Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Автоматизації, комп'ютерно-інтегрованих технологій та систем
(повна назва)

Кафедра Комп’ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Розроблення підсистеми резервного копіювання та аварійного відновлення даних для АСУ ТП
(тема)

Виконав:
здобувач 4 року навчання,
групи АКТАКІТ-22-1
Олександр КРЕМЗУКОВ
(власне ім’я, прізвище)

Спеціальність 151 Автоматизація та комп’ютерно-інтегровані технології
(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма Автоматизація та комп’ютерно-інтегровані технології
(повна назва освітньої програми)

Керівник доц. Оксана СИЧОВА
(посада, власне ім’я, прізвище)

Допускається до захисту

Завідувач кафедри КІТАРБІ _____ Ігор НЕВЛЮДОВ
(підпис) (власне ім’я, прізвище)

2026 р.

Я, Кремзуков Олександр Вікторович, як здобувач вищої освіти ХНУРЕ, розумію і підтримую політику закладу з академічної доброчесності. Я не надавав і не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Я не використовував штучний інтелект для підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

" 20 " червня 2026 р.  Олександр КРЕМЗУКОВ

Харківський національний університет радіоелектроніки

Факультет Автоматизації, комп'ютерно-інтегрованих технологій та систем
Кафедра Комп’ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії
Рівень вищої освіти перший (бакалаврський)
Спеціальність 151 Автоматизація та комп’ютерно-інтегровані технології
(код і повна назва)
Тип програми освітньо-професійна
Освітня програма Автоматизація та комп’ютерно-інтегровані технології
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«27» квітня 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
здобувачеві Кремзукову Олександру Вікторовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Розроблення підсистеми резервного копіювання та аварійного відновлення даних для АСУ ТП
затверджена наказом університету від 04.06.2026 р. № 472 Ст
2. Термін подання здобувачем роботи до екзаменаційної комісії 14.07.2026 р.
3. Вихідні дані до роботи 3.1 Вимоги до забезпечення надійності даних з урахуванням особливостей функціонування АСУ ТП; 3.2 Модель безпеки, політики зберігання та життєвого циклу резервних копій; 3.3 Командний інтерпретатор та скриптова мова Bash для автоматизації процесів; 3.4 Програмне забезпечення для резервного копіювання Restic та система моніторингу Zabbix; 3.5 Тестовий середовище на базі операційної системи Linux (Ubuntu) та системи управління базами даних MySQL

4. Перелік питань, що потрібно опрацювати в роботі 4.1 Аналіз АСУ ТП та вимог до надійності даних; 4.2 Дослідження методів резервного копіювання; 4.3 Аналіз загроз КІБ; 4.4 Проєктування архітектури системи; 4.5 Розробка моделі безпеки та політик зберігання; 4.6 Алгоритм моніторингу; 4.7 Обґрунтування вибору інструментів; 4.8 Тестування та оцінка відповідності RPO/RTO; 4.9 Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) Демонстраційний матеріал, представлений у форматі презентації PowerPoint (*.ppt). – 14 с.ф. А 4.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Аналіз технічного завдання	27.04.26-30.04.26	виконано
2	Проєктування підсистеми автоматизованого резервного копіювання	01.05.26-22.05.26	виконано
3	Проєктування підсистеми резервного копіювання та відновлення даних	23.05.26-19.06.26	виконано
4	Тестування та аналіз ефективності підсистеми	20.06.26-29.06.26	виконано
5	Оформлення пояснювальної записки	30.06.26-02.07.26	виконано
6	Подання роботи на нормоконтроль	03.07.26-05.07.26	виконано
7	Подання роботи на перевірку Інтернет-сервісом Unicheck	06.07.26-07.07.26	виконано
8	Подання роботи на рецензію	07.07.26-10.07.26	виконано
9	Подання роботи на підпис зав. кафедри	11.07.26-13.07.26	виконано
10	Подання кваліфікаційної роботи в ЕК	14.07.26	виконано

Дата видачі завдання 27.04.2026 р.

Здобувач _____ Олександр КРЕМЗУКОВ
(підпис) (власне ім'я, прізвище)

Керівник роботи _____ доц. Оксана СИЧОВА
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 105 с., 12 табл., 27 рис., 5 дод., 17 джерел.

АВАРІЙНЕ ВІДНОВЛЕННЯ, АВТОМАТИЗАЦІЯ, АСУ ТП, ДЕЦЕНТРАЛІЗОВАНА АРХІТЕКТУРА, ЗАХИСТ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, МОНІТОРИНГ, РЕЗЕРВНЕ КОПІЮВАННЯ.

Об’єктом дослідження є процеси резервного копіювання, зберігання та аварійного відновлення даних у критичних компонентах АСУ ТП. Предметом дослідження є методи, моделі та програмні засоби автоматизації резервного копіювання і захисту даних. Метою роботи є забезпечення надійності зберігання даних шляхом розробки підсистеми автоматизованого резервного копіювання та аварійного відновлення даних АСУ ТП.

У роботі проаналізовано сучасні підходи до резервного копіювання та аварійного відновлення, досліджено типові кіберзагрози для систем резервування й розглянуто сучасні стратегії резервування та принципи Zero Trust. Запропоновано архітектуру підсистеми резервного копіювання із застосуванням сервера-бастіону, політик зберігання резервних копій, механізмів моніторингу та контролю їх цілісності. Для реалізації використано ОС Linux Ubuntu, систему резервного копіювання Restic, систему моніторингу Zabbix, SSH-аутентифікацію та криптографічний захист даних.

Проведене тестування підтвердило працездатність розробленої підсистеми, її стійкість до несанкціонованого видалення й модифікації резервних копій та відповідність вимогам RPO і RTO. Практичне значення роботи полягає у підвищенні надійності, безпеки та ефективності процесів резервного копіювання і аварійного відновлення даних в АСУ ТП промислових підприємств.

ABSTRACT

Explanatory note: 105 p., 12 tables, 27 figures, 5 appendices, 17 sources.

DISASTER RECOVERY, AUTOMATION, ACS, DECENTRALIZED ARCHITECTURE, INFORMATION PROTECTION, CYBERSECURITY, MONITORING, BACKUP.

The object of the study is the processes of backup, storage and disaster recovery of data in critical components of the ACS TP. The subject of the study is methods, models and software tools for automating backup and data protection. The purpose of the work is to develop a subsystem of automated backup and disaster recovery of data, which provides protection of backup copies from loss, unauthorized access and modification, as well as quick recovery of information after failures or cyberattacks.

The work analyzes modern approaches to backup and disaster recovery, investigates typical cyber threats for backup systems and considers modern backup strategies and Zero Trust principles. The architecture of the backup subsystem using a bastion server, backup storage policies, monitoring mechanisms and control of their integrity is proposed. The Linux Ubuntu OS, the Restic backup system, the Zabbix monitoring system, SSH authentication and cryptographic data protection are used for implementation.

The testing confirmed the operability of the developed subsystem, its resistance to unauthorized deletion and modification of backup copies, and compliance with RPO and RTO requirements. The practical significance of the work lies in increasing the reliability, security, and efficiency of data backup and disaster recovery processes in the ACS of industrial enterprises.

ЗМІСТ

Перелік умовних скорочень 9
Вступ 10
1 Аналіз технічного завдання 12
1.1 Аналіз особливостей АСУТП та вимог до забезпечення надійності даних 12
1.2 Аналіз основних принципів та методів резервного копіювання 15
1.3 Аналіз загроз та підходів до захисту систем резервного копіювання 18
1.4 Аналіз сучасних рішень резервного копіювання 22
1.5 Постановка задачі на розробку 29
2 Проєктування підсистеми автоматизованого резервного копіювання 32
2.1 Формування вимог та розробка загальної архітектури підсистеми 32
2.2 Розробка моделі безпеки та захисту даних 34
2.3 Розробка моделі життєвого циклу резервних копій та політики зберігання 39
2.4 Розробка алгоритму моніторингу та контролю резервного копіювання 42
2.5 Обґрунтування вибору інструментів реалізації 45
2.6 Модель автоматизованої системи аварійного відновлення даних як об’єкта автоматичного керування 48
3 Проєктування підсистеми резервного копіювання та відновлення даних 59
3.1 Налаштування середовища на базі ОС Linux (Ubuntu) та конфігурація системи резервного копіювання 59
3.2 Реалізація скриптів для автоматизації процесів резервного копіювання 62
3.3 Імплементація політик зберігання та ротації резервних копій 66
3.4 Налаштування Zabbix Agent моніторингу на сервері-бастіоні 69
4 Тестування та аналіз ефективності підсистеми 71
4.1 Імітація атаки з повним доступом до виробничого сервера 71
4.2 Аналіз результатів тестування 71

4.3 Охорона праці 73
Висновки 75
Перелік джерел посилання 77
Додаток А Програмний код розробленого рішення 80
Додаток Б Скрипт, що аналізує метадані репозиторію у форматі JSON 83
Додаток В Шаблон для системи моніторингу “Restic Backup Check” 87
Додаток Г Апробація результатів кваліфікаційної роботи 91
Додаток Д Демонстраційний матеріал 104

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСУ ТП – автоматизована система управління технологічними процесами;

БД – база даних;

ІС – інформаційна система;

КІБ – кібербезпека;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СКД – система контролю доступу;

ШІ – штучний інтелект;

API – application programming interface;

DR – disaster recovery;

GFS – модель ротації резервних копій grandfather-father-son;

HMI – human-machine interface;

ICS – industrial control system;

KMS – key management system;

PLC – programmable logic controller;

RPO – recovery point objective;

RTO – recovery time objective;

SCADA – supervisory control and data acquisition;

SSH – secure shell.

ВСТУП

Сучасний розвиток інформаційних технологій та автоматизації виробництва зумовлює зростання ролі автоматизованих систем управління технологічними процесами у критично важливих галузях, таких як енергетика, транспорт і промисловість. Збої в роботі таких систем можуть призвести до значних економічних втрат або аварій, що визначає необхідність забезпечення безперервності їх функціонування та збереження даних.

Важливою складовою надійності АСУ ТП є системи резервного копіювання та аварійного відновлення даних. Дані цих систем включають конфігурації, параметри процесів і журнали подій, а їх втрата може призвести до зупинки виробництва. У сучасних умовах особливої актуальності набуває захист резервних копій від кіберзагроз, зокрема атак типу ransomware та компрометації доступу.

Сучасні підходи передбачають використання ізольованих середовищ зберігання, шифрування, незмінюваних копій та концепції Zero Trust, що підвищують стійкість систем до атак. Важливу роль також відіграє автоматизація процесів резервного копіювання та моніторингу, яка дозволяє забезпечити регулярність створення копій і контроль їх цілісності.

Ця тема є особливо актуальною в контексті сучасних кіберзагроз, зокрема в умовах війни. На відміну від класичних атак, спрямованих на викрадення інформації чи отримання викупу, сучасні загрози все частіше мають на меті цілеспрямоване шкідництво – повне знищення даних та виведення з ладу промислових об'єктів. Традиційні підходи до резервного копіювання демонструють критичну вразливість: у випадку повної компрометації виробничого сервера (отримання root-доступу) зловмисник, як правило, може знищити не тільки основні дані, але й усі пов'язані з ними резервні копії, що створює єдину точку відмови та ставить під загрозу можливість аварійного відновлення.

Метою роботи є забезпечення надійності зберігання даних шляхом розробки підсистеми автоматизованого резервного копіювання та аварійного відновлення даних АСУ ТП.

Для досягнення мети необхідно:

– проаналізувати особливості АСУ ТП та вимоги до надійності даних;

– дослідити методи резервного копіювання та загрози;

– розробити архітектуру підсистеми;

– реалізувати підсистему резервного копіювання та відновлення даних і провести тестування.

Об’єктом дослідження є процеси резервного копіювання, зберігання та аварійного відновлення даних у критичних компонентах АСУ ТП.

Предметом – методи, моделі та програмні засоби автоматизації резервного копіювання і захисту даних.

Практичне значення полягає у підвищенні надійності, безпеки та ефективності процесів резервного копіювання і аварійного відновлення даних в АСУ ТП промислових підприємств, а робота отримала апробацію у [1].

Пояснювальну записку оформлено згідно з ДСТУ 3008:2015 [2], а також з рекомендаціями з підготовки й оформлення кваліфікаційної роботи здобувачами першого (бакалаврського) рівня вищої освіти [3-5].

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Аналіз особливостей АСУТП та вимог до забезпечення надійності даних

АСУ ТП є складними багаторівневими ІС, що забезпечують моніторинг, управління та автоматизацію виробничих процесів у реальному часі. На відміну від класичних ІС, основною характеристикою АСУ ТП є їх взаємодія із фізичні процеси, що обумовлює підвищені вимоги до надійності, доступності та безпеки.

Ключовими компонентами АСУ ТП є SCADA, PLC, HMI, а також сервери обробки даних і БД. Ці компоненти утворюють ієрархічну структуру, яка визначає логіку функціонування системи та розподіл відповідальності між рівнями. На рисунку 1.1 зображено архітектуру SCADA/АСУТП відповідно до Purdue Model, яка є де-факто стандартом для побудови ICS.

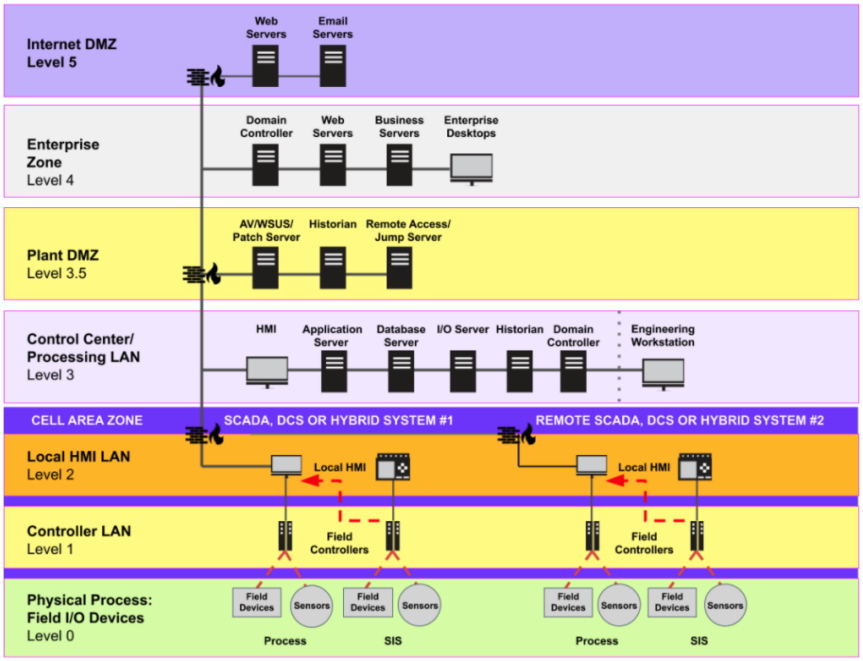


Рисунок 1.1 – Архітектура SCADA/АСУТП (Purdue Model)

Дана модель передбачає поділ системи на рівні – від фізичних процесів (рівень 0) до корпоративних ІС (рівень 4-5). Нижні рівні (0-2) включають польові

пристрої, датчики та PLC, які безпосередньо взаємодіють із технологічним процесом. Середній рівень (3) представлений SCADA, HMI, серверами додатків і БД, що забезпечують централізоване управління та обробку даних. Верхні рівні (4-5) інтегрують АСУ ТП з бізнес-ІС підприємства.

Особливу роль у структурі відіграє проміжна зона (DMZ), яка забезпечує ізоляцію між виробничим середовищем і корпоративною мережею. Саме на цьому рівні часто розміщуються сервери доступу, historian та інші компоненти, критичні для резервного копіювання і DR. На рисунку 1.2 зображено типову мережеву архітектуру SCADA-системи, яка ілюструє взаємодію між центральними серверами, локальними вузлами та польовими пристроями.

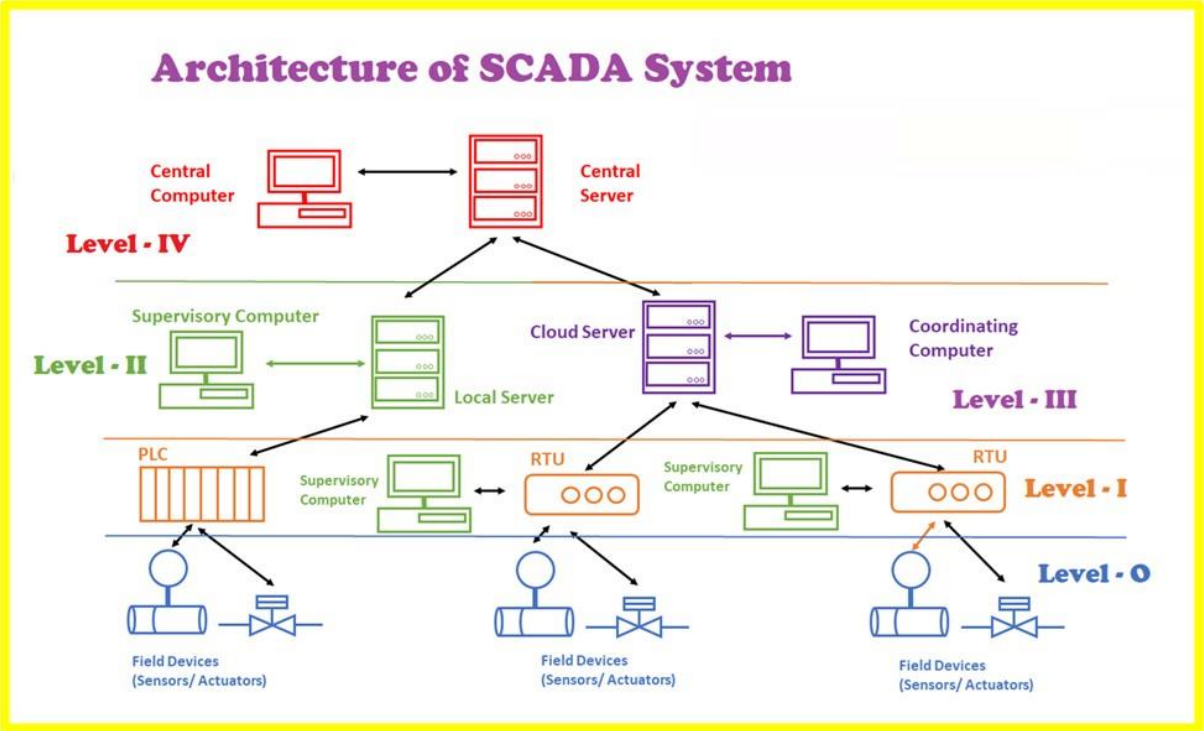


Рисунок 1.2 – Типова мережева архітектура SCADA-системи

У такій архітектурі дані передаються від сенсорів і виконавчих механізмів через PLC або RTU до SCADA-серверів, де відбувається їх обробка, зберігання в БД та відображення через HMI [6]. Важливою особливістю є розподіленість системи та наявність кількох точок збору і обробки даних.

З точки зору резервного копіювання та DR, така архітектура має ряд специфічних особливостей:

– реальний час обробки даних, адже затримки чи втрата даних можуть призвести до порушення технологічного процесу;

– використання різних типів ПЗ, протоколів і обладнання;

– обмежені ресурси нижніх рівнів (PLC та польові пристрої часто не підтримують стандартні механізми резервування);

– розподіленість системи (дані зберігаються на різних рівнях і вузлах);

– високі вимоги до доступності. Простої системи неприпустимі.

Ці особливості безпосередньо впливають на формування вимог до систем резервного копіювання.

Основні вимоги до забезпечення надійності даних в АСУ ТП можна узагальнити у вигляді таблиці 1.1.

Таблиця 1.1 – Основні вимоги до забезпечення надійності даних в АСУ ТП

Вимога	Характеристика
Доступність	Забезпечення безперервного доступу до даних і систем
Цілісність	Захист від несанкціонованої зміни або пошкодження даних
Конфіденційність	Обмеження доступу до критичних даних
RTO	Мінімальний час відновлення після збою
RPO	Мінімальні втрати даних
Стійкість до атак	Захист резервних копій від видалення або шифрування
Автоматизація	Мінімізація впливу людського фактору

Особливу увагу слід приділяти показникам RPO та RTO, які визначають ефективність системи резервного копіювання. Для критичних компонентів АСУ ТП значення RTO мають бути мінімальними, а RPO – близькими до нуля, що забезпечує практично безперервне відновлення даних.

Крім того, важливо враховувати вимоги КІБ. Сучасні загрози спрямовані не лише на основні системи, але й на резервні копії. Це вимагає впровадження

додаткових механізмів захисту, таких як ізоляція середовища резервування, використання шифрування (KMS), контроль доступу та сегментація мережі.

Таким чином, особливості архітектури АСУ ТП, їх багаторівнева структура та критичність оброблюваних даних визначають підвищені вимоги до систем резервного копіювання та DR. Ефективна реалізація таких систем повинна враховувати як технічні обмеження, так і сучасні загрози КІБ, забезпечуючи надійність, безперервність і захищеність функціонування всієї ІС.

1.2 Аналіз основних принципів та методів резервного копіювання

Резервне копіювання є базовим механізмом забезпечення надійності ІС та реалізації стратегій DR, а в контексті АСУ ТП – критично важливим елементом забезпечення безперервності технологічних процесів. На відміну від традиційних ІС, у середовищах ICS резервування повинно враховувати роботу в режимі реального часу, обмежені ресурси на рівні PLC, а також високі вимоги до доступності та цілісності даних. Це означає, що класичні підходи до резервного копіювання потребують адаптації з урахуванням специфіки промислових систем.

Основою будь-якої системи резервування є вибір методу створення копій, що безпосередньо впливає на ефективність відновлення та використання ресурсів. На рисунку 1.3 зображено порівняльну схему типів резервного копіювання (Full, Differential та Incremental), яка наочно демонструє відмінності між підходами за обсягом даних і логікою накопичення змін.

З практичної точки зору, кожен метод має свої особливості:

– повне резервне копіювання забезпечує максимальну надійність і простоту відновлення, але створює значне навантаження на систему;

– диференціальне резервне копіювання дозволяє скоротити обсяг даних, проте з часом збільшує розмір копій;

– інкрементальне резервне копіювання мінімізує обсяг переданих даних, але ускладнює процес відновлення.

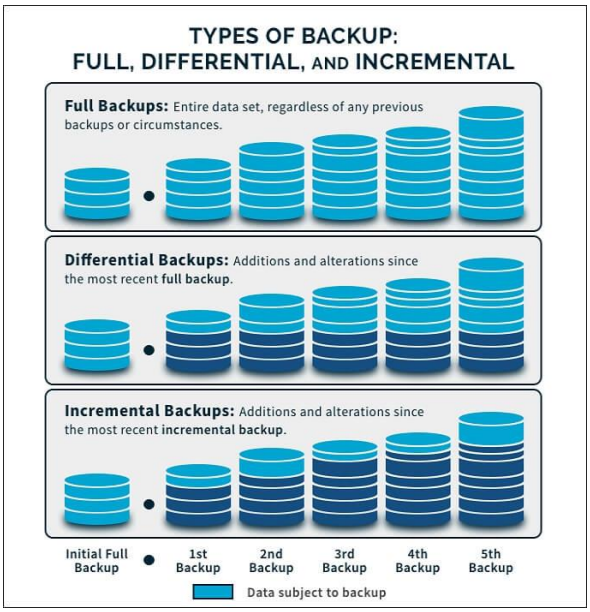


Рисунок 1.3 – Порівняльна схема типів резервного копіювання (Full, Differential та Incremental)

У промислових ІС зазвичай застосовується комбінований підхід, який дозволяє досягти балансу між продуктивністю та надійністю:

– періодичне створення повних копій;

– регулярне створення інкрементальних або диференціальних копій між ними.

Порівняльні характеристики методів резервного копіювання наведено в таблиці 1.2.

Таблиця 1.2 – Порівняння методів резервного копіювання

Метод	Переваги	Недоліки
Full	проста процедура відновлення, висока надійність	великий обсяг даних, тривалий час
Differential	компроміс між швидкістю і відновленням	збільшення обсягу копій
Incremental	мінімальний обсяг даних, швидкість	складне відновлення

Однак вибір методу резервування є лише частиною задачі. Не менш важливим є дотримання принципів побудови системи резервного копіювання,

які визначають її ефективність у реальних умовах експлуатації. До ключових принципів належать:

– регулярність створення копій, що забезпечує актуальність даних;

– надмірність зберігання, яка передбачає наявність кількох копій у різних середовищах;

– ізоляція резервного середовища від виробничої мережі;

– автоматизація процесів резервування;

– контроль цілісності даних.

У випадку АСУ ТП ці принципи доповнюються специфічними вимогами, пов’язаними з обмеженнями систем реального часу:

– мінімальний вплив на продуктивність технологічного процесу;

– відсутність простоїв під час виконання резервного копіювання;

– можливість роботи з різнорідними компонентами ICS.

Аналіз традиційних систем резервного копіювання показує, що вони мають суттєві архітектурні вразливості, які особливо критичні для АСУ ТП. Основною проблемою є централізоване управління доступом і надмірна довіра до виробничого середовища. У таких умовах компрометація одного вузла може призвести до повної втрати резервних копій. Найбільш характерними вразливостями є:

– наявність єдиної точки відмови;

– можливість видалення або модифікації резервних копій;

– відсутність механізмів захисту від ransomware-атак;

– недостатній контроль процесів резервування.

У відповідь на ці загрози сучасні системи резервного копіювання впроваджують нові підходи, орієнтовані на підвищення рівня КІБ. До них належать:

– забезпечення незмінності даних (immutability), що виключає можливість їх модифікації або видалення;

– використання append-only сховищ;

– застосування WORM-механізмів;

– шифрування даних із використанням KMS;

– сегментація доступу через СКД;

– використання захищених каналів передачі (SSH).

Важливим аспектом є також розподіл функцій між компонентами системи. У сучасних архітектурах процеси створення, зберігання та контролю резервних копій виконуються різними вузлами. Це дозволяє розірвати ланцюг атаки та підвищити загальну стійкість системи до компрометації.

Окрему роль відіграє організація життєвого циклу резервних копій. Для цього застосовуються політики зберігання, серед яких найбільш поширеною є модель GFS [7]. Вона передбачає багаторівневе зберігання копій:

– короткострокове (щоденні копії);

– середньострокове (щотижневі копії);

– довгострокове (щомісячні копії).

Такий підхід дозволяє оптимізувати використання сховища та забезпечити доступ до історичних версій даних.

Не менш важливим компонентом системи резервного копіювання є моніторинг, який забезпечує контроль її працездатності. Без належного моніторингу можливі так звані “тихі відмови”, коли резервні копії не створюються або створюються некоректно, але це не фіксується системою. Ефективна система моніторингу повинна забезпечувати:

– контроль виконання завдань резервного копіювання;

– перевірку доступності сховищ;

– виявлення аномалій;

– своєчасне сповіщення про збої.

1.3 Аналіз загроз та підходів до захисту систем резервного копіювання

Системи резервного копіювання в АСУ ТП є критичним елементом забезпечення безперервності ІС, проте саме вони дедалі частіше стають основною ціллю сучасних кібератак. Якщо раніше резервні копії розглядалися

як гарант відновлення після інцидентів, то сьогодні їх компрометація фактично означає повну втрату можливості відновлення. Це особливо небезпечно для ICS, де зупинка процесів може мати фізичні наслідки.

Основною загрозою для систем резервного копіювання є атаки типу ransomware, які еволюціонували від шифрування робочих даних до цілеспрямованого знищення або пошкодження резервних копій. На рисунку 1.4 зображено алгоритм атаки ransomware, представлений IT-компанією “Blade technologies” [8], який складається з кількох етапів: початковий доступ до системи, закріплення в мережі, поширення на інші вузли, шифрування даних та вимагання викупу.



Рисунок 1.4 – Алгоритм атаки ransomware на систему резервного копіювання

Важливою особливістю є те, що на етапі поширення зловмисник намагається отримати доступ до backup-інфраструктури, після чого видаляє або

шифрує резервні копії. Таким чином, резервна система стає не захистом, а додатковою точкою атаки.

Крім ransomware, існує ряд інших загроз, характерних для систем резервного копіювання в АСУ ТП:

– компрометація облікових записів із привілейованим доступом;

– централізоване управління, що створює єдину точку відмови;

– можливість модифікації або видалення резервних копій;

– відсутність ізоляції між виробничою та backup-інфраструктурою;

– недостатній моніторинг і контроль процесів резервування.

Особливо небезпечною є ситуація, коли агент резервного копіювання, встановлений на сервері АСУ ТП, має повний доступ до сховища. У такому випадку зловмисник, отримавши контроль над сервером, автоматично отримує контроль над резервними копіями. Це створює критичну архітектурну вразливість, яка робить традиційні підходи неприйнятними для сучасних умов.

У відповідь на ці загрози сформувалися сучасні підходи до захисту систем резервного копіювання, які базуються на принципах КІБ та відмові від моделі довіри. Центральною концепцією є Zero Trust, яка передбачає, що жоден компонент ІС не вважається довіреним за замовчуванням. На рисунку 1.5 зображено загальну структуру архітектури Zero Trust, яка демонструє принцип “never trust – always verify”. Будь-який доступ до ресурсів проходить через механізми автентифікації та перевірки контексту, після чого застосовуються політики доступу.

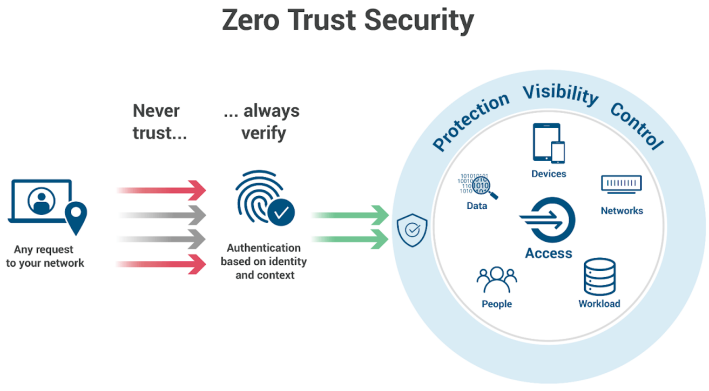


Рисунок 1.5 – Загальна структура архітектури Zero Trust

У контексті резервного копіювання це означає зміну архітектури системи таким чином, щоб навіть компрометація виробничого вузла не давала можливості знищити резервні копії. Реалізація цього підходу включає:

– розділення ролей між компонентами системи (створення, зберігання, управління);

– використання ізольованих середовищ (backup-сегмент, bastion-вузли);

– обмеження доступу до сховища резервних копій;

– використання багатофакторної автентифікації.

Одним із ключових технічних механізмів захисту є забезпечення незмінності даних. Це досягається за рахунок:

– використання WORM-сховищ;

– реалізації append-only моделей;

– застосування Object Lock у сучасних сховищах.

Такі механізми гарантують, що навіть у разі компрометації доступу зловмисник не зможе змінити або видалити вже створені резервні копії.

Додатковим рівнем захисту є криптографічна безпека. Сучасні системи резервного копіювання використовують шифрування на стороні клієнта, що дозволяє забезпечити незалежність від сховища. Це означає, що навіть у випадку повного доступу до сховища зловмисник не зможе отримати доступ до даних без ключів. Для цього застосовуються:

– симетричні алгоритми шифрування (наприклад, AES-256);

– системи управління ключами (KMS);

– контроль доступу до ключів.

Не менш важливим є питання ізоляції інфраструктури резервного копіювання. Найбільш ефективним підходом є використання логічної або фізичної ізоляції (air-gap), що передбачає відсутність прямого доступу між виробничим середовищем і сховищем резервних копій. Це значно ускладнює реалізацію атак, оскільки навіть при компрометації мережі зловмисник не має прямого доступу до backup-системи.

З урахуванням складності сучасних атак важливу роль відіграє моніторинг. Система моніторингу повинна не лише фіксувати помилки, але й аналізувати поведінку системи, виявляючи аномалії. Основні функції моніторингу:

– контроль виконання резервного копіювання;

– виявлення відхилень у графіку створення копій;

– контроль доступу до сховища;

– генерація сповіщень про підозрілу активність.

Таким чином, сучасні системи резервного копіювання в АСУ ТП повинні розглядатися як частина загальної архітектури КІБ. Ефективний захист можливий лише за умови комплексного підходу, який поєднує:

– сучасні принципи безпеки (Zero Trust);

– технічні механізми захисту (шифрування, immutability);

– архітектурні рішення (ізоляція, розподіл функцій);

– постійний моніторинг.

Такий підхід дозволяє забезпечити стійкість системи до сучасних загроз і гарантувати можливість відновлення навіть у випадку повної компрометації окремих компонентів ІС.

1.4 Аналіз сучасних рішень резервного копіювання

Сучасні системи резервного копіювання є невід’ємною частиною забезпечення надійності ІС та реалізації стратегій DR. Для АСУ ТП ці системи мають відповідати підвищеним вимогам до безпеки, доступності та незалежності від виробничого середовища. На відміну від класичних ІТ-рішень, резервування в ICS повинно враховувати обмеження продуктивності, заборону на втручання в роботу критичного ПЗ та необхідність ізоляції інфраструктури. Додатково важливим аспектом є забезпечення безперервності технологічних процесів навіть під час виконання процедур резервного копіювання. Це вимагає мінімізації впливу операцій архівації на продуктивність серверів та мережевої інфраструктури.

Ключовим елементом сучасних рішень є використання стандартизованих стратегій резервного копіювання, які визначають підхід до розміщення та зберігання даних. Базовою моделлю є стратегія 3-2-1, яка передбачає наявність трьох копій даних, використання двох різних носіїв і зберігання однієї копії поза основною системою. На рисунку 1.6 зображено стратегію резервного копіювання 3-2-1, яка ілюструє класичний підхід до побудови відмовостійкої системи. Однак для сучасних умов цього вже недостатньо, оскільки ця модель не враховує загрозу знищення резервних копій у разі компрометації мережі.

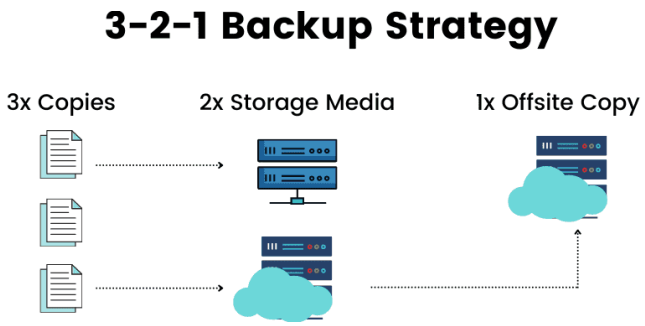


Рисунок 1.6 – Стратегія резервного копіювання 3-2-1

Розширенням класичного підходу є стратегія 3-2-1-1-0, яка враховує сучасні вимоги КІБ. Вона доповнює базову модель обов'язковою наявністю ізольованої копії та вимогою відсутності помилок у резервних копіях. На рисунку 1.7 зображено стратегію резервного копіювання 3-2-1-1-0, яка демонструє більш захищений підхід до зберігання даних. Додавання ізольованого середовища є критично важливим для АСУ ТП, оскільки дозволяє гарантувати збереження даних навіть у випадку повної компрометації мережевої інфраструктури.

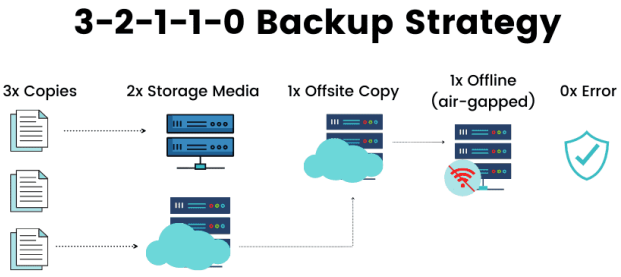


Рисунок 1.7 – Стратегія резервного копіювання 3-2-1-1-0

Для систем із максимальною критичністю застосовується стратегія 4-3-2, що передбачає більшу кількість копій та середовищ зберігання. На рисунку 1.8 зображено стратегію резервного копіювання 4-3-2, яка використовується у високонавантажених ІС з жорсткими вимогами до RPO та RTO. Такий підхід дозволяє мінімізувати ризики втрати даних, однак значно ускладнює інфраструктуру та збільшує витрати.

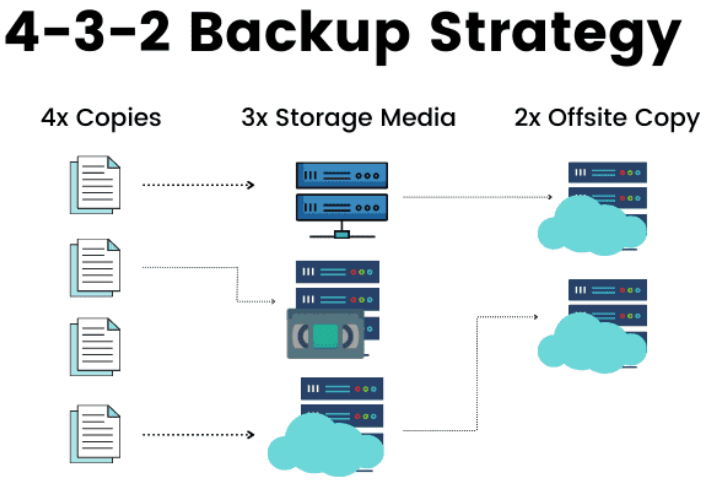


Рисунок 1.8 – Стратегія резервного копіювання 4-3-2

Порівняння стратегій резервного копіювання наведено в таблиці 1.3.

Таблиця 1.3 – Порівняння стратегій резервного копіювання

Стратегія	Кількість копій	Типи носіїв	Offsite	Ізоляція	Рівень захисту	Складність
3-2-1	3	2	1	Ні	Середній	Низька
3-2-1-1-0	3+	2+	1	Так	Високий	Середня
4-3-2	4	3	2	Частково	Дуже високий	Висока

Крім стратегій резервування, важливим є вибір конкретного ПЗ. У сучасних умовах рішення резервного копіювання поділяються на комерційні та open source. Комерційні системи забезпечують централізоване управління,

інтеграцію з корпоративними ІС та високий рівень автоматизації, але при цьому мають значні обмеження у контексті АСУ ТП. Зокрема, вони часто створюють додаткове навантаження на систему, використовують закриті механізми безпеки та потребують довіри до внутрішньої логіки роботи. Додатковим недоліком є залежність від виробника та складність адаптації таких систем до специфічних вимог промислової інфраструктури. Це може обмежувати можливості гнучкого налаштування механізмів захисту та резервування даних.

Open source рішення, навпаки, дозволяють реалізувати більш контрольовану та прозору модель безпеки. Вони забезпечують можливість шифрування на стороні клієнта, гнучке налаштування політик резервування та інтеграцію з різними типами сховищ. Проте такі рішення потребують більш глибокого розуміння архітектури системи та правильної конфігурації.

Для об’єктивної оцінки сучасних рішень резервного копіювання важливо враховувати не лише функціональність, а й архітектурну модель безпеки, рівень контролю над даними та відповідність вимогам АСУ ТП. Особливо критичним є питання – чи довіряє система виробничому середовищу, чи реалізує принцип Zero Trust. Критерії представлені в таблиці 1.4.

Таблиця 1.4 – Порівняльна характеристика підходів до резервного копіювання

Критерій	Комерційні enterprise-рішення	Open Source (класичні)	Сучасні lightweight рішення (типу Restic/Borg)
1	2	3	4
Архітектура	Централізована, server-based	Клієнт-сервер	Децентралізована, client-side
Модель безпеки	Довіра до агента	Часткова довіра	Zero Trust
Шифрування	Часто опціональне або серверне	Є, але залежить від конфігурації	Завжди client-side

Продовження таблиці 1.4

1	2	3	4
Доступ до backup	Через сервер або агент	Через сервер	Безпосередньо обмежений (ключі)
Ризик компрометації	Високий при захопленні сервера	Середній	Низький
Прозорість	Закрита (пропрієтарна)	Відкрита	Відкрита
Навантаження на АСУ ТП	Високе (агенти, сервіси)	Середнє	Мінімальне
Складність впровадження	Низька–середня	Висока	Низька
Гнучкість сховищ	Обмежена екосистемою	Середня	Висока (SFTP, S3, FTP тощо)
Підтримка ізоляції	Частково	Залежить від реалізації	Вбудована концептуально
Вартість	Висока	Низька	Низька

З точки зору експлуатації в АСУ ТП, вибір рішення повинен базуватися не лише на функціональності, але й на відповідності архітектурним вимогам безпеки. Критично важливими є такі характеристики:

– мінімальний вплив на продуктивність виробничих систем;

– підтримка шифрування даних на стороні клієнта;

– можливість роботи в ізольованих або частково ізольованих середовищах;

– підтримка сучасних стратегій резервування;

– відсутність залежності від сторонніх сервісів або компонентів.

Для АСУ ТП найбільш небезпечними є рішення, що базуються на довірі до агента або сервера. Вони створюють єдину точку компрометації, через яку можна знищити всі резервні копії. Саме тому сучасні підходи зміщуються в сторону client-side шифрування та Zero Trust архітектури.

Окрім вибору ПЗ, важливим є правильний вибір методу резервного копіювання залежно від конкретного сценарію використання. Універсального рішення не існує – метод повинен відповідати вимогам до RPO, RTO та обмеженням середовища. Рекомендації до методу резервного копіювання на основі сценарію використання представлені в таблиці 1.5.

Таблиця 1.5 – Вибір методу резервного копіювання залежно від сценарію

Сценарій використання	Рекомендований метод	Обґрунтування
Критичні компоненти АСУ ТП (SCADA, БД)	Full + Incremental	Мінімізація RPO при збереженні продуктивності
PLC / embedded системи	Full (періодично)	Обмежена підтримка інкрементальних механізмів
Historian / великі БД	Incremental	Великий обсяг даних, важлива економія трафіку
Конфігурації систем	Differential	Простота відновлення при невеликому обсязі
Резервне копіювання в ізольованому середовищі	Full	Надійність важливіша за ефективність
Системи з високими вимогами до RTO	Full	Найшвидше відновлення
Системи з обмеженим каналом передачі	Incremental	Мінімальний обсяг переданих даних
Довготривале зберігання архівів	Full + GFS	Збереження історії змін

З урахуванням наведеного аналізу можна зробити більш точний інженерний висновок: ефективна система резервного копіювання для АСУ ТП – це не просто вибір інструменту або стратегії, а комбінація трьох рівнів:

– правильної стратегії (3-2-1-1-0 або 4-3-2);

– безпечної архітектури (Zero Trust, ізоляція, шифрування);

– оптимального методу резервування під конкретне навантаження.

Такий підхід дозволяє забезпечити не лише збереження даних, але й стійкість системи до сучасних кіберзагроз та апаратних збоїв. Додатково це створює основу для масштабування підсистеми відповідно до потреб промислового підприємства та зростання обсягів даних.

Для обґрунтування доцільності розробки проведено порівняльний аналіз із типовими аналогами, серед яких класичні enterprise-рішення резервного копіювання, open-source рішення загального призначення та запропонована підсистема. Порівняння цих систем наведено в таблиці 1.6.

Таблиця 1.6 – Порівняльна характеристика підсистем та DR

Критерій	Enterprise-рішення	Open-source рішення	Запропонована підсистема
1	2	3	4
Архітектура	Централізована	Частково розподілена	Розподілена (Zero Trust)
Модель довіри	Довіра до мережі	Часткова довіра	Нульова довіра
Шифрування	Частково (серверне)	Налаштовується	Обов’язкове client-side
Захист від ransomware	Середній	Середній	Високий
Ізоляція компонентів	Обмежена	Часткова	Повна логічна ізоляція
Розмежування доступу	Обмежене	Часткове	Чітке (append-only, read-only, full)
Незалежна верифікація	Відсутня	Обмежена	Повноцінна
Моніторинг	Вбудований	Обмежений	Зовнішній незалежний

Продовження таблиці 1.6

1	2	3	4
Єдина точка відмови	Присутня	Можлива	Відсутня
Гнучкість конфігурації	Низька	Висока	Висока
Автоматизація	Висока	Середня	Висока
Масштабованість	Висока	Середня	Висока
Складність впровадження	Низька	Висока	Середня
Вартість	Висока	Низька	Низька
Відповідність RPO/RTO	Висока	Середня	Висока
Придатність для АСУ ТП	Обмежена	Часткова	Висока

Аналіз результатів показує, що запропонована підсистема не є абсолютним лідером за всіма критеріями, однак забезпечує найбільш збалансоване поєднання безпеки, гнучкості та вартості. Зокрема, вона поступається enterprise-рішенням за рівнем готових інтеграцій та простотою впровадження, але значно перевершує їх у питаннях КІБ та стійкості до атак. Постановка ж задачі полягає у створенні підсистеми резервного копіювання, яка усуває ключові недоліки існуючих рішень, забезпечує захист даних навіть у разі компрометації АСУ ТП та відповідає сучасним вимогам до безпеки та надійності ІС.

1.5 Постановка задачі на розробку

Аналіз існуючих рішень показує, що більшість підсистем резервного копіювання мають спільні недоліки – централізовану архітектуру, відсутність повноцінної ізоляції та залежність від довіреного середовища. Це робить їх

вразливими до атак, особливо у випадку компрометації виробничого серверу. У більшості випадків такі системи передбачають наявність єдиного центру керування, який одночасно відповідає за створення, зберігання та відновлення резервних копій. Подібний підхід формує єдину точку відмови, компрометація якої може призвести до втрати всієї резервної інфраструктури. Особливо небезпечними є атаки типу ransomware, які спрямовані не лише на шифрування основних даних, а й на знищення резервних копій та механізмів відновлення.

Для АСУ ТП проблема резервного копіювання є особливо критичною, оскільки від безперервності функціонування ІС залежить стабільність виробничих процесів та безпека обладнання. Втрата телеметричних даних, журналів подій або параметрів технологічного процесу може призвести до порушення роботи промислових систем, фінансових втрат та простою виробництва. Крім того, відсутність коректних резервних копій унеможливлює оперативне відновлення роботи після аварійних ситуацій або кібератак. Саме тому сучасна підсистема резервного копіювання повинна забезпечувати не лише збереження даних, а й гарантувати їх цілісність, конфіденційність і доступність навіть у випадку компрометації окремих компонентів інфраструктури.

У зв’язку з цим виникає задача розроблення підсистеми автоматизованого резервного копіювання та аварійного відновлення даних для АСУ ТП, яка забезпечує:

– захист резервних копій від несанкціонованого доступу та видалення;

– гарантовану цілісність і доступність даних;

– незалежну верифікацію стану резервних копій;

– відповідність вимогам RPO та RTO;

– стійкість до сучасних загроз КІБ, включаючи ransomware;

– автоматизацію процесів резервного копіювання та контролю.

Метою розробки є створення підсистеми резервного копіювання, яка базується на принципах Zero Trust, забезпечує розподіл повноважень між компонентами та виключає наявність єдиної точки відмови. Важливою особливістю підсистеми має стати ізоляція критичних компонентів та мінімізація

рівня довіри між окремими вузлами інфраструктури. Такий підхід дозволяє локалізувати потенційні інциденти безпеки та зменшити ризик компрометації всієї системи резервування. Крім того, підсистема повинна підтримувати можливість масштабування та адаптації до різних типів промислових середовищ і навантажень.

Для досягнення поставленої мети необхідно реалізувати такі ключові функції:

– автоматизоване створення резервних копій із шифруванням;

– організація захищеного сховища з обмеженим доступом;

– реалізація політик зберігання та ротації резервних копій;

– моніторинг стану резервних копій та перевірку їх цілісності;

– реалізацію механізмів аварійного відновлення даних;

– розмежування прав доступу між компонентами системи відповідно до принципу мінімальних привілеїв.

2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ АВТОМАТИЗОВАНОГО РЕЗЕРВНОГО КОПІЮВАННЯ

2.1 Формування вимог та розробка загальної архітектури підсистеми

Проєктування підсистеми автоматизованого резервного копіювання для АСУ ТП починається з формування чітких вимог, що враховують як технічні особливості ICS, так і сучасні загрози КІБ. На відміну від класичних ІС, у даному випадку система резервування повинна розглядатися не як допоміжний компонент, а як критична частина інфраструктури, від якої безпосередньо залежить можливість відновлення після інцидентів.

Аналіз матеріалів проєкту (зокрема опис архітектури та вибору інструментів) дозволяє сформулювати ключові вимоги до підсистеми резервного копіювання. Важливо відразу відкинути застарілі підходи, що базуються на довірі до внутрішньої мережі, оскільки вони не відповідають сучасним умовам.

До основних вимог належать:

– забезпечення стійкості до повної компрометації виробничого сервера;

– неможливість видалення або модифікації резервних копій з боку АСУ ТП;

– використання шифрування даних на стороні клієнта;

– забезпечення незалежної перевірки цілісності резервних копій;

– мінімальний вплив на продуктивність виробничих систем;

– підтримка автоматизації процесів резервного копіювання та контролю;

– можливість роботи в ізольованих або сегментованих мережах;

– контроль життєвого циклу резервних копій із розмежуванням доступу.

Окрему увагу слід приділити вимогам до безпеки, які формують основу всієї архітектури. У сучасних умовах ключовим є не просто збереження даних, а гарантія того, що вони залишаться доступними навіть у разі атаки. Це означає, що система повинна відповідати таким принципам:

– відсутність єдиної точки відмови;

– реалізація принципу мінімальних привілеїв;

– ізоляція критичних операцій (особливо видалення даних);

– розподіл функцій між різними компонентами;

– незалежність процесів створення, зберігання та перевірки копій.

Сформовані вимоги безпосередньо визначають підхід до побудови архітектури підсистеми резервного копіювання. На відміну від традиційних централізованих рішень, запропонована архітектура базується на принципах Zero Trust, згідно з якими жоден компонент ІС не вважається довіреним за замовчуванням [7].

У межах даного підходу вся система розглядається як потенційно скомпрометована, включно з виробничим сервером. Це дозволяє спроєктувати архітектуру, яка залишається стійкою навіть у найгіршому сценарії.

Загальна архітектура підсистеми включає декілька логічно розділених компонентів, кожен із яких виконує строго визначену функцію:

– виробничий сервер АСУ ТП – джерело даних, відповідальний лише за створення резервних копій;

– сховище резервних копій – централізоване середовище зберігання зашифрованих даних;

– сервер моніторингу – незалежний компонент для перевірки стану резервних копій;

– сервер-бастіон – ізольований вузол для виконання привілейованих операцій.

Такий розподіл дозволяє усунути критичну проблему традиційних систем – наявність повного контролю над резервними копіями з одного вузла.

Взаємодія між компонентами організована таким чином, щоб мінімізувати довіру між ними. Зокрема, виробничий сервер має лише обмежений доступ до сховища резервних копій. Він може створювати нові копії, але не має можливості змінювати або видаляти існуючі дані. Це реалізується через модель доступу

“тільки для дозапису”, яка є одним із ключових механізмів захисту від ransomware.

Сервер моніторингу функціонує незалежно від виробничого середовища та виконує перевірку цілісності та актуальності резервних копій. Такий підхід дозволяє уникнути ситуації, коли скомпрометована система надає недостовірну інформацію про власний стан.

Найбільш критичним компонентом архітектури є сервер-бастіон, який використовується для виконання адміністративних операцій, зокрема управління життєвим циклом резервних копій. Його ізоляція та обмежений доступ дозволяють винести найбільш небезпечні операції за межі автоматизованої частини системи. Для кращого розуміння відповідності між вимогами та архітектурними рішеннями доцільно представити їх у вигляді таблиці 2.1.

Таблиця 2.1 – Відповідність вимог до архітектурних рішень

Вимога	Архітектурне рішення
Захист від видалення копій	Append-only доступ до сховища
Незалежна верифікація	Виділений сервер моніторингу
Відсутність єдиної точки відмови	Розподіл функцій між компонентами
Захист від компрометації	Zero Trust модель
Безпечне управління	Використання серверу-бастіону
Конфіденційність даних	Client-side шифрування
Контроль доступу	Розмежування прав між компонентами

2.2 Розробка моделі безпеки та захисту даних

Модель безпеки підсистеми резервного копіювання в АСУ ТП базується на принциповій відмові від традиційної периметрової моделі захисту та переході до концепції Zero Trust. Такий підхід передбачає, що жоден компонент ІС, включно з виробничими серверами, не вважається довіреним за замовчуванням. Це є

критично важливим, оскільки сучасні атаки спрямовані не лише на доступ до даних, але й на їх знищення або компрометацію резервних копій .

Для розуміння необхідності такого підходу доцільно розглянути класичну модель доступу до ресурсів. На рисунку 2.1 зображено стандартну схему доступу до файлів компанії, у якій користувач або адміністратор має прямий доступ до серверів, БД та сервісів [9]. Така модель є зручною, але створює критичну вразливість – компрометація облікового запису або вузла відкриває прямий доступ до всіх ресурсів, включаючи резервні копії.

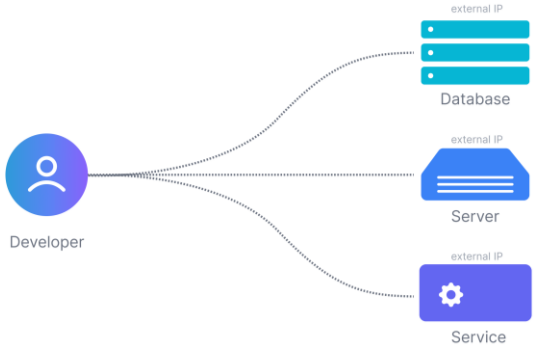


Рисунок 2.1 – Стандартна схема доступу до файлів компанії

На відміну від цього, у запропонованій моделі використовується ізольований доступ через проміжний вузол. На рисунку 2.2 зображено схему доступу через сервер-бастіон, який виступає єдиною контрольованою точкою входу до критичних ресурсів. У цьому випадку прямий доступ до серверів та БД відсутній, а всі дії проходять через додатковий рівень контролю. Це дозволяє суттєво зменшити площу атаки та ускладнити несанкціонований доступ.

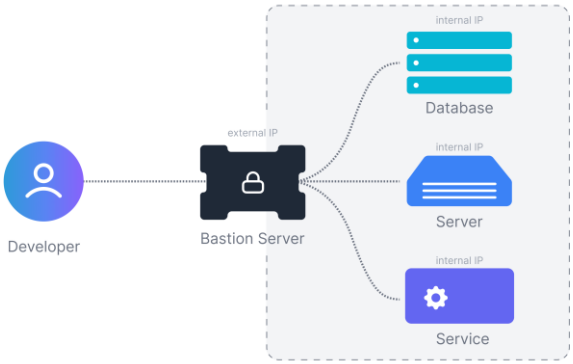


Рисунок 2.2 – Схема доступу до файлів через сервер-бастіон

Центральним елементом моделі безпеки є розподілена архітектура підсистеми резервного копіювання, побудована за принципами сегрегації повноважень. На рисунку 2.3 зображено загальну схему взаємодії між компонентами системи резервного копіювання за принципами нульової довіри.



Рисунок 2.3 – Загальна схема взаємодії між компонентами системи резервного копіювання за принципами нульової довіри

Відповідно до цієї моделі:

– виробничий сервер АСУ ТП відповідає лише за створення резервних копій;

– сховище резервних копій забезпечує їх збереження;

– сервер моніторингу виконує незалежну перевірку стану даних;

– сервер-бастіон використовується для виконання привілейованих операцій.

Особлива увага приділяється контролю доступу до сховища резервних копій. У системі реалізовано розмежування прав доступу відповідно до ролей компонентів. Виробничий сервер використовує модель доступу “тільки для дозапису” (append-only), що означає можливість лише додавання нових даних без права їх зміни або видалення. Сервер моніторингу працює в режимі “тільки для читання”, що забезпечує незалежну верифікацію стану резервних копій без ризику їх пошкодження. Повні права доступу (включаючи видалення) має лише

сервер-бастіон, що відповідає принципу мінімальних привілеїв. З метою формалізації розмежування доступу доцільно представити відповідну модель у вигляді таблиці 2.2.

Таблиця 2.2 – Розмежування прав доступу в системі резервного копіювання

Компонент	Доступ до сховища	Операції
Сервер АСУ ТП	Append-only	Створення резервних копій
Сервер моніторингу	Read-only	Перевірка цілісності та стану
Сервер-бастіон	Full access	Видалення, управління копіями

Критичним елементом моделі безпеки є забезпечення конфіденційності даних. У підсистемі реалізовано шифрування на стороні клієнта, що гарантує захист інформації незалежно від стану сховища. На рисунку 2.4 зображено схему шифрування даних та управління ключами, де показано, що дані шифруються ще до передачі в сховище, а ключі зберігаються окремо від самих резервних копій. Це означає, що навіть при повному доступі до сховища зловмисник не зможе отримати доступ до інформації без ключів шифрування.

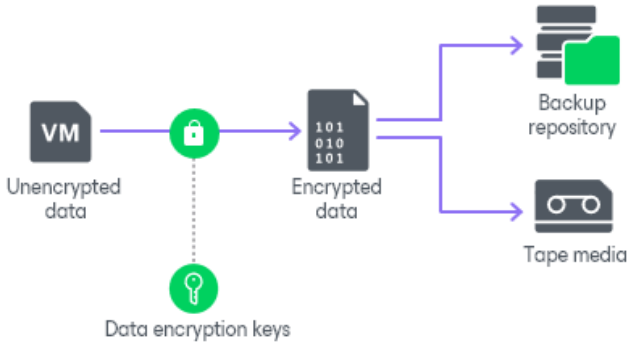


Рисунок 2.4 – Схема шифрування даних та управління ключами

Не менш важливим є захист процесу автентифікації. Доступ до серверу-бастіону реалізовано з використанням багатофакторної автентифікації на основі

апаратних ключів. На рисунку 2.5 зображено процес аутентифікації SSH із застосуванням YubiKey, який передбачає використання криптографічного ключа, що фізично зберігається на пристрої користувача. Навіть у випадку компрометації облікових даних доступ до системи залишається неможливим без фізичного доступу до пристрою.

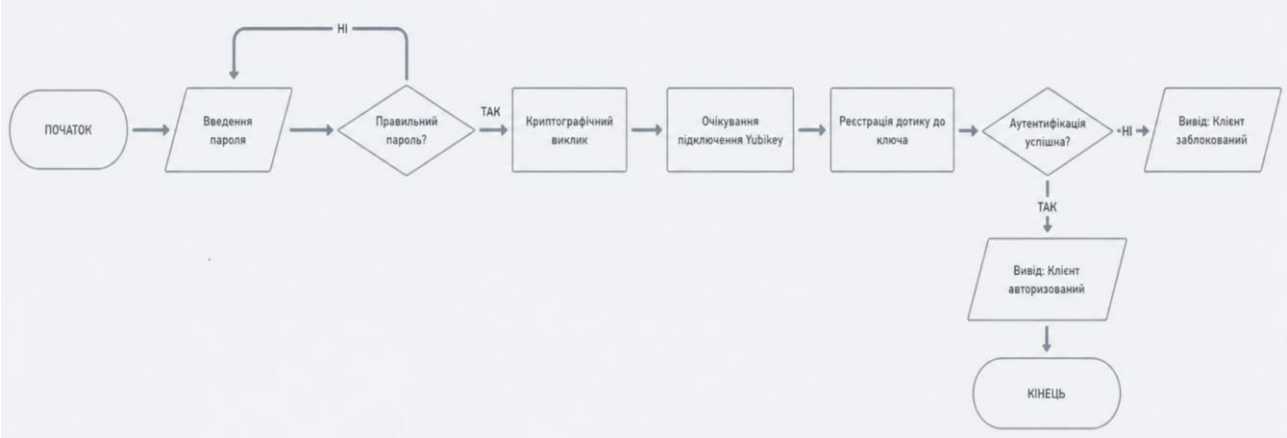


Рисунок 2.5 – Процес аутентифікації SSH із застосуванням апаратного ключа YubiKey

Окремо варто відзначити роль ізоляції в загальній моделі безпеки. Сервер-бастіон розміщується в окремому сегменті мережі та не має прямих зв’язків із виробничими серверами. Це унеможливлює горизонтальне переміщення зловмисника в мережі навіть у випадку компрометації АСУ ТП. Такий підхід є одним із ключових елементів архітектури Zero Trust і забезпечує додатковий рівень захисту критичних операцій.

Ключовим аспектом безпеки є те, що жоден із компонентів не має повного контролю над системою. Це виключає можливість одночасної компрометації всіх резервних копій навіть у разі успішної атаки на один із вузлів.

З урахуванням викладеного, модель безпеки підсистеми резервного копіювання базується на поєднанні трьох фундаментальних принципів:

– розподіл повноважень між компонентами системи;

– ізоляція критичних процесів і ресурсів;

– криптографічний захист даних.

Реалізація цих принципів дозволяє створити систему, стійку до сучасних кібератак, включаючи сценарії повної компрометації виробничого середовища. Така модель гарантує не лише збереження резервних копій, але й їх доступність для відновлення, що є ключовою вимогою для АСУ ТП.

2.3 Розробка моделі життєвого циклу резервних копій та політики зберігання

Ефективність підсистеми резервного копіювання визначається не лише механізмами створення копій, але й правильно організованим життєвим циклом їх існування. У сучасних умовах АСУ ТП критично важливо забезпечити не тільки збереження даних, але й їх актуальність, цілісність та керованість протягом усього періоду використання. Неправильно спроєктований життєвий цикл може призвести до накопичення застарілих даних, перевантаження сховища або втрати критично важливої інформації.

На рисунку 2.6 зображено життєвий цикл резервної копії, який включає основні етапи: створення, зберігання, використання, архівація та видалення. Дана модель є узагальненою, однак у контексті АСУ ТП вона потребує адаптації з урахуванням вимог до КІБ та безперервності технологічних процесів.

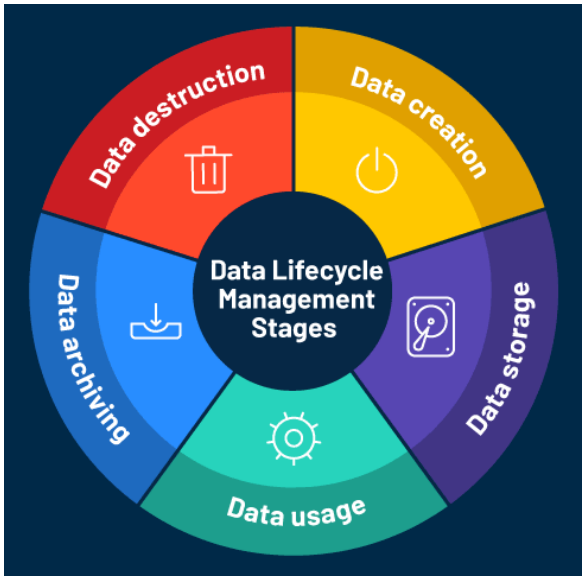


Рисунок 2.6 – Життєвий цикл резервної копії

На етапі створення резервної копії виробничий сервер АСУ ТП формує зашифрований знімок даних за допомогою клієнтського ПЗ. При цьому шифрування виконується до передачі даних у сховище, що гарантує їх захист навіть у разі компрометації каналів зв’язку або самого сховища. Важливою особливістю є використання моделі append-only, яка унеможливлює зміну вже створених копій.

Після створення резервна копія переходить до етапу зберігання. На цьому етапі дані розміщуються у централізованому сховищі, яке виступає пасивним компонентом і не виконує жодних операцій обробки. Це дозволяє мінімізувати ризики пошкодження даних. У контексті АСУ ТП до сховища висуваються підвищені вимоги:

– забезпечення відмовостійкості та доступності;

– підтримка контролю доступу на рівні ролей;

– захист від несанкціонованого видалення;

– масштабованість для довгострокового зберігання.

Наступним етапом є використання резервних копій, яке включає як процес відновлення даних, так і їх перевірку. У запропонованій моделі використовується підхід незалежної верифікації, реалізований через сервер моніторингу. Зокрема, система регулярно виконує перевірку цілісності резервних копій та їх актуальності. Це дозволяє виявити пошкодження або пропущені сеанси резервного копіювання ще до виникнення аварійної ситуації.

З часом частина резервних копій втрачає актуальність і переходить до етапу архівації або видалення. На цьому етапі ключову роль відіграє політика зберігання, яка визначає, які копії повинні бути збережені, а які – видалені. Важливо підкреслити, що видалення є найбільш критичною операцією, тому воно виконується виключно через сервер-бастіон із використанням захищеного механізму доступу. Для формалізації життєвого циклу доцільно представити його основні етапи у вигляді таблиці 2.3.

Таблиця 2.3 – Етапи життєвого циклу резервної копії

Етап	Опис	Відповідальний компонент
1	2	3
Створення	Формування зашифрованої копії	Сервер АСУ ТП
Зберігання	Розміщення у сховищі	Сховище резервних копій
Перевірка	Контроль цілісності та актуальності	Сервер моніторингу
Використання	Відновлення даних при необхідності	Адміністратор
Видалення	Очищення застарілих копій	Сервер-бастіон

Політика зберігання є невід'ємною частиною життєвого циклу та визначає правила управління резервними копіями. У сучасних системах резервного копіювання найбільш поширеною є модель GFS (grandfather-father-son) [10], яка дозволяє поєднати короткострокове та довгострокове зберігання даних.

Суть підходу полягає у збереженні копій із різною періодичністю:

– щоденні копії (son) – для оперативного відновлення;

– щотижневі копії (father) – для аналізу змін;

– щомісячні копії (grandfather) – для довгострокового зберігання.

Однак у контексті АСУ ТП класична модель GFS потребує адаптації. Зокрема, необхідно враховувати вимоги до RPO та RTO, а також обмеження обчислювальних ресурсів. Надмірна кількість копій може призвести до перевантаження БД, тоді як їх недостатня кількість – до втрати критичних даних. Додатково необхідно враховувати інтенсивність змін технологічних параметрів та обсяг телеметричної інформації, що накопичується в системі. Це дозволяє забезпечити баланс між ефективністю зберігання даних і швидкістю їх відновлення у разі аварійної ситуації.

З урахуванням цих факторів доцільно використовувати комбіновану політику зберігання, яка враховує як частоту змін даних, так і критичність системи. Приклад такої політики наведено у таблиці 2.4.

Таблиця 2.4 – Приклад політики зберігання резервних копій

Тип копії	Періодичність	Термін зберігання	Призначення
Інкрементальна	Кожні 6 годин	7 днів	Оперативне відновлення
Щоденна	1 раз на добу	30 днів	Короткостроковий аналіз
Щотижнева	1 раз на тиждень	3 місяці	Середньострокове зберігання
Щомісячна	1 раз на місяць	1 рік	Довгострокове зберігання

Важливою особливістю реалізації політики зберігання є її автоматизація. У запропонованій системі керування життєвим циклом здійснюється автоматично за допомогою планувальника завдань. Видалення застарілих копій виконується відповідно до заданих правил без необхідності ручного втручання, що дозволяє мінімізувати людський фактор та підвищити надійність системи.

2.4 Розробка алгоритму моніторингу та контролю резервного копіювання

У сучасних АСУ ТП наявність резервних копій сама по собі не гарантує можливість відновлення даних. Ключовим фактором є постійний контроль їх стану, цілісності та актуальності. Відсутність ефективного моніторингу призводить до так званих «тихих відмов», коли резервні копії формально існують, але є пошкодженими, застарілими або непридатними для відновлення. Саме тому алгоритм моніторингу та контролю резервного копіювання є невід’ємною частиною загальної архітектури системи.

У запропонованій підсистемі моніторинг реалізовано як незалежний процес, що не залежить від стану виробничого середовища. Відповідно до концепції Zero Trust, перевірка резервних копій не може виконуватись самим сервером АСУ ТП, оскільки він розглядається як потенційно скомпрометований. Для цього використовується окремий сервер моніторингу, який виконує роль довіреного компонента.

Алгоритм моніторингу базується на періодичному виконанні перевірок стану резервних копій у сховищі. Його основна мета – своєчасне виявлення відхилень від нормального функціонування системи та оперативне інформування відповідальних осіб.

Загальна логіка алгоритму включає декілька послідовних етапів.

На першому етапі виконується ініціалізація перевірки. Сервер моніторингу встановлює з’єднання зі сховищем резервних копій, використовуючи обліковий запис із правами тільки для читання. Такий підхід виключає можливість випадкового або навмисного пошкодження даних у процесі моніторингу.

Далі виконується перевірка цілісності резервних копій. Для цього використовується механізм аналізу структури репозиторію, який дозволяє виявити пошкоджені або відсутні блоки даних. Цей етап є критично важливим, оскільки навіть незначне пошкодження може зробити неможливим повне відновлення системи.

Наступним кроком є перевірка актуальності резервних копій. Система аналізує час створення останнього знімка та порівнює його з заданими політиками резервного копіювання. У разі перевищення допустимого інтервалу система фіксує інцидент, що може свідчити про збій у процесі резервного копіювання або про втручання зловмисника.

Окрему увагу приділено контролю обсягу даних. Різке зростання розміру резервної копії може бути індикатором аномальної активності, зокрема шифрування файлів у результаті атаки ransomware. Аналогічно, різке зменшення обсягу може свідчити про втрату частини даних. Для систематизації основних параметрів моніторингу доцільно представити їх у вигляді таблиці 2.5.

Таблиця 2.5 – Основні параметри моніторингу резервного копіювання

Параметр	Опис	Можливі загрози
Цілісність даних	Перевірка структури та блоків даних	Пошкодження, часткова втрата
Актуальність	Час створення останньої копії	Збій резервного копіювання
Обсяг даних	Аналіз розміру копій	Атаки ransomware
Доступність	Можливість доступу до сховища	Відмова інфраструктури

Після виконання перевірок система переходить до етапу аналізу результатів. У разі відсутності відхилень фіксується успішний стан системи. Якщо ж виявлено аномалії, формується подія, яка передається до системи моніторингу для подальшої обробки.

Важливою складовою алгоритму є механізм сповіщень. У разі виникнення критичних подій система автоматично надсилає повідомлення адміністраторам через заздалегідь налаштовані канали зв’язку. Це дозволяє оперативно реагувати на інциденти та мінімізувати можливі наслідки.

Узагальнений алгоритм роботи системи моніторингу можна описати наступним чином:

– підключення до сховища резервних копій у режимі read-only;

– виконання перевірки цілісності даних;

– аналіз актуальності резервних копій;

– оцінка змін обсягу даних;

– формування результатів перевірки;

– генерація сповіщень у разі виявлення відхилень.

Особливістю реалізації є повна автоматизація процесу моніторингу. Перевірки виконуються за розкладом без участі адміністратора, що дозволяє забезпечити постійний контроль стану системи. При цьому результати

моніторингу зберігаються у вигляді історичних даних, що дає можливість аналізувати тенденції та прогнозувати можливі проблеми.

З точки зору безпеки, важливим є те, що система моніторингу не має прав на зміну даних. Це виключає ризик того, що зловмисник зможе використати механізм моніторингу для атаки на резервні копії. Такий підхід відповідає принципу мінімальних привілеїв та підвищує загальну стійкість системи.

2.5 Обґрунтування вибору інструментів реалізації

Проєктування підсистеми резервного копіювання для АСУ ТП вимагає не лише формального виконання функцій збереження даних, але й гарантування їх цілісності, доступності та захищеності в умовах сучасних кіберзагроз. Неправильний вибір інструментів може призвести до ситуації, коли резервні копії існують, але не можуть бути використані для відновлення. Саме тому вибір технологічного стеку має базуватись на чітко визначених вимогах до безпеки, надійності та керованості.

Ключовими критеріями вибору інструментів є:

– забезпечення наскрізного шифрування даних;

– підтримка моделі доступу з мінімальними привілеями;

– стійкість до атак типу ransomware;

– можливість незалежної верифікації резервних копій;

– автоматизація процесів резервного копіювання та моніторингу;

– гнучкість інтеграції в існуючу ІС.

На основі зазначених вимог для реалізації підсистеми було обрано два ключових інструменти – Restic для резервного копіювання та Zabbix для моніторингу. Такий підхід дозволяє розділити критично важливі функції створення та контролю резервних копій, що відповідає принципам Zero Trust.

Restic є сучасним інструментом резервного копіювання, який забезпечує високий рівень захисту даних завдяки вбудованим механізмам шифрування. Однією з ключових переваг є реалізація end-to-end шифрування, при якому дані

шифруються на стороні джерела ще до передачі в сховище. Це означає, що навіть у разі компрометації сховища резервних копій зловмисник не зможе отримати доступ до вмісту даних без ключа шифрування. Важливим аспектом є підтримка режиму append-only, що дозволяє організувати доступ до сховища таким чином, що клієнт має право лише на додавання нових даних. Це критично для захисту від знищення резервних копій у разі компрометації АСУ ТП. Навіть отримавши повний контроль над виробничим сервером, зловмисник не зможе видалити вже створені резервні копії.

Окрім цього, Restic підтримує різні типи сховищ, що дозволяє реалізувати гнучку архітектуру:

– локальні файлові системи;

– мережеві протоколи (SFTP);

– об’єктні сховища (S3-сумісні рішення).

Разом з тим, використання лише інструменту резервного копіювання не забезпечує повної надійності системи. Ключовим ризиком залишаються «тихі відмови», коли процес резервного копіювання формально виконується, але результати є некоректними. Для вирішення цієї проблеми використовується система моніторингу Zabbix.

Zabbix забезпечує незалежну верифікацію стану резервних копій, що є фундаментальним принципом безпеки. На відміну від традиційного підходу, де перевірка виконується на тому ж сервері, що і резервне копіювання, у запропонованій архітектурі моніторинг винесено в окремий довірений контур.

Основні можливості Zabbix включають:

– перевірку цілісності резервних копій шляхом виконання команд перевірки;

– контроль актуальності даних та виявлення пропущених копій;

– моніторинг використання ресурсів сховища;

– виявлення аномалій, зокрема різкого зростання обсягу даних;

– систему сповіщень про критичні події.

На рисунку 2.7 зображено архітектуру Zabbix, яка базується на взаємодії серверу, агентів та проксі.

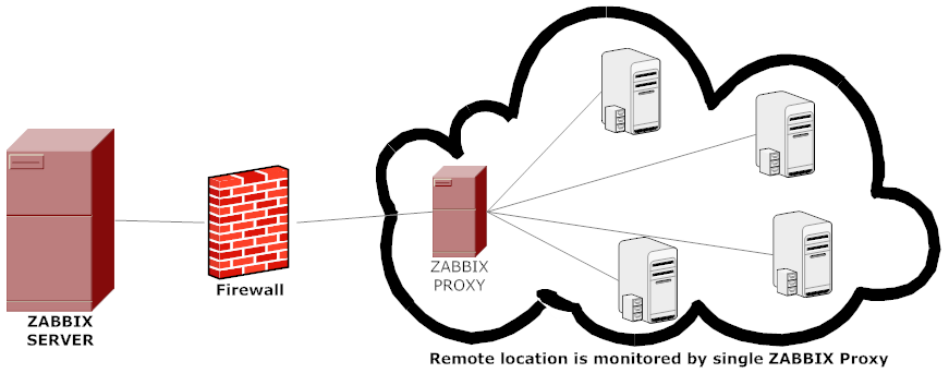


Рисунок 2.7 – Архітектура Zabbix (server–agent)

Центральний сервер відповідає за обробку даних та зберігання інформації, тоді як агенти встановлюються на контрольованих вузлах і передають метрики. У розподілених середовищах використовується Zabbix Proxy, який дозволяє агрегувати дані з віддалених сегментів мережі та передавати їх до центрального сервера через захищений канал. Такий підхід особливо актуальний для АСУ ТП, де мережі часто ізольовані та мають обмежену пропускну здатність. З метою більш наочного порівняння обраних інструментів доцільно представити їх характеристики у вигляді таблиці 2.6.

Таблиця 2.6 – Порівняння інструментів резервного копіювання та моніторингу

Критерій	Restic	Zabbix
Основне призначення	Резервне копіювання	Моніторинг
Шифрування даних	Так (end-to-end)	Ні
Захист від ransomware	Високий (append-only)	Опосередкований
Контроль цілісності	Так	Так (через перевірки)
Автоматизація	Висока	Висока
Незалежна верифікація	Ні	Так
Масштабованість	Висока	Висока

Окремо слід підкреслити, що ці інструменти не конкурують між собою, а доповнюють один одного. Restic відповідає за безпечне створення резервних копій, тоді як Zabbix забезпечує контроль їхнього стану. Така комбінація дозволяє реалізувати багаторівневу систему захисту.

Важливим є також врахування альтернативних рішень. Наприклад, існують комерційні системи резервного копіювання, які поєднують функції створення та моніторингу в одному продукті. Однак такий підхід створює єдину точку відмови та суперечить принципам Zero Trust. Використання окремих інструментів дозволяє уникнути цієї проблеми та підвищити загальну стійкість системи. Вибір Restic та Zabbix є обґрунтованим з точки зору безпеки, функціональності та відповідності сучасним вимогам до ІС. Їх поєднання дозволяє реалізувати архітектуру, в якій процеси резервного копіювання, контролю та управління даними ізольовані між собою, що забезпечує високий рівень захисту та надійності АСУ ТП.

2.6 Модель автоматизованої системи аварійного відновлення даних як об’єкта автоматичного керування

Автоматизовану підсистему аварійного відновлення даних для АСУ ТП доцільно розглядати як замкнену систему автоматичного керування з від’ємним зворотним зв’язком. Об’єктом керування є процес відновлення працездатності інформаційної системи після збою, кібератаки або втрати даних. Структурна схема автоматизованої системи аварійного відновлення даних як об’єкта автоматичного керування представлена на рисунку 2.8.

Опишемо призначення кожного блоку та параметру на розроблений структурної схеми автоматизованої системи аварійного відновлення даних як об’єкта автоматичного керування.

Вхідний вплив $(r(t))$ – задає цільовий рівень відновлення сервісів після аварії або кібератаки та визначає бажаний стан АСУ ТП, якого повинна досягти підсистема аварійного відновлення. У контексті поставленої задачі цей сигнал

формує вимоги до якості відновлення та виступає еталоном для оцінювання ефективності роботи DR-системи.

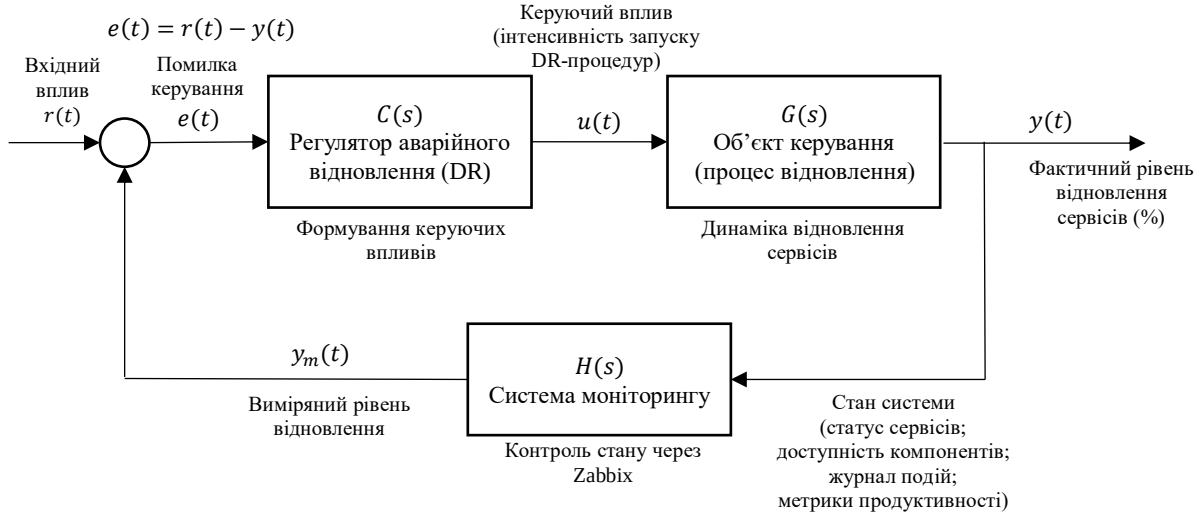


Рисунок 2.8 – Структурна схема автоматизованої системи аварійного відновлення даних як об'єкта автоматичного керування

Помилка керування ($e(t)$) – характеризує різницю між бажаним та фактичним рівнем відновлення сервісів і відображає поточний ступінь невідповідності системи встановленим вимогам. Саме ця величина використовується для формування коригувальних дій, спрямованих на скорочення часу відновлення та досягнення необхідних показників доступності.

Суматор – виконує порівняння заданого та фактичного стану системи, визначаючи величину похибки керування. Його призначення полягає у формуванні інформаційної основи для прийняття рішень щодо інтенсивності та порядку запуску процедур аварійного відновлення.

Регулятор аварійного відновлення ($C(s)$) – аналізує величину похибки та формує керуючий вплив, який визначає інтенсивність виконання процедур DR. З точки зору розв'язуваної задачі цей блок забезпечує адаптацію процесу відновлення до поточного стану АСУ ТП та дозволяє мінімізувати показники RTO і RPO.

Керуючий вплив ($u(t)$) – являє собою сукупність команд і сценаріїв, що запускають процеси відновлення критичних компонентів інформаційної інфраструктури. Величина цього сигналу визначає швидкість та масштаб виконання операцій відновлення даних і сервісів.

Об’єкт керування ($G(s)$) – описує реальний процес аварійного відновлення даних та сервісів АСУ ТП після виникнення відмови. У межах моделі цей блок відображає динаміку відновлення баз даних, конфігурацій SCADA/HMI, журналів подій, резервних копій та інших критичних ресурсів системи.

Динаміка відновлення сервісів – характеризує зміну рівня працездатності АСУ ТП у часі під впливом процедур аварійного відновлення. Вона відображає швидкість повернення системи до штатного режиму функціонування після збою або кібератаки.

Вихід системи ($y(t)$) – представляє фактичний рівень відновлення сервісів у поточний момент часу та є основним показником ефективності функціонування підсистеми DR. Значення цього параметра використовується для оцінювання ступеня досягнення поставленої мети та контролю виконання вимог до доступності системи.

Система моніторингу ($H(s)$) – забезпечує безперервний контроль стану компонентів АСУ ТП та формує інформацію про фактичний рівень їх працездатності. У запропонованій архітектурі цей блок реалізується засобами Zabbix і виконує функції збору метрик, контролю доступності сервісів та виявлення відмов.

Стан системи – являє собою набір діагностичних параметрів, що включають статус сервісів, доступність компонентів, журнали подій та показники продуктивності. Ця інформація використовується для оцінювання поточного рівня працездатності та прийняття рішень щодо подальших дій з відновлення.

Виміряний рівень відновлення ($y_m(t)$) – відображає оцінене системою моніторингу значення фактичного рівня відновлення сервісів та використовується як сигнал зворотного зв’язку. Його призначення полягає у

забезпеченні адаптивного керування процесом відновлення відповідно до реального стану АСУ ТП.

Зворотний зв’язок забезпечує передачу інформації про результати виконання процедур аварійного відновлення до контуру керування. Наявність зворотного зв’язку дозволяє автоматично коригувати інтенсивність DR-процедур та підтримувати стійке функціонування системи навіть за наявності зовнішніх збурень і непередбачених відмов.

Представимо розроблену структурну схема автоматизованої системи аварійного відновлення даних (рис. 2.8) у вигляді моделей на базі передаточних функцій теорій автоматичного керування.

Процес аварійного відновлення даних можна представить наступним чином:

$$W_z(s) = \frac{W_o(s)}{1+W_o(s)}, \quad (2.1)$$

де $W_z(s)$ – передаточна функція замкненої системи аварійного відновлення;

$W_o(s)$ – передаточна функція розімкненої системи.

Модель регулятора аварійного відновлення представимо наступним чином:

$$C(s) = K_p + \frac{K_i}{s}, \quad (2.2)$$

де $C(s)$ – передаточна функція ПІ-регулятора;

K_p – коефіцієнт пропорційного регулювання;

K_i – коефіцієнт інтегрального регулювання.

Процес відновлення даних в АСУ ТП представляється аперіодичною ланкою першого порядку:

$$G(s) = \frac{K}{Ts+1}, \quad (2.3)$$

де $G(s)$ – передаточна функція процесу аварійного відновлення;

K – коефіцієнт ефективності відновлення;

T – стала часу відновлення.

Модель розімкненої системи представимо у вигляді передаточної функції розімкненого контуру визначається як:

$$W_o(s) = C(s) \cdot G(s), \tag{2.4}$$

після підстановки

$$W_o(s) = \frac{K(K_p s + K_i)}{s(Ts+1)}, \tag{2.5}$$

де K – коефіцієнт ефективності відновлення;

K_p – пропорційний коефіцієнт регулятора;

K_i – інтегральний коефіцієнт регулятора.

Похибка відновлення (похибки керування) визначається як:

$$e(t) = r(t) - y(t), \tag{2.6}$$

де $e(t)$ – похибка системи керування;

$r(t)$ – заданий рівень відновлення;

$y(t)$ – фактичний рівень відновлення.

Модель замкненої системи, описує замикання контуру керування:

$$W_z(s) = \frac{K(K_p s + K_i)}{Ts^2 + (1 + KK_p)s + KK_i}, \tag{2.7}$$

де $W_z(s)$ – передаточна функція замкненої системи;

K – коефіцієнт ефективності відновлення;

K_p – коефіцієнт пропорційного регулювання;

K_i – коефіцієнт інтегрального регулювання;

T – стала часу відновлення.

Для аналізу стійкості використовується характеристичне рівняння:

$$D(s) = Ts^2 + \left(1 + KK_p\right)s + KK_i, \tag{2.8}$$

де $D(s)$ – характеристичний поліном системи;

T – стала часу відновлення;

K – коефіцієнт ефективності відновлення;

K_p – коефіцієнт пропорційного регулювання;

K_i – коефіцієнт інтегрального регулювання.

Перевірка стійкості за критерієм Гурвіца, не обхідно щоб система другого порядку виконувала наступні умови:

$$\begin{gathered} a_2 = T > 0\ , \\ a_1 = 1 + KK_p > 0\ , \\ a_0 = KK_i > 0\ , \end{gathered} \tag{2.9}$$

де a_2 – коефіцієнт при s^2;

a_1 – коефіцієнт при s;

a_0 – вільний член характеристичного рівняння.

При виконанні умов:

$$T > 0, K > 0,\ \ K_p > 0, K_i > 0. \tag{2.10}$$

Будемо вважати, що система аварійного відновлення є асимптотично стійкою. Опишемо вхідні та вихідні параметри системи:

– вхідний вектор системи:

$$X = \begin{bmatrix} PRO \\ RTO \\ L_s \\ N_f \end{bmatrix}, \quad (2.11)$$

де PRO – допустима втрата даних;

RTO – допустимий час відновлення;

L_s – завантаження сервера;

N_f – кількість відмов сервісів;

– вихідний вектор системи:

$$Y = \begin{bmatrix} P_r \\ T_r \end{bmatrix}, \quad (2.12)$$

де P_r – відсоток відновлених сервісів;

T_r – фактичний час відновлення системи.

Запропоновані математичні моделі дозволяють формалізувати процес аварійного відновлення даних у вигляді замкненої системи автоматичного керування, що забезпечує можливість кількісного оцінювання динаміки відновлення сервісів, аналізу впливу параметрів регулятора на швидкодію системи та прогнозування її поведінки після виникнення відмов. Використання передаточних функцій і методів теорії автоматичного керування надає можливість виконувати перевірку стійкості системи за критеріями Гурвіца та Найквіста, визначати час перехідного процесу, оцінювати якість відновлення та обґрунтовувати вибір параметрів підсистеми аварійного відновлення. У результаті це забезпечує підвищення надійності функціонування АСУ ТП, зменшення часу відновлення після аварійних ситуацій та мінімізацію ризику втрати критично важливих даних.

Для реалізації програми моделювання процесу відновлення працездатності інформаційної системи після збою, кібератаки або втрати даних обрано мову програмування Python, оскільки вона поєднує простоту розроблення, високу швидкість створення програмного забезпечення та широкі можливості для

математичного моделювання складних динамічних систем. Python має розвинену екосистему наукових бібліотек, зокрема NumPy для виконання чисельних розрахунків, SciPy для моделювання систем автоматичного керування та Matplotlib для побудови графіків перехідних процесів, годографів Найквіста і частотних характеристик. Додатковою перевагою є платформонезалежність, відкритість програмного коду, наявність великої кількості готових інструментів для роботи з мережевими сервісами, базами даних та системами моніторингу, що дозволяє не лише виконувати моделювання, а й надалі інтегрувати розроблену модель із реальними компонентами підсистеми резервного копіювання та аварійного відновлення даних АСУ ТП. Результати моделювання представлені на рисунку 2.9.

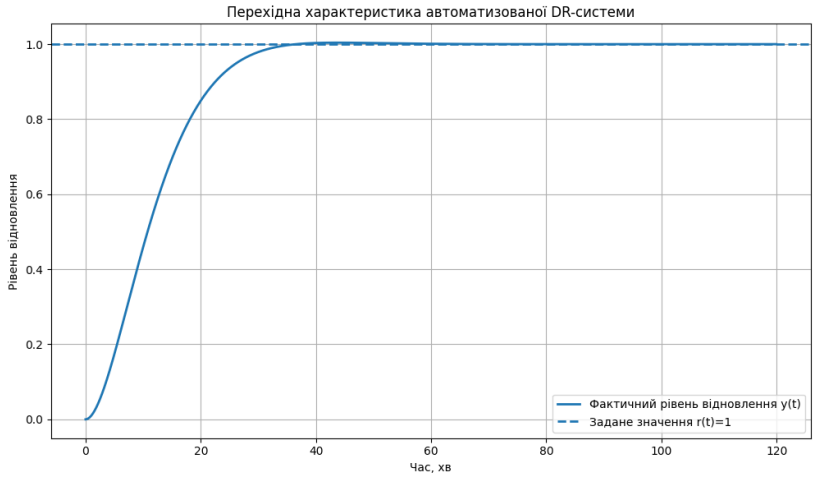


Рисунок 2.9 – Перехідна характеристика автоматизованої DR-системи

Отримана перехідна характеристика свідчить (рис. 2.9), що автоматизована DR-система є стійкою та забезпечує плавне досягнення заданого рівня відновлення без суттєвих коливань і втрати стійкості. Час встановлення становить приблизно 35–40 хвилин, після чого фактичний рівень відновлення наближається до 100 %, що підтверджує ефективність запропонованого регулятора та здатність системи забезпечувати своєчасне відновлення працездатності інформаційної інфраструктури після аварійних ситуацій або кібератак. На рисунку 2.10 представлено розташування коренів характеристичного рівняння.

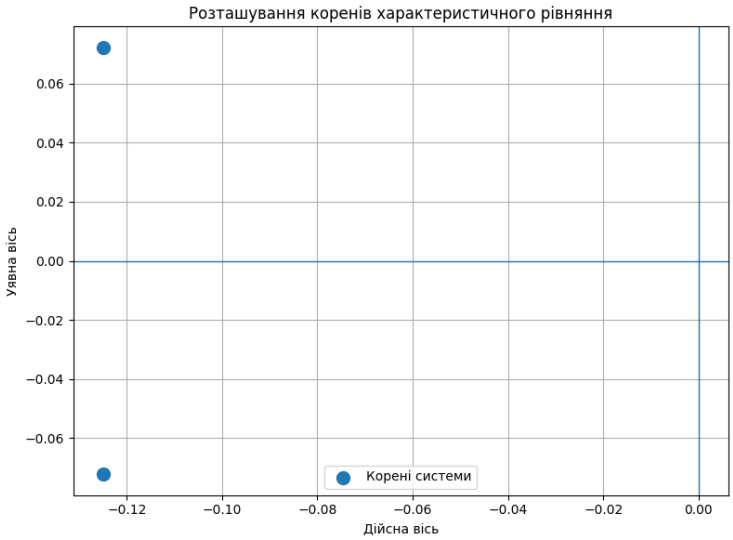


Рисунок 2.10 – Розташування коренів характеристичного рівняння

Отримане розташування коренів характеристичного рівняння (рис. 2.10) у лівій півплощині комплексної площини свідчить про асимптотичну стійкість автоматизованої DR-системи та відсутність ризику наростання коливань у процесі відновлення. Комплексно-спряжений характер коренів вказує на наявність слабко вираженої коливальної складової перехідного процесу, однак значення їх дійсної частини забезпечує достатньо швидке затухання відхилень і досягнення заданого рівня відновлення після виникнення аварійної ситуації. Годограф Найквіста розімкнутої DR- системи представлено на рисунку 2.11.

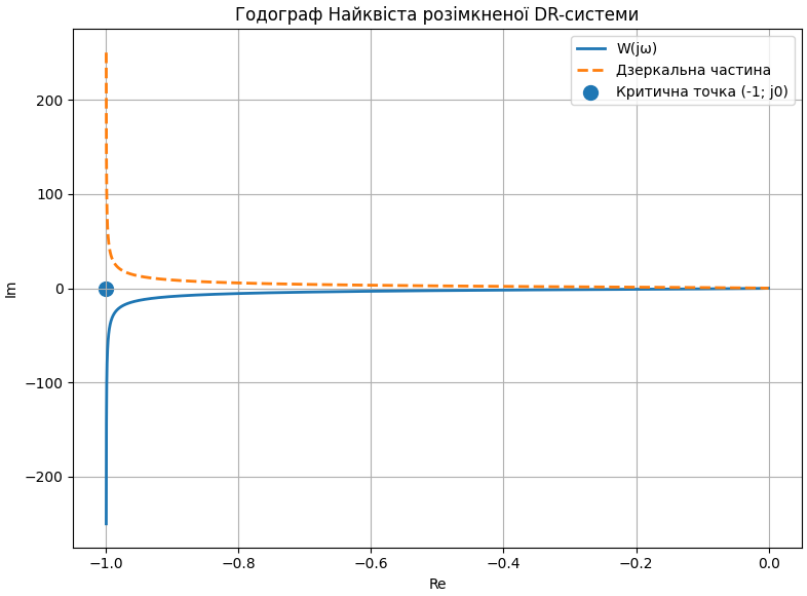


Рисунок 2.11 – Годограф Найквіста розімкнутої DR- системи

Отриманий годограф Найквіста не охоплює критичну точку $(-1; j_0)$ (рис. 2.11), що свідчить про стійкість замкненої автоматизованої DR-системи та наявність запасу стійкості відносно зміни параметрів об’єкта керування і регулятора. Форма годографа демонструє коректну частотну поведінку системи аварійного відновлення, при якій усі збурення та похибки керування згасають у часі, забезпечуючи надійне досягнення заданого рівня відновлення сервісів після збоїв, кібератак або втрати даних. Результати розрахунків представлено на рисунку 2.12.

```
Характеристичне рівняння:
12.000*s^2 + 3.000*s + 0.250 = 0

Корені характеристичного рівняння:
(-0.125+0.07216878364870322j)
(-0.125-0.07216878364870322j)

Система стійка за розташуванням коренів.
Система стійка за критерієм Гурвіца для 2-го порядку.
```

Рисунок 2.12 – Результати розрахунків

Отримані результати підтверджують (рис. 2.12), що характеристичне рівняння має комплексно-спряжені корені з від’ємною дійсною частиною, що свідчить про асимптотичну стійкість автоматизованої DR-системи та її здатність повертатися до заданого режиму роботи після виникнення збурень. Виконання умов критерію Гурвіца додатково підтверджує коректність вибраних параметрів регулятора й об’єкта керування, забезпечуючи надійне та передбачуване відновлення працездатності інформаційної системи після збоїв, кібератак або втрати даних.

Результати моделювання підтвердили працездатність запропонованої моделі автоматизованої системи аварійного відновлення даних та показали її здатність забезпечувати стійке досягнення заданого рівня відновлення після виникнення збоїв, кібератак або втрати даних. Аналіз перехідної характеристики, розташування коренів характеристичного рівняння та

годографа Найквіста засвідчив наявність необхідного запасу стійкості, відсутність нестійких режимів роботи та ефективне згасання відхилень у процесі функціонування системи. Отримані результати свідчать про доцільність використання методів теорії автоматичного керування для проєктування підсистем аварійного відновлення АСУ ТП, що дозволяє підвищити надійність інформаційної інфраструктури та скоротити час повернення системи до штатного режиму роботи.

3 ПРОЄКТУВАННЯ ПІДСИСТЕМИ РЕЗЕРВНОГО КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ

3.1 Налаштування середовища на базі ОС Linux (Ubuntu) та конфігурація системи резервного копіювання

Для демонстрації можливостей розробленої підсистеми та проведення апробації алгоритмів резервного копіювання було розгорнуто стенд на базі операційної системи Ubuntu 24.04 LTS [11]. Дана ОС виступає в ролі сервера управління автоматизованою системою управління технологічними процесами (АСУ ТП). Вибір саме цієї версії зумовлений її стабільністю та тривалим терміном підтримки, що є критично важливим для промислових об’єктів. Додатковою перевагою Ubuntu є високий рівень сумісності із серверним ПЗ та засобами автоматизації адміністрування.

Система також забезпечує підтримку сучасних механізмів мережевої безпеки та контролю доступу. Використання ОС із довготривалою підтримкою дозволяє мінімізувати ризики, пов’язані з несумісністю оновлень і припиненням підтримки компонентів. Це особливо важливо для середовищ АСУ ТП, де стабільність роботи має пріоритет над частим оновленням програмного забезпечення.

Крім того, Linux-платформа забезпечує гнучкі можливості інтеграції з системами резервного копіювання та моніторингу.

Основним компонентом, що підлягає захисту, є система керування базами даних MySQL. У межах дослідження в СКБД розгорнуто дві бази даних:

– production, яка містить актуальні дані технологічного процесу;

– development версія, яку використовують для тестування конфігурацій та оновлень.

У контексті функціонування АСУ ТП (наприклад, під управлінням RapidSCADA або Ignition SCADA) база даних MySQL відіграє роль

центрального сховища телеметричної інформації. У ній акумулюються дані про життєві показники промислового обладнання, обсяги виробленої продукції, показники браку, а також індивідуальні показники виробітку персоналу.

Важливість забезпечення безперервного доступу до цих даних обумовлена наступними факторами [13]:

– технологічна цілісність, адже втрата даних у реальному часі може призвести до розсинхронізації процесів та зупинки виробничих ліній;

– економічна звітність, так як на основі даних виробництва здійснюється розрахунок заробітної плати та оцінка ефективності співробітників;

– аналіз історичних даних. Відсутність архівних даних унеможливлює проведення аналізу причин аварійних ситуацій або відхилень у якості продукції.

Для реалізації процесу архівації було обрано інструмент під назвою Restic.

Процес встановлення програмного забезпечення в ОС Ubuntu здійснюється за допомогою стандартного менеджера пакунків apt:

apt update && apt install restic

Слід зауважити, що для використання найбільш актуальних функцій та виправлень безпеки рекомендується завантажувати готові бінарні файли безпосередньо з офіційного репозиторію розробників, що дозволяє уникнути обмежень, пов’язаних із версією пакунків у репозиторіях ОС які значно повільніше оновлюються [14].

Після завершення інсталяції необхідно підготувати інфраструктуру для безпечної передачі даних. Робота проводиться з правами суперкористувача. Першим кроком є створення директорії для службових скриптів та генерація пари ключів для автентифікації за протоколом SSH:

mkdir bin && cd bin && ssh-keygen -t ed25519

Результат представлено на рисунку 3.1.

Вибір алгоритму ed25519 обґрунтований його високою криптографічною стійкістю при відносно невеликій довжині ключа, що забезпечує швидку роботу при встановленні з’єднання.

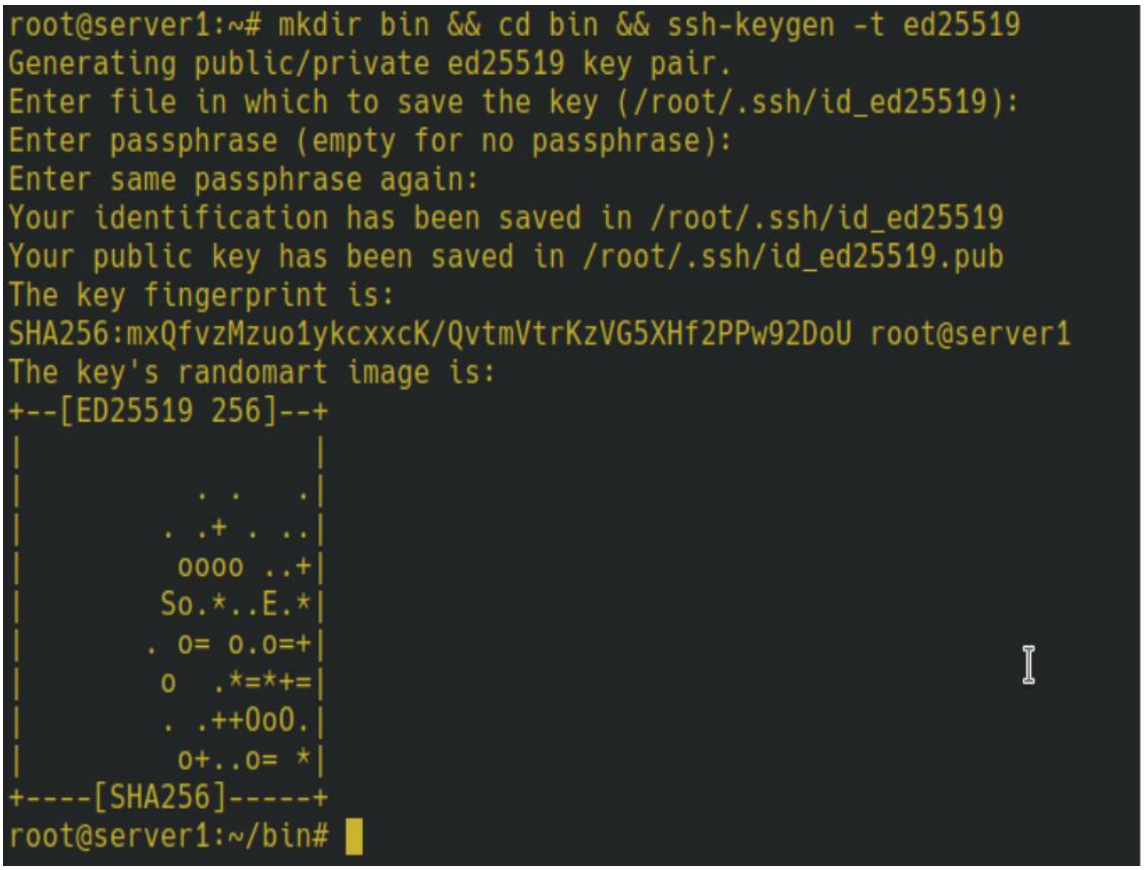


Рисунок 3.1 – Процес створення ключа формату ed25519

Для забезпечення безпечного зберігання снапшотів на віддаленому FTP/SFTP сервері використовується механізм обмеження прав доступу на рівні SSH-ключа. Публічна частина згенерованого ключа, що знаходиться у файлі “/root/.ssh/id_ed25519.pub”, повинна бути додана до файлу “.ssh/authorized_keys” на сервері призначеному для зберігання копій.

Для мінімізації ризиків навмисного видалення даних (наприклад, у випадку атаки вірусу-шифрувальника на основний сервер) запис у файлі “authorized_keys” модифікується спеціальним префіксом:

command=“rclone serve restic --stdio --append-only bucket” ssh-ed25519 AAAAC3NzaC1...

Частини префіксу призначені для виконанання таких функцій:

– rclone serve restic --stdio – ініціює використання rclone як прошарку для взаємодії з restic;

– --append-only – критично важливий параметр, що дозволяє клієнту лише додавати нові дані (снапшоти) до репозиторію, забороняючи видалення або модифікацію вже існуючих блоків;

– bucket – назва цільової директорії на сервері зберігання.

Результат цих дій представлено на рисунку 3.2.

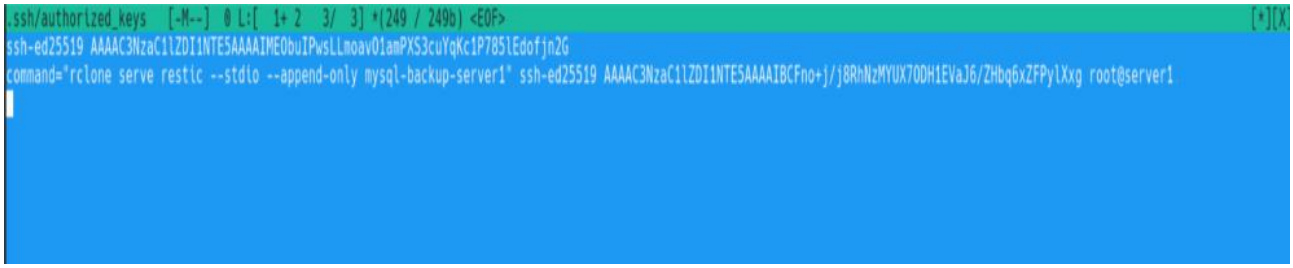


Рисунок 3.2 – Приклад конфігурації ключа із префіксом на сервері FTP

Дана конфігурація реалізує принцип ізоляції привілеїв, гарантуючи, що навіть при повному компрометуванні сервера АСУ ТП, зловмисник не зможе знищити вже створені резервні копії на віддаленому сховищі.

3.2 Реалізація скриптів для автоматизації процесів резервного копіювання

Для забезпечення регулярності та надійності створення резервних копій без участі оператора було розроблено спеціалізований Bash-скрипт. Автоматизація дозволяє виключити людський фактор та гарантує, що стан критичних баз даних АСУ ТП буде зафіксований згідно з визначеним графіком.

Після завантаження скриптів на сервер керування необхідно надати йому права на виконання. Це здійснюється за допомогою стандартної команди зміни атрибутів доступу:

chmod +x backup-mysql.sh

В додатку А наведено структуру та програмний код розробленого рішення.

Логіка роботи скрипта базується на чотирьох основних режимах:

– ініціалізація (init);

– перегляд статистики (stats);

– резервне копіювання (backup);

– відновлення даних (restore).

В ході ініціалізації на віддаленому сервері створюється структура репозиторію. На цьому етапі створюється мастер-пароль, який використовується для шифрування всіх даних.

Перегляд статистики дозволяє оператору перевірити поточний стан сховища та список існуючих копій.

Резервне копіювання виконує основний алгоритм, що експортує дані.

Відновлення даних дозволяє оператору швидко, у разі потреби, завантажити дані із віддаленого сховища на цільовий сервер для подальшого відновлення.

Параметр “--single-transaction” дозволяє робити знімок даних без блокування таблиць, що є критичним для систем, які працюють у режимі 24/7.

Перший запуск системи вимагає ініціалізації сховища Restic командою “bash backup-mysql.sh init” представлено на рисунку 3.3.



Рисунок 3.3 – Процес запуску ініціалізації сховища Restic

Під час цього процесу встановлюється складний пароль, що містить літери різних регістрів, цифри та спеціальні символи. Важливо підкреслити, що архітектура Restic побудована на принципі нульової довіри та повного шифрування, тому втрата цього пароля унеможливлює відновлення даних, оскільки механізм скидання доступу відсутній. Пароль було збережено у захищеному менеджері паролів, а його копія інтегрована у змінну RESTIC_PASSWORD для автоматизації скрипта.

Процес створення копії передбачає багаторівневе стиснення. Спочатку дані обробляються допоміжною програмою pigz (паралельна реалізація gzip), а потім архівуються в .tar. Хоча Restic має власні вбудовані алгоритми компресії та дедуплікації “на льоту”, (що особливо ефективно для застарілого обладнання з обмеженими ресурсами), попереднє стиснення в даному випадку дозволяє зменшити обсяг мережевого трафіку.

Для підтвердження коректності роботи розробленого інструментарію було проведено серію тестових запусків. На рисунку 3.4 зображено термінальний вивід процесу ініціалізації процедури резервного копіювання за допомогою команди “bash backup-mysql.sh backup”.

```
root@server1:~# bash backup-mysql.sh backup
Starting database dumps...
Backing up database: data_dev
Backing up database: data_prod
Backing up system database: mysql
Creating tar archive...
Uploading to remote storage (Restic)...
Backup successfully uploaded to Restic.
Cleaning up local temporary files...
Process completed successfully.
root@server1:~#
```

Рисунок 3.4 – Процес виконання резервного копіювання баз даних

Важливою функцією підсистеми є можливість оперативного моніторингу наявних копій. На рисунку 3.5 продемонстровано вивід команди stats, що відображає історію створених снапшотів.

```
root@server1:~# bash backup-mysql.sh stats
repository cd11ae44 opened (version 2, compression level auto)
found 1 old cache directories in /root/.cache/restic, run `restic cache --cleanup` to remove them
ID        Time                 Host            Tags        Paths                              Size
----------------------------------------------------------------------------------------------------
e0fc22dc  2025-12-04 04:30:13  server1      mysql-backup   /root/backup-mysql/mysql-backup.tar  12.350 MiB
64901e51  2025-12-05 04:30:11  server1      mysql-backup   /root/backup-mysql/mysql-backup.tar  12.950 MiB
1c3fa293  2025-12-06 04:30:13  server1      mysql-backup   /root/backup-mysql/mysql-backup.tar  13.614 MiB
df2766fe  2025-12-07 04:30:14  server1      mysql-backup   /root/backup-mysql/mysql-backup.tar  14.082 MiB
4c029f6d  2025-12-08 04:30:12  server1      mysql-backup   /root/backup-mysql/mysql-backup.tar  14.370 MiB
88e7c274  2025-12-09 04:30:15  server1      mysql-backup   /root/backup-mysql/mysql-backup.tar  15.158 MiB
----------------------------------------------------------------------------------------------------
6 snapshots
root@server1:~#
```

Рисунок 3.5 – Процес виконання резервного копіювання баз даних

Результатом роботи скрипта є створення снапшота – незмінного стану об’єкта в конкретний момент часу. Кожен такий снапшот у сховищі захищений від модифікації, що забезпечує цілісність історичних даних про виробничі показники навіть у разі спроб зловмисного втручання в систему після створення копії.

Для забезпечення повноцінного циклу аварійного відновлення (Disaster Recovery) до основного керуючого скрипта було додано функцію restore. Це дозволяє оперативно повернути базу даних до робочого стану у разі програмного збою або пошкодження файлової системи.

Команда відновлення вимагає введення двох обов’язкових аргументів: ID снапшота та директорія на сервері, куди будуть розпаковані дані.

Результат виконання команди представлено на рисунку 3.6.

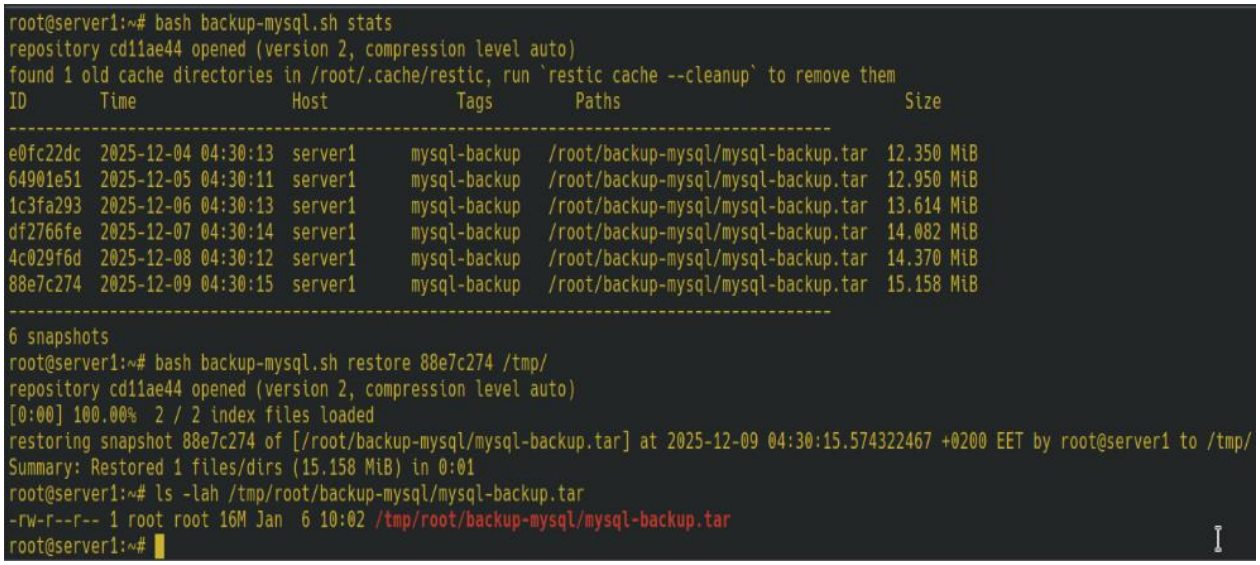


Рисунок 3.6 – Процес успішного відновлення даних із репозиторію за допомогою команди “bash backup-mysql.sh restore [ідентифікатор_снапшота] /шлях/до/директорії”

Restic автоматично перевіряє цілісність індексів, завантажує необхідні блоки даних із віддаленого сховища та проводить їх рекомбінацію на цільовому сервері. Важливою перевагою такого підходу є можливість відновлення “в один крок”, що мінімізує RTO промислового сервера.

Після завершення роботи команди за вказаним шляхом з’являться файли дампів баз даних, які можна імпортувати назад у MySQL стандартними засобами. Це гарантує, що навіть у разі повної втрати інформації на основному вузлі, адміністратор зможе відновити актуальний стан виробничої бази даних за лічені хвилини.

Для перетворення розробленого скрипта на повноцінну автономну підсистему було налаштовано планувальник завдань Cron. Це дозволяє виконувати резервне копіювання в автоматичному режимі без втручання адміністратора.

Редагування таблиці завдань здійснюється командою “crontab -e”, де було додано наступний рядок:

30 4 * * * systemd-run --scope -p CPUQuota=50% -p MemoryHigh=4G /root/bin/backup-mysql.sh backup > /var/log/mysql_backup.log 2>&1

Обраний час (04:30 ранку) обумовлений технологічним регламентом підприємства – у цей період спостерігається мінімальна інтенсивність виробничих процесів та найнижче навантаження на мережеву інфраструктуру та дискову підсистему сервера. Ведення log-файлу /var/log/mysql_backup.log дозволяє здійснювати подальший аудит успішності операцій та оперативно виявляти можливі помилки під час виконання завдання. Додатково через systemd-run встановлено ліміти: 50 % потужності ЦП та 4 ГБ оперативної пам'яті (що становить 50 % від загального обсягу сервера у експериментальному середовищі). Це запобігає потенційному захопленню 100 % RAM процесом бекапу та виключає «боротьбу» за ресурси, яка могла б виникнути без цих обмежень.

3.3 Імплементація політик зберігання та ротації резервних копій

Забезпечення безперервного резервного копіювання потребує ефективного управління дисковим простором віддаленого сховища. Без впровадження політики ротації (видалення застарілих даних) обсяг репозиторію буде невпинно

зростати, що призведе до надлишкових витрат ресурсів. У межах даної роботи було встановлено термін зберігання копій тривалістю 30 діб. Такий період є оптимальним для АСУ ТП, оскільки дозволяє відновити стан системи на будь-який момент протягом останнього місяця, що зазвичай достатньо для виявлення та усунення наслідків збоїв або кібер-інцидентів.

Ключовим аспектом розробленої системи безпеки є розподіл повноважень між серверами. Для реалізації безпечного видалення застарілих даних було впроваджено окремий вузол – сервер-бастіон (Сервер 2). Це мінімальна за ресурсами віртуальна машина (VPS), що виконує роль контролера сховища.

Така архітектура реалізує наступну модель безпеки:

– сервер 1 (Джерело). Має обмежені права (append-only). Він може лише додавати нові дані, але не має технічної можливості видалити жодного байту з репозиторію. Це захищає бекапи від знищення у випадку повного компрометування основного сервера АСУ ТП;

– сервер 2 (Контролер). Має повні права доступу до репозиторію. Це єдиний вузол у мережі, який може виконувати операції очищення.

Для налаштування Сервера 2 на віддалений FTP-сервер було передано публічний SSH-ключ без обмежувальних префіксів, на відміну від конфігурації, представленої раніше на рисунку 3.2. Нові параметри налаштування представлено на рисунку 3.7 нижче.



Рисунок 3.7 – Конфігурація файлу “authorized_keys” з розмежуванням прав доступу

На Сервері 2 розміщено керуючий скрипт, який відповідає за підтримання актуальності глибини архіву. Програмний код для реалізації алгоритму ротації представлено нижче:

```
#!/bin/bash
URI="u31341-sub1@u31341.your-storagebox.de"
RESTIC="/usr/local/bin/restic -o rclone.program='ssh -p 23 -i /root/.ssh/id_ed25519 $URI' -o rclone.args='rclone serve restic --stdio %REPO%' -r rclone: "
export RESTIC_PASSWORD="YouRSec$ePassW@RD"
eval "${RESTIC/\%REPO\%/mysql-backup-server1} forget -q --keep-daily 30 --prune"
```

Логіка роботи скрипта базується на використанні двох ключових команд Restic:

– forget ідентифікує снапшоти, які більше не відповідають заданій політиці зберігання;

– prune проводить фізичне видалення об'єктів з репозиторію, звільняючи місце на FTP-сервері.

Важливою особливістю використання параметру “--keep-daily 30” є його відмовостійкість. Дана команда інтерпретується системою як “залишити останні 30 добових снапшотів”. Це створює критично важливий запобіжник: якщо з будь-яких причин (збій мережі, аварія на Сервері 1 та ін.) нові резервні копії перестануть надходити, скрипт на Сервері 2 не буде видаляти існуючі копії, оскільки загальна кількість актуальних знімків не перевищуватиме ліміт у 30 одиниць. Таким чином, система захищена від ситуації, коли через технічну помилку ми могли б залишитися взагалі без резервних копій.

Скрипт очищення також додається до планувальника Cron на Сервері 2 для виконання раз на добу, забезпечуючи повністю автономний цикл життя даних у підсистемі резервного копіювання.

3.4 Налаштування Zabbix Agent моніторингу на сервері-бастіоні

Припускаючи, що Zabbix Agent 2 вже встановлений та підключений до сервера моніторингу, необхідно розширити його функціонал за допомогою механізму “UserParameter”. У директорії “/etc/zabbix/zabbix_agent2.d/” створено конфігураційний файл “userparameter_restic_check.conf”, який дозволяє агенту зчитувати результати перевірок. Це забезпечує передачу текстових повідомлень про помилки безпосередньо в інтерфейс моніторингу.

На Сервері 2 розміщується скрипт, який за допомогою утиліти jq аналізує метадані репозиторію у форматі JSON. Його логіка полягає у порівнянні часових міток існуючих снапшотів із поточним часом системи. Код наведено в додатку Б.

Цей скрипт перевіряє дві критичні умови:

– “чи актуальні бекапи?” Якщо остання копія старіша за 36 годин, це свідчить про збій на Сервері 1;

– “чи працює ротація?” Якщо в сховищі залишаються дані старіші за 33 дні, це вказує на несправність алгоритмів очищення на самому Сервері 2.

Для збору та агрегації цих даних було розроблено шаблон для системи моніторингу “Restic Backup Check”. Цей шаблон наведено в додатку В.

Основна логіка шаблону базується на наступних елементах:

– items (елементи даних): тип ZABBIX_ACTIVE. Скрипт діагностики налаштований так, що за нормальних умов він не повертає жодного тексту. Будь-яка відповідь (Error/Warning) розцінюється як інцидент;

– triggers (тригери): використовується вираз length(last(/Restic Backup Check/restic_check_fsn1))>0. Якщо довжина отриманого тексту більша за нуль – активується тригер середньої важливості;

– macros (макроси): параметр {$BACKUP_HOURS} встановлено на значення 36. Це значення обрано навмисно, оскільки копіювання великих баз даних MySQL може тривати кілька годин, стандартний поріг у 24 години міг би

призводити до хибних спрацювань. Додатковий часовий проміжок у 12 годин забезпечує стабільність моніторингу і відсутність хибних спрацювань.

Після призначення шаблону хоста та перезапуску служби агенту з використанням команди “service zabbix-agent2 restart” система переходить у режим активного моніторингу.

В результаті виконання практичної частини було розроблено та впроваджено триланкову архітектуру захисту критичних компонентів АСУ ТП:

– сервер 1 (промисловий вузол) виконує створення архівних копій у режимі “лише додавання”, що унеможливлює видалення архіву з боку зловмисника;

– сервер 2 (бастіон) забезпечує безпечну ротацію даних згідно з політикою 30 діб та проводить аудит цілісності репозиторію;

– сервер 3 (система моніторингу) збирає діагностичні дані, візуалізує стан системи та сповіщає персонал у разі відхилення від норм експлуатації.

4 ТЕСТУВАННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ПІДСИСТЕМИ

4.1 Імітація атаки з повним доступом до виробничого сервера

Для перевірки стійкості розробленої підсистеми було проведено стрес-тестування, що імітує цілеспрямовану атаку на критичну інфраструктуру підприємства. У межах сценарію розглядається вектор атаки через методи соціальної інженерії – використання невідомого змінного носія (USB-накопичувача в даному випадку), знайденого персоналом на території об’єкту.

Внаслідок ігнорування протоколів безпеки співробітником, зловмисник отримав віддалений доступ до операційної системи сервера управління АСУ ТП із root-правами доступу. Метою атаки є повна деструкція цифрових активів підприємства [10], що включає:

– видалення робочих баз даних (MySQL data_prod та data_dev), що призводить до миттєвої зупинки моніторингу технологічного процесу;

– знищення резервних копій, щоб унеможливити відновлення системи та змусити підприємство до повної зупинки виробничого циклу без можливості ретроспективного аналізу даних.

Після успішної компрометації сервера зловмисник видалив основні бази даних. Наступним етапом став спроб очищення віддаленого репозиторію Restic, використовуючи наявні на сервері конфігураційні файли та SSH-ключі.

4.2 Аналіз результатів тестування

Результати тестування продемонстрували високу ефективність впровадженої архітектури безпеки. Незважаючи на наявність у зловмисника повних прав доступу на виробничому сервері, спроба видалення снапшотів із віддаленого сховища завершилася невдачею.

На рисунку 4.1 зображено вигляд вікна терміналу при спробі виконати команду видалення даних скомпрометованим сервером АСУ ТП.

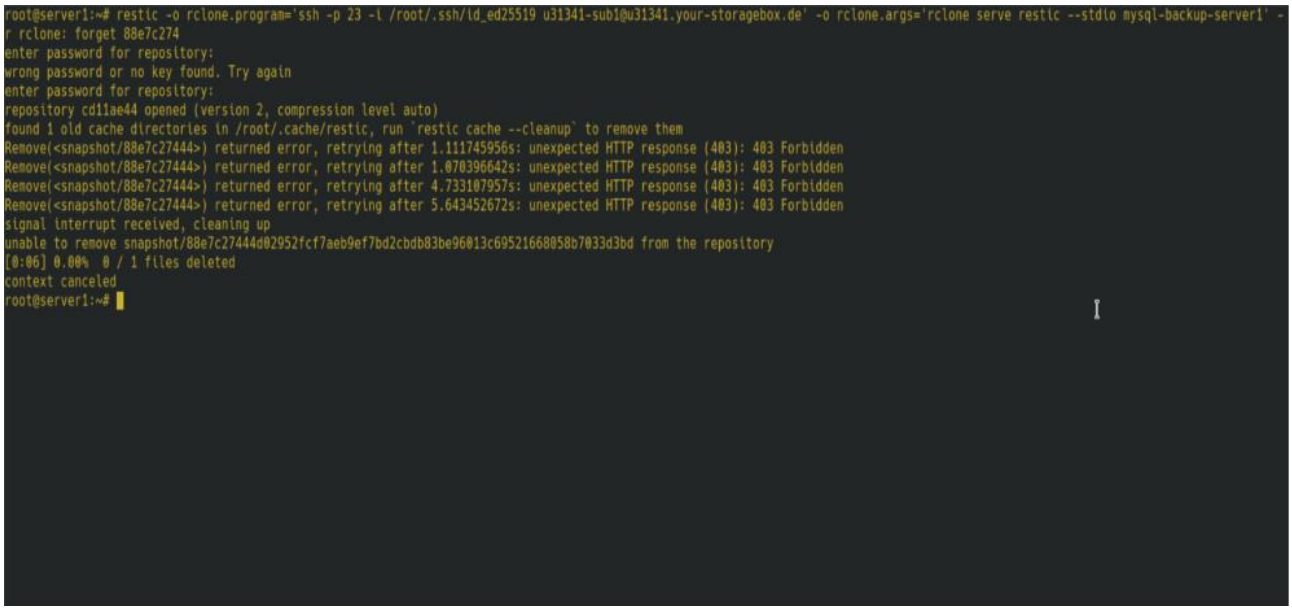


Рисунок 4.1 – Помилка доступу при спробі несанкціонованого видалення резервних копій

Аналіз причин невдачі атаки дозволяє виділити наступні захисні фактори:

– принцип найменших привілеїв для SSH. Завдяки використанню директиви “command="rclone serve restic --stdio --append-only bucket"” у файлі “authorized_keys” на стороні сховища, SSH-ключ виробничого сервера був обмежений виключно операціями запису;

– технологічна ізоляція серверу. Сервер АСУ ТП технічно не має доступу до функцій “forget” або “prune” на рівні протоколу взаємодії. При спробі їх виконання віддалений сервер повертає помилку “403 Forbidden”, блокуючи будь-які деструктивні запити;

– відсутність майстер-ключа на робочій станції. Ключ із повними правами (включаючи можливість видалення) фізично відсутній на виробничому сервері. Він зберігається на ізольованому хості-бастіоні (Сервер 2), про існування якого зловмисник може навіть не здогадуватися, оскільки цей вузол не бере участі в основному технологічному процесі.

Після впровадження цієї системи захисту навіть за умови критичного зламу основної системи, дані залишаються в безпеці. Це підтверджує, що запропонована схема з розподілом прав доступу та використанням режиму append-only є надійним бар’єром проти атак типу Ransomware з використанням вірусів-шифрувальників та цілеспрямованого саботажу.

4.3 Охорона праці

Розроблення підсистеми резервного копіювання та аварійного відновлення даних для АСУ ТП здійснювалося в офісному приміщенні з використанням персонального комп'ютера. Основна діяльність пов'язана з розробленням програмного забезпечення, адмініструванням серверного середовища Linux, налаштуванням систем моніторингу та проведенням тестування.

Для виконання робіт з програмування та адміністрування серверних систем нормативна освітленість робочої поверхні повинна становити не менше 300 лк.

Виконаємо розрахунок загального рівномірного освітлення методом коефіцієнта використання світлового потоку. Візьмемо такі параметри приміщення, як довжина приміщення A = 6 м, ширина приміщення B = 4 м, висота приміщення H = 3 м. Площа приміщення дорівнюватиме:

$$S = A \cdot B = 6 \cdot 4 = 24 \text{ м}^2. \quad (4.1)$$

Робоча поверхня розташована на висоті hp = 0,8 м. Тоді висоту підвісу світильників над робочою поверхнею можна буде розрахувати:

$$h = H - hp = 3 - 0{,}8 = 2{,}2 \text{ м}. \quad (4.2)$$

Індекс приміщення розрахуємо за формулою:

$$i = A \cdot B / h\,(A + B), \qquad (4.3)$$

$$i = 6 \cdot 4 / 2{,}2\,(6 + 4) = 24 / 22 = 1{,}09.$$

Для світлодіодних світильників приймаємо:

– коефіцієнт використання світлового потоку $\eta = 0{,}55$;

– коефіцієнт запасу $Кз = 1{,}5$;

– нормована освітленість $En = 300$ лк.

Необхідний сумарний світловий потік:

$$Ф\Sigma = En \cdot S \cdot Кз / \eta, \qquad (4.4)$$

$$Ф\Sigma = 300 \cdot 24 \cdot 1{,}5 / 0{,}55 = 19636 \text{ лм}.$$

Для освітлення обираємо світлодіодні панелі зі світловим потоком $Ф1 = 3600$ лм, необхідна кількість світильників дорівнюватиме:

$$N = Ф\Sigma / Ф1 = 5{,}45. \qquad (4.5)$$

Тобто, бажана кількість світильників дорівнюватиме 6. Розрахуємо фактичну освітленість за формулою:

$$Ef = N \cdot Ф1 \cdot \eta / S \cdot Кз, \qquad (4.6)$$

$$Ef = 6 \cdot 3600 \cdot 0{,}55 / 24 \cdot 1{,}5 = 330 \text{ лк}.$$

Використання шести світлодіодних світильників забезпечує освітленість 330 лк, що відповідає нормативним вимогам для робіт з використанням ПЕОМ, що сприяє збереженню працездатності персоналу та підвищенню надійності процесів розроблення й супроводу програмного забезпечення для АСУ ТП [15].

ВИСНОВКИ

У межах виконаної роботи розроблено підсистему автоматизованого резервного копіювання та аварійного відновлення даних для критичних компонентів АСУ ТП, орієнтовану на забезпечення високого рівня надійності, безпеки та доступності даних в умовах сучасних кіберзагроз.

На початковому етапі було проведено аналіз особливостей АСУ ТП, визначено ключові вимоги до забезпечення цілісності та доступності даних, а також розглянуто сучасні методи резервного копіювання. Особливу увагу приділено загрозам, зокрема атакам типу ransomware, що дозволило сформувати обґрунтовані вимоги до побудови захищеної підсистеми резервного копіювання.

У процесі проєктування було сформовано архітектуру підсистеми, яка базується на принципах Zero Trust та передбачає чітке розмежування повноважень між компонентами. Розроблено модель безпеки, що включає використання сервера-бастіону, багатофакторної автентифікації та шифрування даних, а також модель життєвого циклу резервних копій і політики їх зберігання. Окремо було визначено алгоритм моніторингу та контролю резервного копіювання, що забезпечує незалежну перевірку цілісності та актуальності даних.

На етапі реалізації виконано налаштування середовища на базі ОС Linux, розроблено скрипти автоматизації резервного копіювання, реалізовано політики ротації резервних копій та інтегровано систему з інструментами моніторингу. Використання Restic дозволило забезпечити надійне шифрування та захист резервних копій, тоді як Zabbix забезпечив постійний контроль стану системи та своєчасне виявлення відхилень.

У межах тестування було проведено перевірку працездатності підсистеми в умовах, наближених до реальних, включаючи імітацію компрометації виробничого сервера. Отримані результати підтвердили стійкість системи до

знищення або пошкодження резервних копій, а також відповідність заданим показникам RPO та RTO.

Результатом роботи є функціональна підсистема резервного копіювання, що забезпечує багаторівневий захист даних, автоматизацію процесів та незалежний контроль їхнього стану. Запропоноване рішення характеризується високою надійністю, масштабованістю та відповідністю сучасним вимогам КІБ, що дозволяє ефективно застосовувати його в реальних умовах експлуатації АСУ ТП.

Отримані результати можна віднести до Цілі сталого розвитку 9 «Промисловість, інновації та інфраструктура», а саме 9.5. Створити фінансову та інституційну системи (інноваційну інфраструктуру), що забезпечуватимуть розвиток наукових досліджень та науковотехнічних (експериментальних) розробок [16].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Кремзуков О.В. Підвищення стійкості АСУТП до кіберзагроз засобами автоматизованого резервного копіювання // Автоматизація та Приладобудування («Automation and Development of Electronic Devices» ADED-2026) : збірник студентських наукових статей. Харків : ХНУРЕ, 2026. Вип. 1. pp. 50-56.

2. ДСТУ 3008:2015 Інформація та документація «Звіти у сфері науки і техніки». Структура та правила оформлювання. / В. Земцева; Ю. Поліщук, 07-01.

3. Невлюдов І.Ш. Навчальний посібник з підготовки кваліфікаційної роботи бакалавра для здобувачів вищої освіти денної і заочної форм навчання спеціальності 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка освітньої програми «Автоматизація та комп'ютерно-інтегровані технології»: Навчальний посібник / І. Ш. Невлюдов, О. І. Филипенко, О. В. Токарєва, С. П. Новоселов, О. В. Сичова. – Харків: Видавництво Іванченка І. С., 2025. – 164 с.

4. Методичні вказівки з підготовки кваліфікаційної роботи для здобувачів першого (бакалаврського) рівня вищої освіти денної і заочної форми навчання спеціальності 151 – Автоматизація та комп'ютерно-інтегровані технології освітньої [Електронний ресурс] / упоряд.: І. Ш. Невлюдов, О. І. Филипенко, О. В. Токарєва, С. П. Новоселов, О.В Сичова; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – електрон. вид. – Харків: ХНУРЕ, 2023.

5. Навчальний посібник з підготовки кваліфікаційної роботи бакалавра для здобувачів вищої освіти денної і заочної форм навчання спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» освітньої програми «Автоматизація та комп'ютерно-інтегровані технології»: Навчальний посібник / І. Ш. Невлюдов, О. І. Филипенко, О. В. Токарєва, С. П. Новоселов, О. В. Сичова. – Харків: Видавництво Іванченка І. С., 2023. – 151 с. ISBN 978-617-8059-94-1, DOI: 10.30837/978-617-8059-94-1

6. Ackerman P. Industrial Cybersecurity: Efficiently secure critical infrastructure systems. – Birmingham: Packt Publishing, 2017. – 800 с.

7. Knapp E. D., Langill J. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. – 2nd ed. – Cambridge: Elsevier, 2015. – 460 с.

8. Blade Technologies. Distribution Industry Solutions [Електронний ресурс]. – Режим доступу: https://www.bladetechinc.com/industries/distribution (дата звернення: 16.03.2026).

9. Новоселов С. П. Основи розробки кросплатформного програмного забезпечення на Avalonia : Навчальний посібник / С. П. Новоселов, О. В. Сичова. – Харків: Видавництво Іванченка І. С., 2024. – 267 с. ISBN 978-617-8332-57-0 DOI: 10.30837/978-617-8332-57-0 (Навчальний посібник) https://publish.nure.ua/catalog/book/500

10. Humble J., Farley D. Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation. – Boston: Addison-Wesley, 2011. – 512 с.

11. Nemeth E., Snyder G., Hein T. R., Whaley B. UNIX and Linux System Administration Handbook. – 5th ed. – Boston: Addison-Wesley, 2017. – 1232 с.

12. Невлюдов І. Ш. Промислові мережі та компоненти АСУТП : Навчальний посібник / І. Ш. Невлюдов, С. П. Новоселов, О. В. Сичова, С. І. Теслюк. – Харків: Видавництво Іванченка І. С., 2025 . – 241 с. (Навчальний посібник) ISBN 978-617-8332-83-9 DOI: 10.30837/978-617-8332-83-9 https://publish.nure.ua/catalog/book/844

13. Restic releases [Електронний ресурс]. – Режим доступу: https://github.com/restic/restic/releases (дата звернення: 20.03.2026).

14. Lewis W. E. Software Testing and Continuous Quality Improvement. – 3rd ed. – Boca Raton: CRC Press, 2009. – 584 с.

15. ДСТУ 3400:2015. Охорона праці. Безпека при роботі з електричними установками. – К.: Національний стандарт України, 2015. – 33 с.

16. Ціль 9. Промисловість, інновації та інфраструктура // Дія, 2025. URL: https://business.diia.gov.ua/entrepreneurhandbook/item/cil_9_promislovist_innovaciyi_ta_infrastruktura (дата звернення: 15.06.2026).