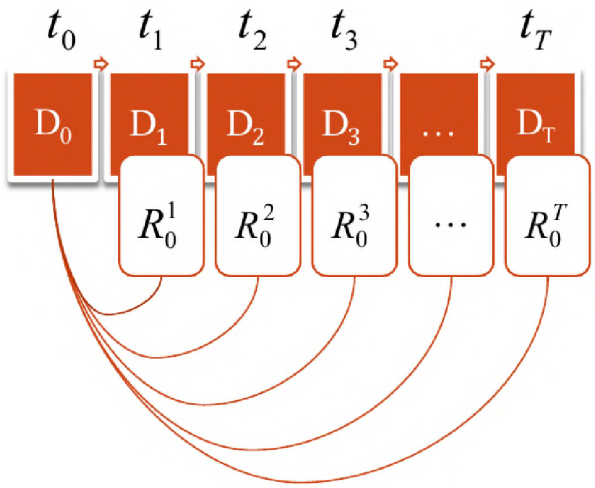

Рисунок 1.6 – Схема повного резервного копіювання

Визначення: алгоритм резервного копіювання, у процесі роботи якого послідовно в моменти часу $\{t_k, де\ k = 0,1,2, ..., T\}$ створюється набір елементів репозиторію виду $R = \{R_0^1; R_0^2; R_0^3; \ldots; R_0^T\}$, називається алгоритмом повного резервного копіювання.

Такий метод є найпростішим алгоритмічним підходом. Слід помітити такі недоліки: копіювання всіх файлів є повільним, а зберігання повних резервних копій на кожний момент часу потребує багато місця.

1.4.2 Інкрементальне резервне копіювання

Інкрементальне резервне копіювання також є традиційним алгоритмічним підходом. Спочатку, в момент часу t_1 створюється повна резервна копія даних R_0^1, а потім, в наступні моменти, створюються копії файлів, змінених з моменту

останнього резервування, тобто R_1^1, R_2^1 і так далі. Рисунок 1.7 ілюструє дану схему.

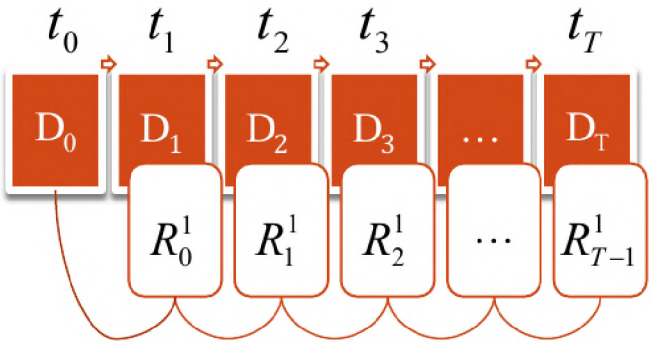

Рисунок 1.7 – Схема інкрементального резервного копіювання

Визначення: алгоритм резервного копіювання, у процесі роботи якого послідовно в моменти часу *{t_k, де $k = 0,1,2, ..., T$}* створюється набір елементів репозиторію виду $R = \{R_0^1; R_1^1; R_2^1; \ldots; R_{T-1}^1\}$, називається інкрементальним.

Інкрементное резервування займає менше часу, так як даних копіюється менше. Проте процес відновлення даних займає значну кількість часу, так як потрібний доступ до великих обсягів даних, бо повинні бути відновлені дані з повної резервної копії, плюс дані всіх наступних інкрементних копій.

Можливий ще один варіант роботи, коли кожна створювана інкрементальна копія тут же застосовується до існуючої повної резервної копії, в цьому випадку вона буде називатися дзеркалом, і потім створюється зворотна інкрементна копія. В результаті роботи такої схеми в наявності завжди існує повна резервна копія і набір зворотних інкрементний, що містять дані про зміни для можливого відновлення на попередні моменти часу.

1.4.3 Диференційне резервне копіювання

При диференціальному резервному копіюванні спочатку, в момент часу t_1 створюється повна резервна копія даних R01, а потім, в наступні моменти, створюються копії, що містять дані, змінені з моменту останнього повного

резервування, тобто R_1^1, R_1^2 і так далі. Дана схема проілюстрована на рисунку 1.8.

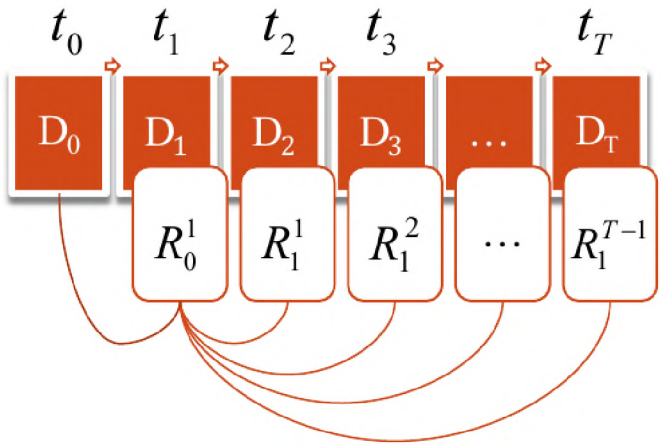

Рисунок 1.8 – Схема диференційного резервного копіювання

Визначення: алгоритм резервного копіювання, у процесі роботи якого послідовно в моменти часу $\{t_k$, де k = 0,1,2, ..., T$\}$ створюється набір елементів репозиторію виду $R = \{R_0^1; R_1^1; R_1^2; \ldots; R_1^{T-1}\}$, називається диференціальним.

Диференціальне резервування прискорює процес відновлення – для відновлення необхідно відновити дані з повної резервної копії та останньої диференціальної.

1.4.4 Мультирівневе резервне копіювання

Між крайнощами традиційних алгоритмів повного і інкрементного копіювання є інші алгоритми дозволяють знайти потрібний баланс між основними характеристиками процесів резервного копіювання. Мультирівнева схема працює таким чином: резервне копіювання ведеться в кілька рівнів: на 0-му рівні створюються повні резервні копії; на наступних - копіюються файли, модифіковані з моменту попереднього резервного копіювання нижчого рівня.

На рисунку 1.9 представлена ілюстрація роботи алгоритму мультирівневих схеми для трьох рівнів і 12-ти періодів резервного копіювання. Суцільними лініями на малюнку позначені операції резервного копіювання нульового рівня, пунктиром - першого, пунктиром з точками - другого.

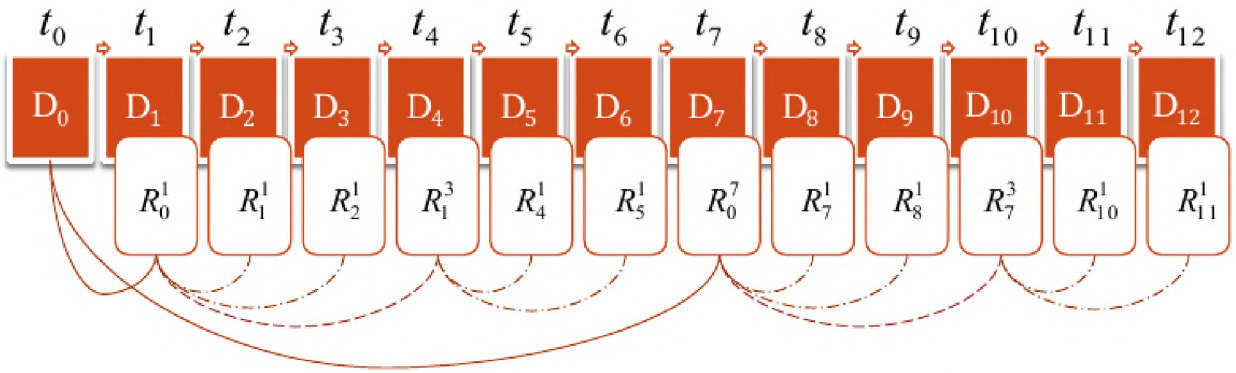

Рисунок 1.9 – Схема мультирівневого резервного копіювання

Загалом, даний алгоритм має гарні характеристиками в порівнянні з традиційними алгоритмами повного і інкрементного копіювання. Для відновлення даних необхідно скористатися останніми елементами репозиторію кожного рівня. Час необхідний для відновлення до початкового стану не на багато перевершує час для схеми повного резервного копіювання. Загальна кількість місця необхідна для зберігання резервних копій порівняна з вимогами інкрементного підходу.

Рівнева схема має недолік – нерівномірне у часі використання пам'яті для створення резервних копій. Так на деякі дні випадає необхідність зберігати в десятки разів більше даних, ніж в інші, тобто користувач повинен утримувати обладнання, яке повинно справлятися з потребами нульового рівня, і яке буде простоювати більшу частину часу.

1.4.5 Схема А.М. Костелло, К. Юманса, Ф. Ву

Розглянемо схему резервного копіювання, розроблену А.М. Костелло, К. Юмансом і Ф. Ву в Університеті Каліфорнії в Берклі, США.

При роботі даного алгоритму копіювання ведеться паралельно, в кілька рівнів, в результаті створюється сукупність наборів елементів сховища. На 0-му рівні створення резервних копій ідентично инкрементній схемі. Всі інші рівні надлишкові - створюються для збільшення швидкості відновлення.

На рисунку 1.10 представлена ілюстрація схеми Костелло-Юманса-Ву для

трьох рівнів і 12-ти періодів резервного копіювання (параметр схеми-база ‖ b = 2).

Часткове створення на малюнку позначено елементами сховища в дужках. Суцільними лініями на малюнку позначені операції резервного копіювання нульового рівня, пунктиром - першого, пунктиром з точками - другого.

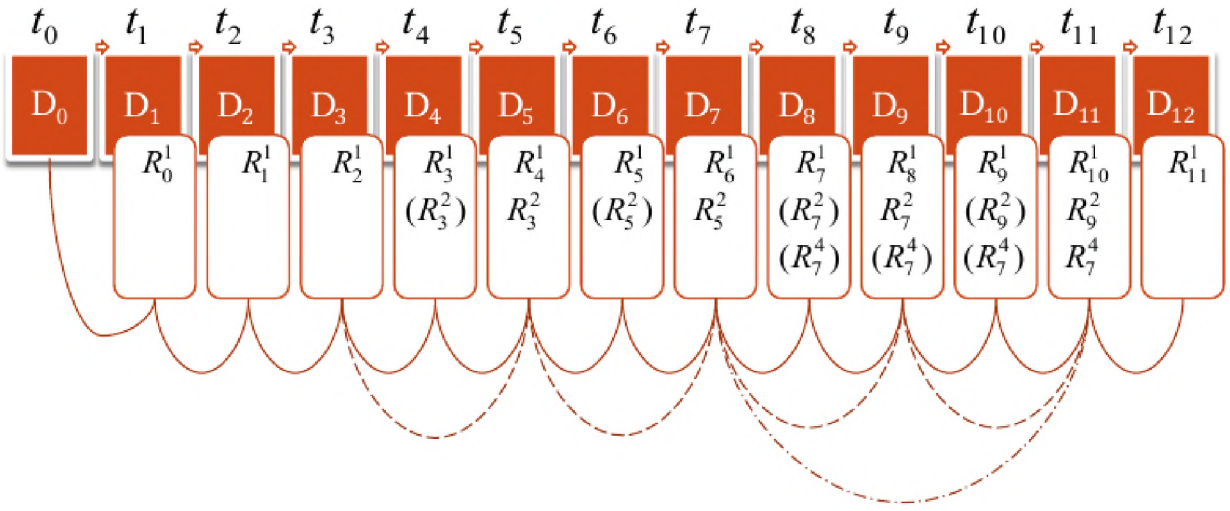

Рисунок 1.10 – Схема резервного копіювання А.М. Костелло, К.Юманса, Ф. Ву

Елементи резервного копіювання створюються поступово в кілька підходів, за кілька моментів резервного копіювання, що забезпечує рівне використання обсягу сховища в часі і робить придатним для online-режиму роботи.

1.4.6 Алгоритм «Z scheme»

Алгоритм резервного копіювання «Z scheme» розроблений у Технологічному Інституті в Джорджії, США. «Z scheme» здійснює паралельні операції резервного копіювання також в декілька потоків, в результаті створюється сукупність наборів елементів сховища. На нульовому рівні створення резервних копій ідентично инкрементной схемою. Всі інші рівні надлишкові і створюються для збільшення швидкості відновлення.

Файли копіюються деяким потоком рівня і якщо тільки він був змінений b^i моментів створення резервних копій (наприклад, днів) назад, де b - зовнішній

параметр схеми, названий базою. Нульовий рівень є не що інше, як інкрементна схема.

Алгоритм «Z scheme» близький за основними характеристиками до мультирівневої схеми, але позбавлений недоліку зв'язаного з нерівномірним використанням пам'яті.

1.5 Висновок

У розділі було розглянуто особливочті методів резервного копіювання даних, та систем зберігання інформації.

Основні стандартні алгоритми резервування даних:

- повне резервування;
- інкрементальне резервування;
- диференційне резервування.

Огляд та аналіз існуючих алгоритмів дав можливість визначити переваги та недоліки кожного з них.

Були оглянуті та проаналізовані засоби зберігання інформації:

- носії інформації;
- спеціалізовані системи зберігання інформації;
- віртуальне зберігання інформації.

Отже, дослідження системи резервування підприємства повинно вказати на недоліки існуючої системи та допомогти в розробці критеріїв для впровадження нової системи резервування, яка б відповідала потребам підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Аналіз циркулюючої інформації на підприємстві

Всю інформацію, що циркулює на підприємстві можна розділити на відкриту та інформацію з обмеженим доступом (ІзОД) (рисунок 2.1).

Інформація з обмеженим доступом – інформація доступ до якої має лиш обмежене коло осіб і оприлюднення якої заборонено законом.

До відкритої інформації комерційного підприємства можна віднести:

- прайс-листи підприємства;
- перелік послуг;
- презентації;
- зображання;
- відеоматеріали (медіа контент).

До інформації з обмеженим доступом відноситься:

- персональні дані;
- бухгалтерська документація;
- бізнес плани.

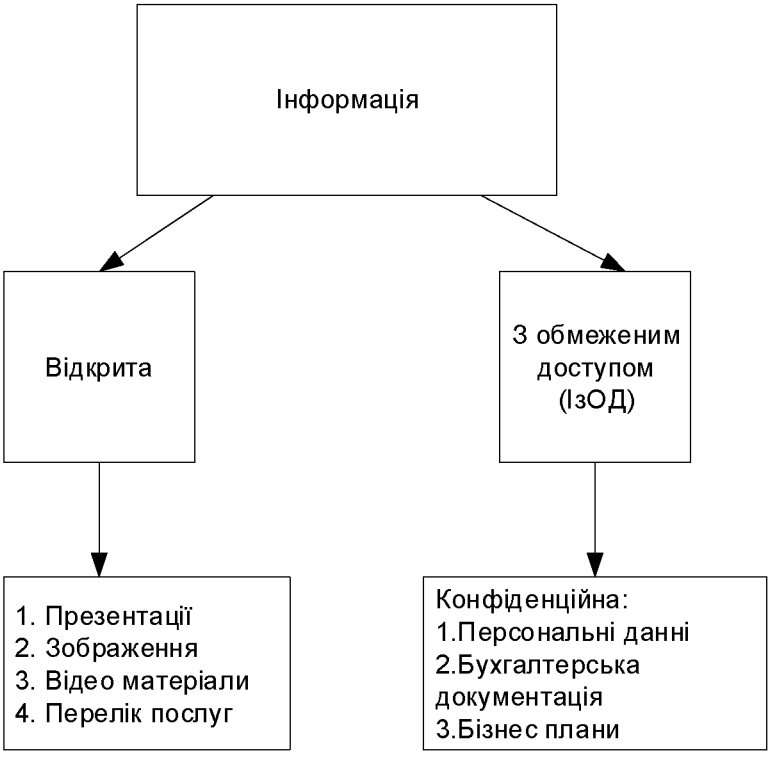

Рисунок 2.1 – Інформація на підприємстві

2.2 Аналіз загроз

Загрози для інформації можна класифікувати за ймовірністю їх втілення. Аналіз загроз представлена в таблиці 2.1.

Таблиця 2.1 – Аналіз загроз

Перелік загроз	Ймовірність
Ненавмисне псування або видалення даних через помилку користувача	1
Ненавмисне псування або видалення даних через помилку адміністратора	2
Повна або часткова(погані блоки) відмова диска	2
Втрата сервера (крадіжка, пожежа, затоплення)	2
Помилки додатків, які призводять до видалення і псування даних	1
Помилки ОС, що приводять до пошкодження файлової системи або окремих файлів	2
Раптове відключення живлення, що призводить до невідновного пошкодження файлової системи	2
Псування чи видалення даних в результаті дій зловмисника або вірусної програми	3
Виявлення пропажі даних після закінчення зберігання резервних копій.	3

Ймовірність: 1 – висока, 2 – середня, 3 – низька.

Наслідки втрати даних:

- прямі втрати для бізнесу (клієнти, замовлення);
- погіршення іміджу підприємства, проблеми з наглядовими органами
- втрати робочого часу;
- невпевненість працівників, вони починають копіювати дані власноруч;

– адміністративні наслідки для системного адміністратора або керівника відділу.

2.3 Модель порушника

Модель порушника являє собою формальний опис порушника, його можливих дій та результатів його дій щодо даних підприємства.

По відношенню до АС порушники можуть бути внутрішніми або зовнішніми.

Внутрішніми порушниками можуть бути:

а) працівники підприємства;

б) системні адміністратори.

Зовнішнім порушником є зловмисники які можуть провести атаку на мережу підприємства з мережі Інтернет.

Метою порушника є:

– отримання інформації у потрібному обсязі та асортименті;

– внесення змін в інформаційні потоки у відповідності зі своїми намірами;

– нанесення збитків шляхом знищення інформації;

– призупинення роботи підприємства шляхом обмеження доступу до даних.

Внутрішні порушники мають доступ до всієї циркулюючої інформації на підприємстві, тому результатом їх дій може бути порушення конфіденційності, цілісності та доступності інформації при будь-яких видах атак.

Працівники підприємства мають можливість змінити або пошкодити данні, не коректна виконуючи різні додатки, чи навмисно видалити їх або заразити систему вірусними програмами.

Системні адміністратори мають повний обсяг можливостей щодо впливу на інформацію на рівні проектування системи зберігання та резервування даних, реалізації, впровадження, супроводження АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації. Володіють інформацією про функції та механізм дії засобів захисту.

Використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи.

2.4 Профіль захищеності

Інформація, яка резервується повинна мати рівні гарантій, які забезпечують її цілісність, доступність та конфіденційність. Рівні гарантій зіставляються із існуючими профілями захищеності. Рівні гарантій можуть бути розширеними, якщо необхідно виконати необхідні додаткові умови для нормального функціонування додатку згідно запропонованим бізнес – механізмам.

Важливість резервованої інформації зумовлює те, що забезпечення цілісності, доступності та конфіденційності інформації, що циркулює на підприємстві є найбільш пріоритетним завданням. Висока пріоритетність пояснюється тим, що користувачі повинні отримати доступ до інформації, що була втрачена або зіпсована у найкоротший проміжок часу, для того щоб збитки були мінімальними.

Забезпечення конфіденційності інформації у системі резервування даних включає в себе механізми захисту інформації з обмеженим доступом із використанням програмних засобів.

Використавши документ НД ТЗІ 2.5-005-99 визначаємо наступний мінімально необхідний рівень послуг безпеки для забезпечення захисту інформації від загроз.

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

3.КЦД.1 = {КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

КД-2 – базова довірча конфіденційність;

КО-1 – повторне використання об'єктів;

КВ-1 – мінімальна конфіденційність при обміні;

ЦД-1 – мінімальна довірча цілісність;

ЦО-1 – обмежений відкат;

ЦВ-1 – мінімальна цілісність при обміні;

ДР-1 – квоти;

ДВ-1 – ручне відновлення;

НР-2 – захищений журнал;

НИ-2 – одиночна ідентифікація і автентифікація;

НК-1 – однонаправлений достовірний канал;

НО-2 – розподіл обов'язків адміністраторів;

НЦ-2 – КЗЗ з гарантованою цілісністю;

НТ-2 – самотестування при старті;

НВ-1 – автентифікація вузла.

В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації.

Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів.

КС забезпечує послугу повторне використання об'єктів (КО-1), якщо перед наданням користувачеві або процесу в розділювальному об'єкті не залишається інформації, яку він містив, і скасовуються попередні права доступу до об’єкта. Критерії не встановлюють, коли саме має виконуватися очищення

об'єкта. Залежно від реалізованих механізмів можна виконувати очищення об'єкта під час його звільнення користувачем або безпосередньо перед його наданням наступному користувачу. Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

Послуга конфіденційність при обміні (КВ-1) дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування. Так, реалізація даної послуги на рівні КВ-1 забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

Мінімальна довірча цілісність (ЦД-1). На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

Відкат (ЦО-1) є багатосторонньою послугою, що дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або апаратури і підтримувати цілісність баз даних, додатків, побудованих на транзакціях і т. ін. Дана послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об’єкт до попереднього стану. Дана

послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівень ЦВ-1 даної послуги забезпечує мінімальний захист.

Послуга мінімальної цілісності при обміні (ЦВ-1), що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.

Послуга використання ресурсів (ДР-1) дозволяє керувати використанням послуг і ресурсів користувачами. Найслабкішою формою контролю за використанням ресурсів є використання квот. Всі захищені об'єкти КС (наприклад, дисковий простір, тривалість сеансу, час використання центрального процесора і т. ін.) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу. На даному рівні послуги немає гарантій, що користувач не зможе повністю захопити решту певного ресурсу, обмежуючи тим самим доступ до нього інших користувачів.

Послуга відновлення після збоїв (ДВ-1) забезпечує повернення КС до відомого захищеного стану після відмови або переривання обслуговування. Якщо відновлення неможливе, то КЗЗ повинен переводити систему до стану, з якого її може повернути до нормального функціонування тільки адміністратор.

Реєстрація (НР-2) – це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Використання засобів перегляду і аналізу журналів, а особливо засобів налагодження механізмів фіксування подій, має бути прерогативою спеціально авторизованих користувачів. Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке

переміщення таких даних має виконуватись способом, що гарантує їх безпеку. Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку забезпечують реалізовані послуги конфіденційності і цілісності. Повинні бути вироблені угоди щодо планування і ведення архівів даних реєстрації. Критична для безпеки подія визначається як подія, пов'язана з звертанням до якої-небудь послуги безпеки або результатів виконання якої-небудь функції КЗЗ, або як будь-яка інша подія, яка хоч прямо і не пов'язана з функціонуванням механізмів, які реалізують послуги безпеки, але може призвести до порушення політики безпеки.

Ідентифікація і автентифікація (НИ-2) дозволяють КЗЗ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем. За результатами ідентифікації і автентифікації користувача система (КЗЗ), по-перше, приймає рішення про те, чи дозволено даному користувачеві ввійти в систему, і, по-друге, використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача, що увійшов.

Послуга достовірний канал (НК-1) дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається).

Послуга розподіл обов'язків (НО-2) дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій. Система, що претендує на включення даної послуги до рейтингу, повинна передусім забезпечувати існування ролей для адміністратора і звичайного користувача

(рівень НО-1). Для наступного рівня даної послуги вимагається, щоб система підтримувала дві або більше адміністративних ролей зі специфічними наборами адміністративних обов'язків. Одна з цих ролей повинна бути роллю адміністратора безпеки (ця роль може бути поділена на ролі адміністратора реєстрації (аудиту) і адміністратора каталогів або облікових карток користувачів). Роль адміністратора безпеки повинна бути визначена так, щоб обов'язки, що мають відношення до безпеки, могли бути виконані тільки в цій ролі. Ролі не обов’язково мають бути абсолютно взаємовиключними, оскільки деякі функції або команди можуть знадобитись і адміністратору, і користувачу, або різним адміністраторам і т. ін.

Послуга цілісність комплексу засобів захисту (НЦ-2) визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Рівень НЦ-1 даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг. Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Самотестування (НТ-2) дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС.

Послуга ідентифікація і автентифікація при обміні (НВ-1) дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Реалізація рівня НВ-1 даної послуги дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні [1-4].

Проаналізуємо, чи всі функціональні послуги безпеки стандартного профілю реалізовані в АС підприємства.

Послуга КД-2 реалізується службою каталогів (Active Directory) ОС Windows Server і передбачає, що атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково існує можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації

Послуга КВ-1 реалізується за допомогою програмного шифрування файлів перед їх передачею каналами зв'язку або прозорого шифрування файлів перед їх записуванням на диск за допомогою вбудованих в ОС криптоалгоритмів (ПЗ BitLocker Drive Encryption, що використовує надійні криптоалгоритми для прозорого шифрування даних).

Послуга ЦД-1 реалізується в системі за допомогою розмежування прав доступу (групові політики) в ОС. Існує можливість розмежування доступу для груп користувачів.

Послуга ЦО-1 реалізується за допомогою стандартної утиліти Microsoft Windows, що дозволяє відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу, також можна використати спеціальне програмне забезпечення для відновлення роботи системи корпорації Symantec Backup Exec або .

Послуга ЦВ-1 реалізується за рахунок використання контрольних сум, хеш-функцій та цифрового підпису, що присутні в ОС. КЗЗ забезпечує можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.

Послуга ДР-1 реалізується наданням адміністратором квот користувачам (дискового простору, оперативної пам’яті, ресурсів процесора та інше) стандартними засобами серверної ОС.

Відновлення системи (послуга ДВ-1) проходить за допомогою засобів ОС і забезпечує повернення КС до відомого захищеного стану після відмови або переривання обслуговування.

Для реалізації послуги НР-2 використовується журнал реєстрації Windows, що протоколює все значимі події безпеки, а також всі основні дії користувача в системі.

Для реалізації послуги НИ-2 використовується служба каталогів (протоколи NTLMv4 або Kerberos, більш надійний другий протокол).

Реалізація послуги НК-1 передбачає використання протоколу SSL 3.0 або TLS1.0 та ЕЦП (наприклад, ECDSA), які присутні в ОС.

Для реалізації послуги НО-2 необхідне виділення ролей адміністратора системи та адміністратора безпеки, тому треба розділити роль адміністратора системи на дві – адміністратор безпеки та системний адміністратор.

Послуга НЦ-2 реалізована за допомогою підтримки КЗЗ власного домену виконання завдяки засобам розмежування доступу ОС.

Для реалізації послуги НВ-1 необхідне використання протоколу автентифікації Kerberos, що наявний в ОС Windows.

Послуга НТ-2 реалізована частково, тому що самотестування КЗЗ здійснюється при старті системи за допомогою процедури POST (Poweronself-test), а для тестування на запит користувача можна використовувати ПЗ Memtest, HDDScan.

Послуга КО-1 частково реалізована, тому що після завершення роботи користувач повинен вимкнути або перезавантажити комп’ютер, якщо зробити це неможливо, треба використовувати спеціальне ПЗ для декількаразового перезапису оперативної пам'яті комп'ютера Ainvo Memory Cleaner 2.4.3.570. Зазвичай, достатнім вважається трьохразовий перезапис випадковими даними.

Тобто, маємо три частково реалізовані та нереалізовані послуги безпеки: НО-2, НТ-2 та КО-1.

3.КЦД.1 = { КД-2, КО-1, КВ-1,

ЦД-1, ЦО-1, ЦВ-1,

ДР-1, ДВ-1,

НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }.

Також, слід звернути увагу на те, що послуга НО-1 є необхідною умовою для реалізації послуг ДР-1 та ДВ-1. Тобто, поки не реалізована функціональна послуга безпеки НО-1, послуги ДР-1 та ДВ-1 теж вважаємо нереалізованими.

Запропоновано наступні рекомендації щодо приведення КЗЗ до захищеного стану:

– потрібно розділити роль адміністратора системи на дві – адміністратор безпеки та системний адміністратор.

Дана міра необхідна через те, що адміністратор – це особа, що має високі привілеї, знання та повноваження в автоматизованій системі і несе відповідальність за роботу АС та КЗЗ. Від адміністратора залежить працеспроможність всієї автоматизованої системи, а його дії підзвітні лише керівникові, який може не мати достатньої компетенції в питаннях адміністрування та захисту системи. Якщо адміністраторів буде декілька, вони зможуть контролювати виконання службових обов'язків один одного та не допустити витоку інформації з обмеженим доступом. До того ж, часто обсяг роботи адміністратора дуже значний та перевищує навантаження на одну людину;

– для тестування КЗЗ на запит користувача використовувати ПЗ Memtest. Найкритичнішим етапом самотестування КЗЗ є перевірка оперативної пам'яті. Тому для підвищення надійності перевірки, запропоновано використання програмного забезпечення MemTest 4.1.

MemTest – утиліта, призначена для тестування надійності роботи оперативної пам'яті. При тестуванні оцінюється здатність пам'яті записувати і зчитувати дані. Є можливість задавати кількість мегабайт для тестування. Розробники рекомендують використовувати цю утиліту для тестування оперативної пам'яті при «розгоні» системи з метою виявлення відхилень і нестабільності роботи комп'ютера. MemTest допоможе протестувати стабільність системи після внесених змін;

– використовувати спеціальне ПЗ для кількаразового (бажано 3 рази) перезапису оперативної пам'яті комп'ютера Ainvo Memory Cleaner 2.4.1.470.

Перед кожним входом користувача в систему необхідно проводити очищення оперативної пам'яті для унеможливлення витоку інформації з обмеженим доступом через зчитування змісту регістрів.

2.5 Процес планування системи резервування та відновлення даних

1. Чому необхідна система резервування даних:

– розбиття даних на групи;

– оцінка вартості втрати/пошкодження даних;

– оцінка вартості простою на час відновлення системи.

2. Що необхідно резервувати:

– всю систему (диск, розділ);

– окремі файлові системи;

– окремі файли.

3. Визначення RTO і RPO для кожної групи даних та причини втрати

4. Розклад резервування:

– Періодичність повного та інкрементального резервування;

– Допустимий рівень втрати продуктивності виробничої системи. (вікно резервування).

5. Де повинні зберігатися зарезервовані дані: закрите приміщення або зовнішнє сховищє, каталог (БД) носіїв (номер, ім'я , місце), мітки на носіях, сховищє носіїв.

6. Хто відповідальна особа.

2.6 Дослідження засобів резервування

Резервування даних на підприємстві:

Інформація з серверу резервується на окремий жорсткий диск.

Використовується алгоритм повного резервного копіювання, тобто кожен раз зберігається повна копія даних.

Автоматизація резервного копіювання відсутня, при потребі відновити дані всі операції потрібно робити вручну.

Шифрування даних не відбувається.

В таблиці 2.2 наведене дослідження засобів резервування.

Таблиця 2.2 – Дослідження засобів резервування підприємства

Вимоги	Результат
Використовуваний алгоритм резервування даних	Повне копіювання
Архівація, шифрування даних	Архівація

Продовження таблиці 2.4

Вимоги	Результат
Автоматизація резервного копіювання	Відсутня, резервування відбувається вручну.
Розклад резервування	1 раз на місяць
Місце зберігання резервованих даних	Сервер
Стійкість до відмов	Відсутня

Недоліки:

– постійне повне копіювання. Повне копіювання є повільним, зберігання повних копій на кожний момент часу потребує багато місця;

– на підприємстві циркулює інформація з обмеженим доступом, тому шифрування даних резервної копії необхідно;

– автоматизація забезпечує обов’язкове копіювання даних за розкладом, у той час як в ручному режимі відповідальна особа може забути зробити резервну копію;

– резервування інформації 1 раз на місяць є недостатнім, так як резервна копія даних на початок місяця буде значно відрізнятися від інформації в середині місяці або ж на прикінці;

– зберігати резервну копію даних у тому ж місці де зберігається основна база даних не рекомендується. При виході з ладу серверу, резервна копія буде знищена або пошкоджена;

– немає дублювання інформації.

2.6.1 Тести на швидкість резервного копіювання даних

Було проведено ряд тестів часу резервного копіювання. В якості вихідних даних були використані файли які добре стискаються(тестові, документи), так і ті які погано піддаються стисканню, такі як аудіо та відео файли, зображання.

Таблиця 2.3 – Результати тестування системи резервування

Вихідні дані	Ступінь стиснення	Отримана резервна копія (Повна)
Кількість файлів: 65 124 Сукупний об’єм:64ГБ	Без стискання	Час створення: 3 години 34 хвилини 21 секунда Розмір: 64 Гб
	Середній	Час створення: 4 години 23 хвилини 17 секунд Розмір: 41 Гб
	Максимальний	Час створення: 5 годин 41 хвилина 56 секунд Розмір:35 Гб

2.7 Аналіз програмних засобів для резервування інформації

У таблиці 2.4 наведені результати аналізу програмних засобів резервування

Таблиця 2.4 – Аналіз програмних рішень для резервування даних

Назва	Genie Backup Manager	Acronis True Image	NTI Backup Suite	PowerBac	Norton Ghost	AISBackup	Exiland Backup	Handy Backup	Migo PC Backup	WinBackup
Схеми резервного копіювання										
Повне	+	+	+	+	+	+	+	+	+	+
Інкрементальне	+	+	+	+	+	+	+	+	+	+
Диференційне	+	+	+	+			+		+	
Можливості										
Резервування окремих файлів	+	+	+	+	+	+	+	+	+	+

Продовження таблиці 2.4

Назва	Genie Backup Manager	Acronis True Image	NTI Backup Suite	PowerBac	Norton Ghost	AISBackup	Exiland Backup	Handy Backup	Migo PC Backup	WinBackup
Резервування окремих каталогів	+	+	+	+	+	+	+	+	+	+
Створення образів диску		+			+	+	+	+	+	
Копіювання реєстру	+	+	+		+	+		+	+	
Задання розкладу	+	+	+	+	+	+	+	+	+	+
Підтримка резервного копіювання для поштових клієнтів										
Outlook Express	+	+	+	+		+	+	+		+
Outlook	+	+	+	+		+	+			+
Носії резервних копій										
Жорсткі диски	+	+	+	+	+	+	+	+	+	+
Змінні носії (CD, DVD, Flash)	+	+	+	+	+	+	+	+	+	+
FTP	+	+	+			+	+	+	+	
Додаткові можливості										

Парольний захист	+	+	+	+	+	+	+	+	+	+
Шифрування резервних копій	+	+	+			+	+	+		
Стискання даних	+	+	+	+	+	+	+	+	+	+
Налагодження фільтрів для файлів що копіюються	+	+	+	+	+	+	+	+	+	+
Верифікація копій	+	+	+	+	+	+	+	+	+	+
Журналювання	+	+	+	+	+	+	+		+	+
Запис оптичних дисків	+	+	+	+	+	+	+	+	+	+
Створення самозавантажуваних резервних копій	+		+	+			+	+	+	+
Підтримувані ОС										
Windows 7 / 8 / 10	+	+			+	+	+	+	+	
Windows XP	+	+	+	+	+	+	+	+	+	+
Windows Server 2008	+						+	+		

За даними аналізу ПЗ для резервного копіювання, рекомендовано вибрати Exiland Backup.

2.8 Порівняння основних алгоритмів резервування даних

Основні алгоритми резервування:

- повне резервне копіювання;
- інкрементне резервне копіювання;
- диференціальне резервне копіювання.

На таблиці 2.5 представлена порівняльна характеристика алгоритмів резервного копіювання.

Таблиця 2.5 – Порівняльна характеристика алгоритмів резервного копіювання

	Повне	Інкрементне	Диференційне
Швидкість створення резервних копій	Низька	Висока	Середня

Швидкість відновлення інформації	Висока	Низька	Середня
Можливість часткового відновлення даних	Відсутня	Відновлення з будь-якої інкрементної копії	Відновлення тільки з останньої інкрементної копії
Місце яке займається на диску	Кожна копія займає повний обсяг місця	Місце займає 1 повна копія та часткові інкрементні копії	Місце займає 1 повна копія і 1 копія з останніми змінами даних

2.9 Рекомендації до побудови системи резервування даних

– використання програмної системи;

– використання шифрування і архівації інформації з обмеженим доступом;

– використання алгоритму, який як найкраще відповідав вимогам підприємства;

– резервне копіювання повинно відбуватися автоматично за розкладом;

– резервні копії повинні робитися на зовнішніх носіях;

– об’єм носіїв повинен бути достатнім для збереження резервних копій за певний проміжок часу;

– повинна робитися більше ніж 1 резервна копія;

– носії з резервними копіями повинні зберігатися в надійному місці.

2.10 Рекомендована система резервування

Таблиця 2.6 – Рекомендації

Критерії	Рекомендації
Програма резервування	Exiland Backup Server
Шифрування, архівація	Проведення архівації і шифрування даних використовуючи метод 256 bit-AES
Алгоритм резервування	Інкрементне резервне копіювання
Розклад резервування	Раз на місяць повне резервне копіювання, кожен тиждень інкрементне резервування
Носії інформації	Зовнішні жорсткі диски
Дублювання інформації	Резервування відбувається паралельно на 2 носія для того щоб покращити доступність інформації
Місце зберігання носіїв	Після проведення резервного копіювання диски зберігаються в захищеному приміщені

2.11 Висновок

Результатом проведеної роботи в розділі став вибір профілю захищеності для системи резервування даних, аналіз загроз інформації, огляд стандартних алгоритмів резервного копіювання, проведений аналіз програмних засобів резервування.

Проведено дослідження засобів резервування даних, виявлено їх недоліки.

Розроблені рекомендації до побудови системи резервування даних на підприємстві.

Створена система резервування даних підприємства, яка відповідає всім поставленим вимогам.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою цього розділу є обґрунтування економічної доцільності застосування методів підвищення захищеності засобів резервування даних на комерційному підприємстві. Для досягнення поставленої мети необхідно здійснити наступні розрахунки:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від засобів резервування даних на комерційному підприємстві;

– показники економічної ефективності застосування засобів резервування даних на комерційному підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

3.1.1. Визначення витрат на створення програмних засобів захисту інформації

3.1.1.1 Визначення трудомісткості розробки та опрацювання засобів резервування даних на підприємстві

Визначення трудомісткості розробки та опрацювання засобів резервування даних на підприємстві здійснюється, виходячи з тривалості кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації:

$$t = tmз + tв + ta + tmехн + tр + tn + tс + tвпр \text{ , годин,} \qquad (3.1)$$

де $tmз$ – тривалість складання технічного завдання на розробку додаткових рекомендацій та посадових інструкцій, $tmз$ = 8 год.;

$tв$ – тривалість вивчення ТЗ, літературних джерел за темою тощо, $tв$=16 год.;

ta – тривалість аналізу нормативно-правової бази України, ta= 24 год.;

$tmехн$ – тривалість аналізу технології резервування даних, $tmехн$= 20 год.;

tp – тривалість складання моделі ризику, tp= 16 год.;

tn – тривалість складання моделі порушника, tn= 16 год.;

tc – тривалість розробки додаткових рекомендацій та посадових інструкцій, tc = 32 год.;

$tвпр$ – тривалість впровадження резервування даних, $tвпр$ = 24 год.

Тоді:

$$t = tmз+tв+ta+tпр+tопр+ tд=8+16+24+20+16+16+32+24=156 \text{ год.}$$

3.1.1.2 Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту ***Кпз*** складаються з витрат на заробітну плату виконавця програмного забезпечення ***Ззп*** і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК ***Змч***:

$$K_{пз} = З_{зп} + З_{мч} . \qquad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування) і визначається за формулою:

$$З_{зп} = t \cdot З_{пр}, \quad \text{грн.}, \tag{3.3}$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн./годину.

За формулою (3.3) визначається заробітна плата виконавця з урахуванням середньогодинної заробітної плати з нарахуваннями у розмірі 100,25 грн./годину.

$$З_{зп} = 156 \cdot 100{,}25 = 15639 \quad \text{грн.},$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_{д} \cdot С_{мч}, \quad \text{грн.}, \tag{3.4}$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_{д}$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою (3.4):

$$З_{мч} = 6{,}75 \cdot 2{,}85 + 2{,}1 \cdot 2{,}85 = 24{,}19 \quad \text{грн.}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot Се + \frac{Ф_{зал} \cdot На}{F_р} + \frac{К_{лпз} \cdot На_{пз}}{F_р}, \quad \text{грн.}, \tag{3.5}$$

де P – встановлена потужність ПК (P = 0,8 кВт);

C_e – тариф на електричну енергію (C_e = 1,64 грн./кВт за годину);

$Ф_{зал}$ – залишкова вартість ПК на поточний рік ($Ф_{зал}$ = 3997 грн.);

H_a – річна норма амортизації на ПК (H_a = 0,1 частки одиниці);

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення ($H_{апз}$ = 0,2 частки одиниці);

$K_{лпз}$ – вартість ліцензійного програмного забезпечення ($K_{лпз}$ = 1827 грн.);

F_p – річний фонд робочого часу (за 40-годинного робочого тижня (F_p = 1920 годин).

Вартість 1 години машинного часу ПК визначається за формулою (3.5):

$$C_{Мч} = 0{,}8 \cdot 1 \cdot 1{,}64 + \frac{3997 \cdot 0{,}1}{1920} + \frac{1827 \cdot 0{,}2}{1920} = 2{,}85 \text{ грн.}$$

Витрати на створення програмного продукту $К_{пз}$ визначаються за формулою (3.2)

$$K_{пз} = 15639+24{,}19=15663{,}19 \text{ грн.}$$

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Визначена таким чином вартість створення програмного забезпечення *Кпз* є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Вартість безстрокової ліцензії Exiland Backup Standard для юридичних осіб при закупівлі її на 2-15 ПК складає 650 грн. Програмне забезпечення встановлюється на 3 ПК.

Таким чином, капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}\ , \qquad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки ($К_{пр}$=15663,19 грн.);

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), ($К_{зпз}$ = 650*3=1950 грн.);

Капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки визначаються за формулою (3.6):

$$К = 15663,19 + 1950 = 17613,19 \text{ грн.}$$

3.1.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}\ , \quad \text{грн.} \qquad (3.7)$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в}$ = 0);

$С_{к}$ - витрати на керування системою в цілому обчислюються за формулою (3.8);

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ = 0 грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.} \qquad (3.8)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н$ = 0 грн.).

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій.

Амортизації підлягає програмне забезпечення Exiland Backup Standard загальною вартістю 1950 грн. з припустимим строком дії користування 2 роки. Таким чином, річні амортизаційні відрахування за прямолінійним методом нарахування складуть:

$$С_а = 1950 / 2 = 975 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.15)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного системного адміністратора на місяць складає 15000 грн. Додаткова заробітна плата –8% від основної заробітної плати. Отже,

$$С_з = 15000*12 + 15000*12*0,08= 194400 \text{ грн.}$$

З 01.01.2016 року ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 194400*0,22 = 42768 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р = 0,8 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою (3.16):

$$С_{ел} = 0,8*1920*1,64 = 2519,04 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат -1% ($С_{тос}$ = 17613,19*0,01=176,13 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються за формулою (3.8):

$$С_к = 975 + 194400 + 42768 + 2519,04 + 176,13 = 240\,838,17 \text{ грн.}$$

Річні поточні витрати на функціонування системи інформаційної безпеки визначаються за формулою (3.9):

$$С = 240\,838,17 \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості збитку застосовуємо спрощену модель оцінки.

Необхідні вхідні дані для розрахунку:

де $t_п$ – час простою вузла внаслідок атаки ($t_п$ = 12 годин);

$t_в$ – час відновлення після атаки персоналом ($t_в$ = 8 годин);

$t_{вi}$ – час повторного введення загубленої інформації співробітниками атакованого сегменту мережі ($t_{вi}$ = 7 годин);

$З_о$ – заробітна плата обслуговуючого персоналу ($З_о$ = 8000 грн. на місяць);

$З_с$ – заробітна плата співробітників атакованого вузла ($З_с$ = 10000 грн. на місяць);

$Ч_о$ – чисельність обслуговуючого персоналу ($Ч_о$ = 2 особи);

$Ч_с$ – чисельність співробітників атакованого сегменту мережі ($Ч_с$ = 2 особи);

О – обсяг продажів атакованого сегменту мережі, (О = 260000 грн. на рік);

$П_{зч}$ – вартість заміни устаткування або запасних частин, ($П_{зч}$ = 0 грн.);

I – число атакованих вузлів (I = 3);

N – середнє число атак на рік (N = 30).

Упущена вигода від простою атакованого вузла становить:

$$U = П_п + П_в + V, \qquad (3.10)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн.;

$П_в$ – вартість відновлення працездатності сегмента мережі, грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла, грн.

Упущена вигода від простою атакованого вузла визначається за формулою (3.10):

$$U = 681,82 + 761,37 + 3375 = 4818,19 \text{ грн.},$$

Втрати від зниження продуктивності співробітників атакованого сегмента мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} \cdot t_п \quad , \tag{3.11}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить F = 176 годин).

Втрати від зниження продуктивності співробітників атакованого сегмента мережі визначаються за формулою (3.18):

$$П_п = \frac{10000}{176} \cdot 12 = 681{,}82 \text{ грн.},$$

Витрати на відновлення працездатності сегмента мережі включають кілька складових:

$$П_в = П_{ві} + П_{пв} + П_{зч}, \tag{3.12}$$

де $П_{ві}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення сегмента мережі, грн.;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн..

Витрати на відновлення працездатності сегмента мережі визначаються за формулою (3.12):

$$П_в = 397{,}73 + 363{,}64 = 761{,}37 \text{ грн.},$$

Витрати на повторне введення інформації $П_{ві}$ розраховуються, виходячи з розміру заробітної плати співробітників атакованого сегмента мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ві}$:

$$П_{вi} = \frac{\sum Зс}{F} \cdot t_{вi} \ . \qquad (3.13)$$

Витрати на повторне введення інформації визначаються за формулою (3.13):

$$П_{вi} = \frac{10000}{176} \cdot 7 = 397{,}73 \text{ грн.}$$

Витрати на відновлення сегмента мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу:

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в \ . \qquad (3.14)$$

Витрати на відновлення сегмента мережі визначаються за формулою (3.14):

$$П_{пв} = \frac{8000}{176} \cdot 8 = 363{,}64 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого сегмента мережі визначаються виходячи із середньогодинного обсягу продажів типового підприємства і сумарного часу простою атаковано сегмента мережі:

$$V = \frac{O}{Fp} \cdot (t_п + t_в + t_{вi}) \text{ , грн.} \qquad (3.15)$$

де $F_р$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько ($F_р$ = 2080 годин).

Втрати від зниження очікуваного обсягу продажів типового підприємства визначаються за формулою (3.15):

$$V = \frac{260000}{2080} \cdot (12 + 8 + 7) = 3375 \text{ грн.},$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum_l \sum_n U = 3*30*4818,19=433637,1 \text{ грн} \quad (3.16)$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.}, \quad (3.17)$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (95%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і визначається за формулою (3.17):

$$E = 433637,1*0,95 - 240\ 838,17 = 171117,075 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \tag{3.18}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI визначається за формулою (3.18):

$$ROSI = \frac{171117,075}{17619,19} = 9,71, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (N_{деп} - N_{інф})/100), \tag{3.19}$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (13%).

Розрахункове значення коефіцієнта повернення інвестицій визначається за формулою (3.19):

$$35,86 > (18 - 13)/100 = 9,71 > 0,05.$$

Термін окупності капітальних інвестицій T_o визначається за формулою (3.20) та показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{9,71} = 0,1, \quad \text{років.} \qquad (3.20)$$

3.4 Висновок

Результатом проведеної роботи в даному розділі є обґрунтування економічної доцільності застосування методів підвищення захищеності засобів резервування даних на приватному підприємстві.

Розраховані капітальні витрати, які складають 17619,19 грн., поточні витрати на експлуатацію системи інформаційної безпеки, що становлять 240 838,17 грн. Визначена величина економічного ефекту складає 171117,08 грн. Коефіцієнт повернення інвестицій складає 9,71 та швидкість повернення - 0,1 року.

Аналіз проведених розрахунків дозоляє зробити висновок про економічну доцільність застосування засобів резервування даних на приватному підприємстві.

ВИСНОВКИ

В роботі було розглянуто питання резервного копіювання даних, та систем зберігання інформації.

Основні стандартні алгоритми резервування даних:

- повне резервування;
- інкрементальне резервування;
- диференційне резервування.

Огляд та аналіз існуючих алгоритмів дав можливість визначити переваги та недоліки кожного з них.

Були оглянуті та проаналізовані засоби зберігання інформації:

- носії інформації;
- спеціалізовані системи зберігання інформації;
- віртуальне зберігання інформації.

Отже, дослідження системи резервування підприємства повинно вказати на недоліки існуючої системи та допомогти в розробці критеріїв для впровадження нової системи резервування, яка б відповідала потребам підприємства.

Результатом проведеної роботи став вибір профілю захищеності для системи резервування даних, аналіз загроз інформації, огляд стандартних алгоритмів резервного копіювання, проведений аналіз програмних засобів резервування.

Проведено дослідження засобів резервування даних, виявлено їх недоліки.

Розроблені рекомендації до побудови системи резервування даних на підприємстві.

Створена система резервування даних підприємства, яка відповідає всім поставленим вимогам.

ПЕРЛІК ПОСИЛАНЬ

1. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

2. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.;

3. Савяк В. RAID Levels. http://www.ixbt.com/storage/raids.html. iXBT.http://www.ixbt.com/storage/raids.html, 2017.– Загол. з екрану.

4. Седых В., Мелов Г. Корпоративные СХД в примерах, или Идеи напрокат.CompDoc.http://www.compdoc.ru/peripherals/drives/corporative_ssd_in_example/, 2018. – Загол. з екрана.

5. Системы хранения данных и резервного копирования. http://network.xsp.ru/6_2.php, 2017. – Загол. з екрана.

6. Тищенко А. Новые уровни RAID: цифры, буквы и то, что за ними. Компьютерное Обозрение, №21 (589). http://www.itc.ua/node/28408, 2009. – Загол. з екрана.

7. Шпик В. Система резервного копирования – «последний бастион» защиты корпоративной информации. Connect! Мир Связи, октябрь, 2006. http://www.connect.ru/article.asp?id=7197, 2012. – Загол. з екрана.

8. Казаков В.Г., Федосин С.А. Моделирование схем резервного копирования с целью получения сравнительной оценки объема данных для хранения в репозитории. Технологии Microsoft в теории и практике программирования. Материалы конференции / Под ред. проф. Р.Г. Стронгина. – Нижний Новгород: Изд-во Нижегородского госуниверситета, 2011. – С. 151-155.

9. Мелов Г., Лось А. СХД для SMB. CITForum. http://www.citforum.ru/nets/storage/for_smb/, 2010. – Загол. з екрана.

10. Simpson D. Reader survey reveals backup-and-recovery trends. http://www.infostor.com/display_article/244384/23/ARTCL/none/none/1/Readersurvey-reveals-backup-and-recovery-trends/, 2016. – Загол. з екрана.

11. Millard E. Smaller Players In The Backup Market. Processor Vol.29 Issue 4. http://www.processor.com/editorial/article.asp?article=articles/P2904/22p04/22p04.as p&guid=28256067B91148FE8042DDC980CC9737, 2011. – Загол. з екрана.

12. Iron Mountain, Inc. Data Protection and Recovery – The Why, The How, and Who To Go To., 2012.

13. History of Enterprise Disk to Disk Backup. http://www.storagesearch.com/d2dhistory.html, 2008. – Загол. з екрана.

14. Microsoft Corporation. Description of Full, Incremental, and Differential Backups. http://support.microsoft.com/kb/136621, 2008. – Загол. з екрана.

15. Boston Computing Network. Data Loss Statistics. http://www.bostoncomputing.net/consultation/databackup/statistics/, 2013. – Загол. з екрана.

16. Google Backup and Sync: Is It Really Backup? https://spanning.com/blog/google-backup-and-sync-is-it-really-backup/, 2020 – Загол. з екрана.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	2	
5	А4	1 Розділ	26	
6	А4	2 Розділ	19	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу магістра на тему:
Дослідження ефективності методів резервування даних приватного підприємства
студентки групи 125м-19-2
Бобошко Марини Анатоліївни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерела та __ додатка.

Актуальність теми полягає в необхідності підвищення рівня захищеності інформації в ІТС комерційного підприємства при використанні систем резервного копіювання даних.

Зміст та структура роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі було розглянуто актуальність технології RAID, технології з'єднання систем зберігання даних з обчислювальними системами DAS, SAN, NAS, розглянуті переваги та недоліки алгоритмів резервного копіювання даних, виконано аналіз загроз, визначений профіль захищеності та методи його реалізації, обґрунтовані методи підвищення захищеності засобів резервування даних на комерційному підприємстві.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Бобошко Марина Анатоліївна заслуговує на оцінку «_____».

Керівник роботи,