Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)
спеціальність *125 Кібербезпека*
(код і назва спеціальності)
освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)
на тему: «Засоби захисту розподіленої інформаційної системи об'єкта критичної інфраструктури»

Виконавець: студентка ІІ курсу, групи КБм-22
_____ **Валерія СОЛОДОВНИК**
(підпис) (Ім’я, ПРІЗВИЩЕ)

	Ім’я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Сергій ТОЛЮПА	
Нормоконтроль	Яніна ШЕСТАК	

Київ 2024

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-22 (група) Солодовник Валерії Олегівні (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Засоби захисту розподіленої інформаційної системи об'єкта критичної інфраструктури

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес розробки програми резервного копіювання даних.
Предмет досліджень	Методи побудови захищених розподілених інформаційних систем
Мета	Розробка скрита резервного копіювання даних на віддалений

сервер з подальшою можливістю об’єднання цього процесу з технологією Air-Gap для об’єктів критичної інфраструктури.

Вихідні дані для проведення роботи Методи побудови розподілених інформаційних систем.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Розробка скрипта автоматизованого бекапування файлів, з метою зниження ризиків, пов'язаних з людським фактором, та покращення процесу виконання бекапів.

Практична цінність Автоматизація виконання резервного копіювання в розподіленій інформаційній системі

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	17.11.2023 – 29.01.2024
Аналіз літературних джерел	30.01.2024 – 01.03.2024
Проведення категоріювання об’єкта критичної інфраструктури	02.03.2024 – 10.03.2024
Аналіз методів та засобів захисту розподілених інформаційних систем	11.03.2024 – 20.03.2024
Розробка скрипта для резервного копіювання в лабраторних умовах	21.03.2024 – 05.04.2024
Пропозиція імплементації на об’єкти ОКІ процедури резервного копіювання в поєднанні з технологією Air-Gap	06.04.2024 – 20.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	21.04.2024 – 12.05.2024
Подача пакету документів на розгляд ЕК	13.05.2024 – 17.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків через знищення даних.

Соціальний ефект	Покращення процесу створення резервних копій для розподілених інформаційних систем.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Сергій ТОЛЮПА
(підпис) (Ім’я, ПРІЗВИЩЕ)

Завдання прийняв
до виконання _____ Валерія СОЛОДОВНИК
(підпис) (Ім’я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.
Термін подання кваліфікаційної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, використаних джерел та додатків. Основний текст займає 95 сторінок, містить 25 рисунків і 4 таблиці. Список використаних джерел має обсяг 6 сторінок, і складється із 53 найменувань. Крім того, робота містить 2 додатки із загальною кількістю сторінок 5.

Метою роботи є розробка скрита резервного копіювання даних на віддалений сервер з подальшою можливістю об’єднання цього процесу з технологією Air-Gap для об’єктів критичної інфраструктури.

Об’єктом дослідження є процес розробки програми резервного копіювання дани з подальшою можливістю імплетементації додаткових технологій захисту для даних, які зберігаються в цих системах.

Предметом дослідження є методи побудови захищених розподілених інформаційних систем.

Практичною цінністю отриманих результатів є створення програми для виконання резервного копіювання в розподіленій інформаційній системі із подальшою можливістю імплементації технології Air-Gap після створення резервних копій. Надання пропозицій щодо впровадження технології Air-Gap в поєднанні із програмою резервного копіювання для підвищення безпеки розподіленої інформаційної системи.

Результати зроблених у магістерській кваліфікаційній роботі досліджень можуть бути використані для: впровадження програмного забезпечення для розширення функціоналу безпеки, підвищення рівня захищеності резервних копій інформаційних систем.

Наукова новизна полягає у розробці скрипта бекапування файлів, розробленого у межах магістерської роботи, який автоматизує процес резервного копіювання, від створення копій до їх збереження та логування, що знижує ризики, пов'язані з

людським фактором, та покращує процес виконання бекапів.

Напрямки подальших досліджень: покращення продуктивності інформаційних системи, економічна доцільність впровадження новішого програмного та апаратного забезпечення, покращення процесу створення резервних копій та можливість поєднання цього процесу із технологією Air-Gap для підвищення відмовостійкості критичних системи.

Методи дослідження включають структурний аналіз, порівняльний аналіз, системний підхід та моделювання.

Ключові слова: розподілена інформаційна система, вразливості, архітектура, захист інформації, безпека, критична інфраструктура, захист інформації, резервне копіювання, кібербезпека, уразливості, функціонування системи, моніторинг, технічний захист, програмний захист, апаратна складова, програмна складова, інфраструктура, відмовостійкість, структурний підрозділ, реплікація, система сховищ, сервери, комутаційне обладнання.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

OSI	–	Open Systems Interconnection
DoS	–	Denial-of-service attack
DDoS	–	Distributed denial-of-service attack
IT	–	Information Technology
IP	–	Internet Protocol
ARP	–	Address Resolution Protocol
MAC	–	Media Access Control
ACL	–	Access Control List
BSD	–	Berkeley Software Distribution
DNS	–	Domain Name System
KVM	–	Kernel-based Virtual Machine
SQL	–	Secure Shell
XSS	–	Application Programming Interface
MITM	–	Man-in-the-middle
HTTP	–	Hypertext Transfer Protoco
HTTPs	–	Hypertext Transfer Protocol Secure
EOL	–	End-of-life
MTTR	–	Mean time to repair
ESG	–	Enterprise Strategy Group
IDS	–	Intrusion Detection System
IPS	–	Intrusion Prevention System
WORM	–	Write once, read many
VM	–	Virtual machine
LTS	–	Long-term support
NFS	–	Network file system
HIPAA	–	Health Insurance Portability and Accountability Act

HITRUST	–	Health Information Trust Alliance
FINRA	–	Financial Industry Regulatory Authority
FISMA	–	Federal Information Security Modernization Act
NFV	–	Network Functions Virtualization
GDPR	–	General Data Protection Regulation
HDD	–	Hard disk drive
ТК	–	Телекомунікаційна компанія
ОКІ	–	Об’єкт критичної інфраструктури
РІС	–	Розподілена інформаційна система
КНЕДП	–	Кваліфікований надавач електронних довірчих послуг
РК	–	Рівень критичності
ІКМ	–	Інфокомунікаційної мережі
ЗБС	–	Загроза безпеки системи
ПЗ	–	Програмне забезпечення
СЗД	–	Система зберігання даних
ОС	–	Операційна система
СБУ	–	Служба Безпеки України
ПК	–	Персональний комп’ютер

ЗМІСТ

ВСТУП

У сучасному світі, де технології та інформаційні системи глибоко інтегровані в усі сфери людської діяльності, захист критичної інфраструктури набуває особливого значення. Розподілені інформаційні системи, які є частиною об'єктів критичної інфраструктури, включають складні мережі з численними вузлами та взаємозалежностями. Захист цих систем перед загрозами кібербезпеки, технічними збоями та фізичними втручаннями є ключовим для забезпечення національної безпеки, економічної стабільності та соціального благополуччя.

У рамках цієї магістерської роботи зосереджено увагу на розробці та оптимізації ефективних методів захисту для розподілених інформаційних систем, які виступають у ролі критично важливих об'єктів інфраструктури.

Об'єкт дослідження - це процес забезпечення інформаційної безпеки в розподілених інформаційних системах на об'єктах критичної інфраструктури, використовуючи засоби резервного копіювання.

Мета даної магістерської роботи полягає у дослідженні, аналізі та створенні ефективних методів резервного копіювання, які можуть бути інтегровані з іншими безпековими технологіями. Це робиться для підвищення стійкості розподілених інформаційних систем критичної інфраструктури проти існуючих та потенційних загроз.

Предметом дослідження виступають методи побудови захищених розподілених інформаційних систем.

Методи дослідження включають структурний аналіз, порівняльний аналіз, системний підхід та моделювання.

Наукова новизна полягає у розробці скрипта бекапування файлів, розробленого у межах магістерської роботи, який автоматизує процес резервного копіювання, від створення копій до їх збереження та логування, що знижує ризики, пов'язані з людським фактором, та покращує процес виконання бекапів.

Практичною цінністю отриманих результатів є створення програми для виконання автоматизованого резервного копіювання в розподіленій інформаційній системі із подальшою можливістю імплементації технології Air-Gap після створення резервних копій.

У ході роботи було проведено всебічний аналіз нормативно-правової бази критичної інфраструктури, виявлено сильні та слабкі сторони розподілених інформаційних систем, проведено категоризацію об'єктів критичної інфраструктури у секторі телекомунікацій. Також були розглянуті інциденти, що відбулися на цих об'єктах, та обговорено методи та засоби захисту, які використовуються для забезпечення безпеки розподілених інформаційних систем.

В контексті цієї магістерської роботи розглядається розробка та покращення ефективних засобів захисту для розподілених інформаційних систем, що відіграють роль об'єктів критичної інфраструктури.

Для реалізації мети дослідження були поставлені наступні завдання:

- Аналіз сучасного стану інформаційної безпеки на об'єктах критичної інфраструктури.
- Ідентифікація ключових вразливостей та потенційних загроз для розподілених інформаційних систем.
- Розробка рекомендацій щодо вдосконалення засобів захисту та процедур реагування на інциденти.
- Розробка програми для автоматизації процесу резервного копіювання в розподілених інформаційних систем.
- Розглянути можливість об’єднання технології Air-Gap та класичного резервного копіювання.

РОЗДІЛ 1
ОСОБЛИВОСТІ ЗАХИСТУ ОБ’ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Оскільки об'єкти критичної інфраструктури є невід'ємною складовою суспільної стабільності та економічної безпеки, їх захист вимагає злагоджених зусиль, як на рівні організацій, так і на рівні держави. Основою створення та управління цими об’єктами є нормативно-правова база, оскільки вона розкриває, як законодавство впливає на заходи безпеки та які обов'язки і відповідальність покладаються на учасників управління критичною інфраструктурою. Також має бути проаналізована розподілена інформаційна система, з точки зору її структурних характеристик та важливості у контексті критичної інфраструктури. Не менш необхідним є категоріювання ОКІ задля прийняття оптимальних та виважених рішень щодо рівнів захисту ресурсів.

1.1 Нормативно - правове забезпечення на об'єктах критичної інфрастуктури

Нормативно-правове забезпечення на об'єктах критичної інфраструктури є ключовим елементом забезпечення національної безпеки та стабільності держави. Далі будуть розглянуті основні законодавчі та регуляторні рамки, які регламентують діяльність та захист цих життєво важливих об'єктів. З огляду на складність та міжсекторальний характер критичної інфраструктури, ефективне нормативно-правове забезпечення вимагає комплексного підходу, що включає як загальнодержавні, так і специфічні для галузі норми і стандарти.

Національні закони, підзаконні акти, нормативні документи, які регулюють роботу об'єктів критичної інфраструктури є ключовими документами та потребують детального огляду. Особливу увагу слід зосередити на нормативних актах, які фокусуються захисті інформації на об’єктах критичної інфраструктури, зокрема в галузі телекомунікацій.

Забезпечення правової визначеності та прогнозованості, а також розроблення чітких та дієвих механізмів регулювання і контролю є важливими для підтримання високого рівня захисту критичної інфраструктури. Це також включає оцінку існуючих норм і практик, виявлення потенційних правових прогалин та розроблення рекомендацій щодо їх усунення. Основна мета — створення надійної правової основи, яка забезпечить ефективне управління ризиками та захист об'єктів критичної інфраструктури в умовах постійно змінювальних загроз.

Отже, до основних нормативних актів, які регулють функціонування об’єктів критичної інфраструктури та інформації в них належвть:

- Закон України "Про національну безпеку України"

  В ньому встановлюються правові засади забезпечення національної безпеки України. Цей Закон є фундаментальним документом, що визначає стратегічні цілі та пріоритети держави у сфері захисту об'єктів критичної інфраструктури [1].

- Закон України "Про критичну інфраструктуру"

Даний документ є ключовим для визначення об'єктів критичної інфраструктури, їх класифікації, а також встановлення вимог до їх захисту та безпеки. Він окреслює механізми ідентифікації таких об'єктів, вимоги до їх фізичного та кібернетичного захисту [2].

- Закон України "Про основні засади забезпечення кібербезпеки України"

З огляду на зростаючі загрози в кіберпросторі, цей закон відіграє критичну роль у захисті інформаційних систем та інфраструктур критично важливих об'єктів. Він встановлює правила та стандарти кібербезпеки, яких повинні дотримуватись власники та оператори об'єктів критичної інфраструктури [3].

- Закон України "Про захист інформації в інформаційно-комунікаційних системах"

Закон про захист інформації в інформаційно-комунікаційних системах регулює правові, організаційні та технічні заходи, спрямовані на забезпечення безпеки інформації в цих системах. Його мета полягає в захисті інформації від несанкціонованого доступу, використання, зміни, розкриття або знищення [4].

- Закон України "Про захист персональних даних"

Оскільки оператори телекомунікацій обробляють значні обсяги персональних даних користувачів, цей документ є важливим для регулювання збору, обробки, зберігання та захисту цих даних. Він встановлює вимоги до конфіденційності та захисту персональної інформації [5].

- Закон України "Про інформацію"

Документ визначає загальні принципи отримання, використання, поширення, захисту та інших способів обробки інформації. Він акцентує увагу на свободі інформації, її захисті та доступі [6].

Закон України "Про національну безпеку України" встановлює загальні засади забезпечення безпеки держави у різних сферах, включаючно із кібербезпекою та захистом критичної інфраструктури. Хоча конкретні вимоги до інформаційних систем операторів телекомунікаційного зв'язку можуть детально регулюватись іншими нормативними актами, зокрема Законом України "Про кібербезпеку", основи національної безпеки задають загальну рамку для забезпечення безпеки у цій важливій галузі [1, 2].

Закон України про національну безпеку, прийнятий у 2018 році, відіграє критично важливу роль у формуванні та виконанні політики безпеки та оборони країни. Він забезпечує інтегрований підхід до розуміння та управління національною безпекою, обороною та розвитком воєнних сил на основі міжнародних стандартів, особливо стандартів НАТО. Нижче розглянемо основні компоненти т азасади цього закону [1, 2]:

- Структура національної безпеки. Закон встановлює, що національна безпека України охоплює не лише традиційну військову безпеку, а й безпеку в таких сферах як економіка, енергетика, кіберпростір, соціальний сектор та екологія. Такий підхід забезпечує комплексність захисту від різноманітних загроз.
- Принципи демократичного контролю. Закон передбачає розвиток механізмів громадського та парламентського контролю над сектором безпеки і оборони.

Це може включати регулярний нагляд, аудит та звітність перед Верховною Радою України.

- Сумісність зі стандартами НАТО. Одним із ключових аспектів закону є адаптація українських оборонних структур до стандартів НАТО. Це важливо для підтримки сумісності і співпраці з альянсом та іншими партнерами.
- Кібербезпека. Окрема увага приділяється кібербезпеці, яка включає захист критичної інфраструктури та боротьбу з кіберзагрозами, що набувають все більшого значення у сучасному світі.
- Оборонна та військова політика. Закон передбачає реформування військових сил, підвищення іхпрофесіоналізму, а також забезпечення прозорості та ефективності військових витрат.

Закон України "Про критичну інфраструктуру" встановлює правові основи для визначення, використання, захисту та відновлення критичної інфраструктури, що є важливим для забезпечення національної безпеки, економічної стабільності, здоров'я та безпеки населення. Інформаційні системи операторів телекомунікаційного зв'язку є ключовою частиною критичної інфраструктури, оскільки забезпечують важливі комунікаційні послуги, що підтримують функціонування суспільства та економіки в цілому [3, 4].

Закон визначає критичну інфраструктуру як об'єкти або системи, які є важливими для забезпечення життєдіяльності суспільства, де невиконання функцій ,поеладених на них, або руйнування може мати серйозні наслідки. Документ розроблений для того, щоб встановити механізми ідентифікації, захисту, відновлення та регулювання критичної інфраструктури [3, 4].

Згідно цього документу вимоги до інформаційних систем операторів телекомунікаційного зв'язку включають в себе наступне [3, 4]:

1. Оператори повинні визначити та класифікувати свої інформаційні системи відповідно до їх значення та ролі в критичній інфраструктурі.
2. Встановлення заходів для захисту інформаційних систем від кіберзагроз, несанкціонованого доступу, збоїв в роботі, фізичного впливу та інших ризиків.

Це включає заходи фізичного захисту, програмного забезпечення, а також процедури управління безпекою.

3. Розробку та імплементацію планів відновлення для гарантування неперервності послуг у випадку серйозних інцидентів або збоїв в роботі інформаційних систем.
4. Оператори зобов'язані співпрацювати з уповноваженими державними органами в частині обміну інформацією про загрози, інциденти безпеки, а також участі у загальнодержавних програмах забезпечення кібербезпеки.
5. Проведення регулярних оцінок ризиків для виявлення потенційних загроз для інформаційних систем та розробка заходів щодо їх мінімізації.
6. Організація навчання та підвищення кваліфікації співробітників у сфері кібербезпеки та управління інформаційною безпекою.
7. Ведення записів про заходи безпеки, інциденти, їх аналіз та вжиті заходи реагування. Забезпечення звітності перед компетентними державними органами відповідно до законодавчих вимог.

Закон України "Про основні засади забезпечення кібербезпеки України" визначає правовий та організаційний базис для забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі. В цьому законі також визначено основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [5, 6].

Таким чином, даний закон України спрямований на забезпечення стабільної роботи та безпеки інформаційних систем, важливих для функціонування держави, економіки і суспільства. Основними цілями та положеннями цього закону є [5, 6]:

1. Визначення ключових понять та термінів таких як, "кібербезпека", "кіберінцидент", "кібератака". Такий підхід дозволяє чітко регулювати ці аспекти на законодавчому рівні.

2. Встановлення вимог до кібербезпеки накладає на всі державні органи, підприємства, установи та організації вимоги щодо забезпечення кібербезпеки їхніх інформаційних систем і ресурсів.

3. Координація зусиль у сфері кібербезпеки передбачає створення координаційних структур на державному рівні для взаємодії між усіма зацікавленими сторонами у сфері кібербезпеки, включаючи відповідні міністерства, відомства, служби безпеки та правоохоронні органи.

4. Реагування на кіберінциденти вимагає від усіх суб'єктів, що входять до критичної інфраструктури, впровадження процедур для реагування на них та відновлення роботи систем після атак.

5. Освіта та підвищення обізнаності є одним із важливих аспектів, який наголошує на необхідності проведення навчань та кампаній для підвищення обізнаності громадян і співробітників державних установ у сфері кібербезпеки.

6. Захист персональних даних. Частина закону, що підкреслює важливість захисту персональних даних у кіберпросторі та встановлює вимоги до їх обробки та зберігання.

7. Міжнародне співробітництво, як основний елемент, який підкреслює необхідність співпраці з міжнародними організаціями та іншими країнами для зміцнення глобальної кібербезпеки.

Цей закон має особливе значення для об'єктів критичної інфраструктури, оскільки забезпечує їх захист від кібератак, що потенційно матимуть руйнівні наслідки для національної безпеки та громадського порядку. Встановлення чітких правил та координація зусиль на державному рівні допомагає знизити ризики і забезпечити стабільне функціонування цих критично важливих об'єктів.

Закон України "Про захист інформації в інформаційно-комунікаційних системах" є важливим нормативно-правовим актом, який регламентує засоби та процедури захисту інформації, її обробки та зберігання в інформаційних системах. Закон встановлює вимоги до захисту даних від несанкціонованого доступу, зміни,

знищення або розкриття, забезпечуючи конфіденційність, цілісність та доступність інформації [7, 8].

До основних аспектів цього закону слід віднести [7, 8]:

- Визначення ключових понять таких як "інформаційно-комунікаційні системи", "захист інформації", "конфіденційність", "цілісність", "доступність", що дозволяє уніфікувати підходи до кібербезпеки.
- Встановлення загальних та специфічних вимог до різних категорій інформаційних систем, вимагаючи від усіх учасників забезпечувати належний захист оброблюваних даних.
- Визначення конкретних технічних та організаційних заходів, які мають бути впроваджені для захисту інформації. Це включає шифрування, аутентифікацію користувачів, регулярні аудити та інші заходи кібербезпеки.
- Встановлення відповідальності для організацій за недотримання вимог закону. Створення спеціальних органів або посад осіб, відповідальних за впровадження та контроль заходів захисту інформації.
- Визначення прав та обов'язків всіх суб'єктів, що взаємодіють із інформаційно-комунікаційними системами, включно з правами на доступ до інформації та обов'язок забезпечувати її захист.
- Конкретні санкції за порушення встановлених норм, які можуть включати штрафи, адміністративну або навіть кримінальну відповідальність.

Даний закон є фундаментом для створення безпечного кіберпростору в Україні, надаючи організаціям чіткі настанови щодо захисту інформації та управління кіберризиками. Його впровадження забезпечує зміцнення національної безпеки та підвищення довіри до електронних комунікацій в країні.

Закон України "Про захист персональних даних" встановлює правові основи захисту персональних даних громадян від незаконної обробки, а також визначає права суб'єктів персональних даних та обов'язки контролерів цих даних, серед яких і оператори телекомунікаційного зв'язку. Закон спрямований на забезпечення права

кожної особи на приватність, захист її честі та гідності у зв'язку з поширенням інформаційних технологій [9, 10].

Основною метою закону є встановлення вимог до обробки персональних даних, що включає збір, зберігання, використання, знищення та розповсюдження таких даних. Закон визначає принципи захисту персональних даних, права суб'єктів даних та вимоги до контролерів та обробників цих даних.

Вимоги до інформаційних систем операторів телекомунікаційного зв'язку є наступними[9, 10]:

- Оператори повинні отримати згоду суб'єктів персональних даних на їх обробку, крім випадків, передбачених законом. Згода має бути свідомою, конкретною та інформованою.
- Оператори зобов'язані застосовувати технічні та організаційні заходи для захисту персональних даних від несанкціонованого доступу, знищення, зміни, блокування, копіювання, поширення, а також від інших неправомірних дій.
- Доступ до персональних даних має бути обмежений лише для тих працівників оператора, які потребують цього для виконання своїх службових обов'язків.
- Суб'єкти персональних даних мають право отримувати інформацію про місцезнаходження їх даних, ціль збору та обробки, про осіб, яким передаються їх дані, та про механізм реалізації своїх прав.
- Оператор зобов'язаний виправляти неправильні або неповні персональні дані за запитом суб'єкта даних, а також знищувати або блокувати персональні дані, обробка яких не відповідає вимогам законодавства.
- Оператори повинні надавати суб'єктам персональних даних можливість здійснювати доступ до своїх даних, їх виправлення, видалення або обмеження обробки, а також гарантувати можливість відкликання згоди на обробку даних.
- Оператори несуть відповідальність за порушення вимог закону, що може включати адміністративні штрафи, цивільну або кримінальну відповідальність.

Закон України "Про інформацію" є фундаментальним нормативно-правовим актом, який визначає правові основи отримання, використання, поширення, захисту

та інші способи обробки інформації. Він встановлює загальні принципи діяльності в інформаційній сфері, права та обов'язки суб'єктів інформаційних відносин, а також механізми захисту інформації. Хоча цей закон має широке охоплення проте не є специфічним лише для телекомунікаційної галузі, він закладає основи, які є важливими для діяльності операторів телекомунікаційного зв'язку [11, 12].

Закон "Про інформацію" визначає інформацію як дані, незалежно від форми їх представлення, а також регулює відносини, пов'язані зі створенням, пошуком, отриманням, зберіганням, перетворенням, використанням та поширенням інформації. Метою закону є забезпечення свободи інформації, захисту інформаційної безпеки держави, прав та законних інтересів громадян.

До вимог до інформаційних систем операторів телекомунікаційного зв'язку відносяться такі[11, 12]:

- Оператори зобов'язані забезпечувати свободу отримання, передачі, виробництва та поширення інформації через свої мережі та послуги без необґрунтованого втручання.
- Оператори повинні вживати відповідних заходів для захисту інформації, яка передається або зберігається в їх інформаційних системах, від несанкціонованого доступу, зміни, блокування, копіювання, надання або поширення.
- Особлива увага має бути приділена захисту конфіденційної інформації, в тому числі персональних даних користувачів, з дотриманням законодавства України про захист персональних даних.
- Оператори мають забезпечувати доступність інформаційних послуг широкому колу користувачів, у тому числі особам з обмеженими можливостями.
- Попри те, що основна відповідальність за зміст інформації лежить на її авторах та розповсюджувачах, оператори телекомунікаційного зв'язку мають вживати заходів для запобігання поширенню незаконного вмісту через свої мережі.

- Оператори повинні співпрацювати з державними органами в межах чинного законодавства для забезпечення національної безпеки, боротьби з кримінальною діяльністю та забезпечення дотримання законів.

Комплексне та добре структуроване законодавство сприяє створенню ефективних механізмів виявлення, реагування та відновлення після кібератак, технологічних збоїв чи інших інцидентів, які можуть негативно вплинути на національну безпеку і економічну стабільність.

Неперервне оновлення законодавства для відповідності сучасним викликам є одним з ключових факторів в роботі ОКІ . Інноваційний підхід до правового регулювання, що включає адаптацію до новітніх технологічних реалій та міжнародних практик, зміцнює кіберстійкість країни.

1.2 Поняття розподіленої інформаційної системи – визначення та структура.

Розподілена система — це сукупність автономних комп’ютерних систем, які фізично розділені, але з’єднані централізованою комп’ютерною мережею, оснащеною програмним забезпеченням розподіленої системи. Автономні комп’ютери спілкуватимуться між кожною системою, обмінюючись ресурсами та файлами та виконуючи покладені на них завдання [13, 14, 15, 16].

Розподілена система – це програма, яка зв’язується з кількома розсіяними апаратними та програмними засобами для координації дій багатьох процесів, що виконуються на різних автономних комп’ютерах через мережу зв’язку, так що всі компоненти апаратного та програмного забезпечення співпрацювати разом для виконання набору суміжних завдань, спрямованих на досягнення спільної мети [17].

Більшість людей вважає розподілену систему і мережу комп’ютерів однаковими. Але ці два терміни означають дві різні, але пов’язані речі. Комп’ютерна мережа – це взаємопов’язана сукупність автономних комп’ютерів, які спілкуються між собою. Користувач, який використовує комп’ютерну мережу, розуміє, що він

використовує різні ресурси, що лежать на різних комп'ютерах, оскільки комп'ютерна мережа не приховує існування кількох комп'ютерів [17].

Але розподілена система, з іншого боку, створює відчуття, що користувач працює на одному однорідному більш потужному комп'ютері з більшими ресурсами. Існування кількох автономних комп'ютерів є прозорим для користувача, оскільки програма розподіленої системи, яка працює на комп'ютерах, вибирає відповідні комп'ютери та розподіляє робочі місця без спеціального втручання користувача [17].

Окрім надійності, метою побудови розподілених ІС є [17]:

- прозорість;
- відкритість;
- продуктивність;
- масштабованість.

На рисунку 1 схематично показано структура розподіленої архітектури.

Основними елементами архітектури, показаними на рисунку 1, є [17]:

- Головний центр обробки даних - відповідає за зберігання та обробку всіх даних інформаційної системи
- Центр обробки резервних даних - відповідає за відмовостійкість.
- Користувачі - клієнтське програмне забезпечення (ПЗ) за технологією «товстий клієнт».
- Сервер баз даних, сервер додатків у вузлі - займається зберіганням, обробкою всіх даних у конкретному вузлі (локальна база даних у вузлі).
- Необхідні компоненти системи розподіленої архітектури також включають:
- Телекомунікаційна мережа - забезпечує підключення та обмін даними між різними вузлами. Наприклад, Інтернет або корпоративна мережа.
- Система інформаційної безпеки - відповідає за захист кожного вузла системи.
- Сервери обміну даними - займаються реалізацією обміну даними між вузлами системи.

Очевидними перевагами цієї моделі є те, що їй не потрібно мати постійне телекомунікаційне обладнання для зв'язку з центральним рівнем. Ми вміємо

передавати пакети не тільки по телекомунікаційній мережі, а й по зовнішніх носіях. Також інтерфейс «товстого клієнта» більш ергономічний, ніж веб-інтерфейс, особливо під час масових операцій введення даних через інтерфейс користувача, хоча зараз ця перевага не є значною [17].

До переваг розподіленої системи слід віднести також віднести те, що [15, 17]:

- програми в розподілених системах є за своєю суттю розподіленими програмами;
- інформація в розподілених системах розподіляється між територіально розподіленими користувачами;
- спільне використання ресурсів (автономні системи можуть спільно використовувати ресурси з віддалених місць);
- вона має краще співвідношення ціни та якості та гнучкості;
- вона має менший час відгуку та вищу пропускну здатність;
- вона має більш високу надійність і готовність до відмови компонентів;
- вона має розширюваність, щоб системи можна було розширити у віддалених місцях, а також поступове зростання.

Поряд з позитивними характеристиками використання розподіленої архітектури є негативні. Першим недоліком є те, що кожен вузол системи має локальні бази даних, що ускладнює обмін інформацією між ними. Проте проблема не лише в обміні даними, а й в оновленні та технічному забезпеченні експлуатованих систем [17].

Наявність складних програмних елементів, таких як сервери баз даних, програми, обмін і робочі станції, не полегшує процес виконання системних завдань. Слід зазначити, що для такого елемента, як система управління базами даних, яка є однією зі складових системи, існують варіанти, як безкоштовні, так і постачальники, що в свою чергу, при виборі другого варіанту тягне за собою значні фінансові витрати на впровадження, підтримка та обслуговування [16, 17].

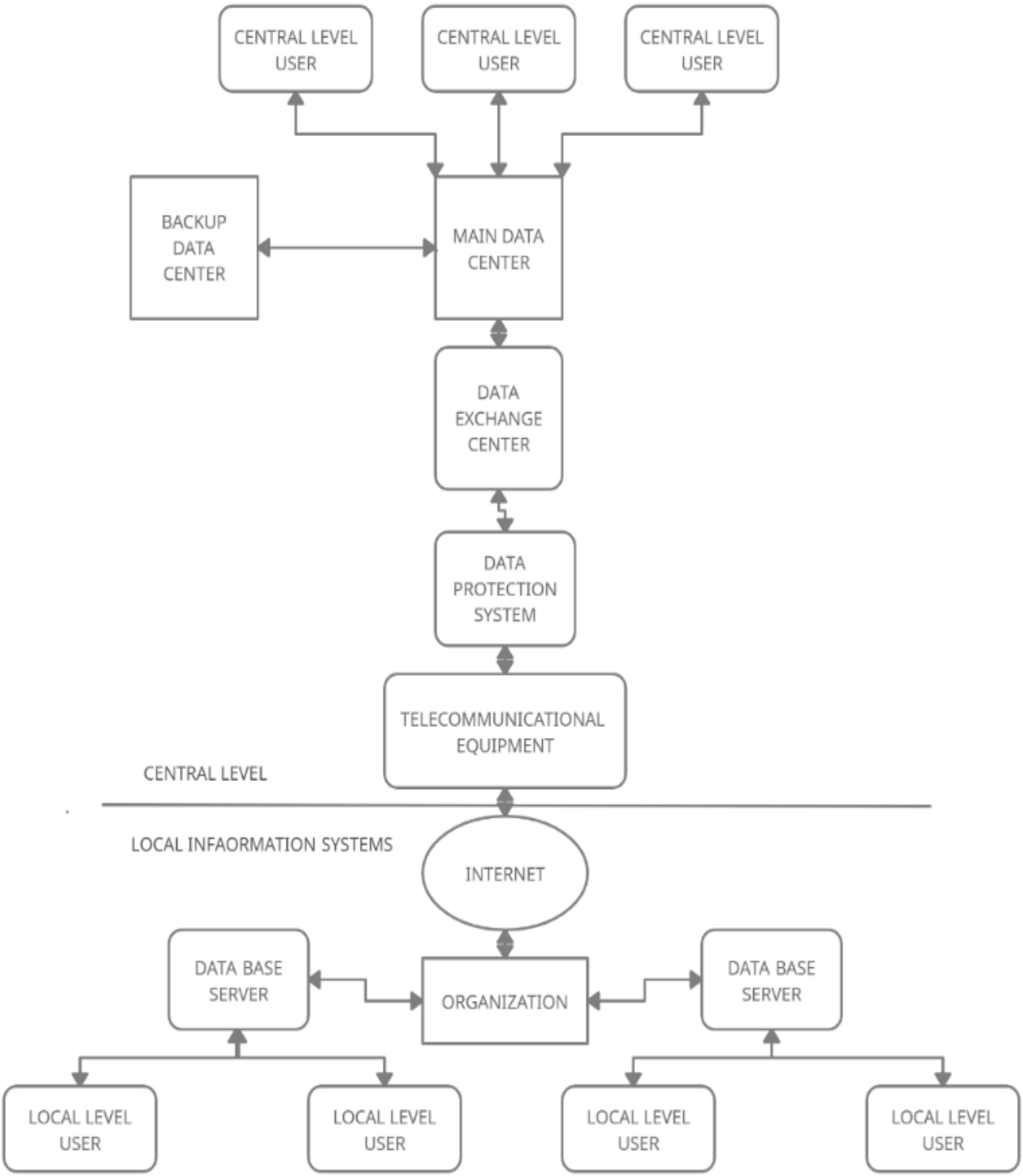

Рис. 1. Схема розподіленої архітектури інформаційної системи [17].

Необхідно йти в ногу з постійним оновленням версій усіх компонентів, що в порівнянні з централізованою архітектурою є значною статтею фінансових і тимчасових витрат. Це одне з найскладніших завдань, особливо під час надзвичайних ситуацій, і мало залежить від алгоритмів обміну даними. Інша проблема полягає в

тому, що розподілена архітектура має меншу гнучкість та ефективність під час створення нових вузлів у своїй архітектурі або їх переміщення [17].

Всі ці аспекти впливають на можливість забезпечення необхідного рівня інформаційної безпеки системи, оскільки на кожному вузлі все залежить від системного адміністратора або менеджера, який може не мати достатнього рівня відповідальності за правила роботи систем безпеки. Також виникають проблеми, коли виникає потреба розгорнути системну точку поза фізичними межами організації. Крім того, підтримання актуальності інформації, що поширюється на центральному рівні, є складною концепцією для виконавців [17].

Сьогодні використовується багато моделей і архітектур розподілених систем. Наприклад [13, 14, 18, 19, 21]:

- Клієнт-серверні системи, найбільш традиційний і простий тип розподіленої системи, включають в себе безліч мережевих комп'ютерів, які взаємодіють з центральним сервером для зберігання даних, обробки або іншої спільної мети.
- Однорангові мережі розподіляють робоче навантаження між сотнями або тисячами комп’ютерів, на яких працює одне й те саме програмне забезпечення.
- Мережі стільникового зв’язку – це розширена розподілена система, яка розподіляє навантаження між телефонами, системами комутації та пристроями, що працюють в Інтернеті.

Отже, найпоширеніші форми розподілених систем сьогодні працюють через Інтернет, передаючи робоче навантаження десяткам хмарних примірників віртуального сервера, які створюються за потреби, а потім припиняються, коли завдання виконано [13].

Характеристики розподіленої системи включають в себе [13]:

1. Спільне використання ресурсів: це можливість використовувати будь-яке обладнання, програмне забезпечення або дані будь-де в системі.
2. Відкритість: пов’язано з розширеннями та вдосконаленнями в системі (тобто

наскільки відкрито програмне забезпечення розробляється та надається іншим)

3. Одночасність: вона природно присутня в розподілених системах, які мають справу з тією самою діяльністю або функціями, які можуть виконувати окремі користувачі, які знаходяться у віддалених місцях. Кожна локальна система має свої незалежні операційні системи та ресурси.
4. Масштабованість: збільшується масштаб системи, оскільки кілька процесорів спілкуються з більшою кількістю користувачів шляхом пристосування для покращення чуйності системи.
5. Відмовостійкість: дбає про надійність системи, якщо в апаратному чи програмному забезпеченні стався збій, система продовжує працювати належним чином без погіршення продуктивності системи.
6. Прозорість: вона приховує складність розподілених систем від користувачів і прикладних програм, оскільки в кожній системі повинна бути конфіденційність.
7. Неоднорідність: мережі, комп’ютерне обладнання, операційні системи, мови програмування та реалізації розробників можуть відрізнятися між компонентами розосередженої системи.

Оскільки ідеальної системи взаємодії між мережевими елементами не існує, нижче наведені недоліки розподіленої системи:

- відповідне програмне забезпечення для розподілених систем наразі не існує;
- безпека є проблемою через легкий доступ до даних, оскільки ресурси спільно використовуються кількома системами;
- насиченість мережі може спричинити перешкоду в передачі даних, тобто якщо є затримка в мережі, користувач зіткнеться з проблемою доступу до даних;
- порівняно з однокористувальницькою системою, база даних, пов’язана з розподіленими системами, набагато складніша та складніша в управлінні;
- якщо кожен вузол у розподіленій системі намагається надіслати дані одночасно, мережа може стати перевантаженою.

В якості прикладів розподілених інформаційних систем слід розглядати наступні[20]:

- телекомунікаційні мережі, які підтримують мобільні та інтернет-мережі
- системи графічного та відео рендерингу
- наукові обчислення, такі як згортання білків і генетичні дослідження
- системи бронювання авіакомпаній і готелів
- багатокористувацькі системи відеоконференцзв'язку
- системи обробки криптовалют (наприклад, bitcoin)
- однорангові системи обміну файлами
- розподілені спільноти обчислювальних систем
- багатокористувацькі відеоігри
- глобальні розподілені роздрібні продавці та управління ланцюгами поставок

Якщо звернутися до дослідження Accenture «Вартість кіберзлочинності» за 2019 рік, за останні п’ять років кількість атак на безпеку зросла на 67%. Абсолютна оцінка небезпеки, пов’язаної з цими цифровими порушеннями, оцінюється в 5,2 трильйона доларів США протягом наступних п’яти років. Тому говорячи про розподілені інформаційні системи, їхню структуру та принципи роботи, доцільно згадати основні кібератаки, які здійснюються на них. Отже, до основних інцидентів кібербезпеки на РІС можемо віднести [21]:

1. Фішинг — це шахрайська дія, яка полягає в розсиланні спаму електронною поштою шляхом імітації законного джерела. По суті, фішинг зловживає людськими мотивами через привабливе повідомлення чи пропозицію. Агресори, як правило, вдаються до фішингових атак, зосереджуючись на величезних зібраннях, і згодом збільшують шанси того, що ймовірно кілька цілей піддадуться нападу. Звичайний випадок фішингового нападу включає агресора, який імітує особу чи фонд, і надсилає повідомлення необізнаним цілям із запитом на швидку допомогу з підключенням, доданим до листування. Невідомий клієнт підключається до підключення, що переносить його на фальшивий сайт, який виглядає як справжній сайт. Особа, не знаючи про пастку, потрапляє в неї і починає пропонувати індивідуальні тонкощі агресору, який у цей момент обшукує клієнта ще до того, як розуміє, що на нього напали.

2. Атаки соціальної інженерії. Соціальна інженерія тепер є поширеною тактикою, яку використовують кіберзлочинці для збору конфіденційної інформації користувачів. Напади соціальної інженерії мають широкий діапазон структур і можуть виконуватися в будь-якому місці, де включена співпраця людей.
3. Програми-вимагачі – це програма програмування шифрування документів, яка використовує спеціальне обчислення шифрування для шифрування записів у об’єктивній структурі. Це конкретне зловмисне програмне забезпечення, яке поширюється для шантажу готівкою від цілей, і є одним із найбільш поширених і відомих випадків кібератак. Програми-вимагачі WannaCry і Maze постійно демонструють, як зловмисне програмне забезпечення може завдати шкоди, змушуючи численні підприємства витрачати біткойни та готівку, щоб заплатити за відновлення підірваних машин і інформації.
4. Атаки ботнетів. Напади ботнетів зазвичай спрямовані на величезні організації та асоціації через величезну кількість інформації. Завдяки цій атаці програмісти можуть контролювати незліченну кількість гаджетів і торгувати ними за свої хитрі наміри. Власники ботнетів можуть звернутись до кількох тисяч комп’ютерів одночасно та наказати їм виконувати шкідливі вправи. Кіберзлочинці спочатку отримують доступ до цих гаджетів, використовуючи унікальні троянські програми для нападу на інфраструктуру безпеки комп’ютерів, а потім виконують накази та програми контролю, щоб дати їм змогу виконувати зловмисні вправи для величезного масштабу. Ці вправи можуть бути механізовані, щоб збільшити кількість синхронних нападів, якщо це було Різноманітні типи атак ботнетів можуть включати [21]:

- DDOS-атаки, які спричиняють імпровізовану програму особистого часу.
- Схвалення домовленостей про невиконання кваліфікацій (напади з використанням сертифікатів), що спонукає до захоплення облікових записів
- Напади на веб-додатки з метою отримання інформації
- Допуск агресора до гаджета та його зв'язок з організацією.

Очевидно, що будь-яка протиправна діяльність спрямована на інформаційні системи, особливо об’єктів критичної інфраструктури негативно впливають на роботу підприємств та установ. До наслідків кібератак відносять [21]:

- Фінансові збитки: кібератаки можуть призвести до фінансових збитків для компаній і окремих осіб, наприклад, до крадіжки даних кредитної картки, реквізитів банківського рахунку та криптовалюти.
- Втрата репутації: кібератаки можуть завдати шкоди репутації компанії та підірвати довіру її клієнтів, що призведе до значних фінансових втрат.
- Втрата даних: кібератаки можуть призвести до втрати критично важливих даних, таких як інформація про клієнтів, комерційна таємниця та інтелектуальна власність.
- Порушення роботи служб: кібератаки можуть порушити роботу критично важливих служб, таких як охорона здоров’я та служби екстреної допомоги, що може мати небезпечні для життя наслідки.

Тим не менш, є інструменти та підходи, які можна вжити, аби запобігти кібератакам, зокрема [21]:

- Встановлення та оновлення антивірусного програмного забезпечення та брандмауерів для запобігання несанкціонованому доступу до комп’ютерних систем і мереж.
- Навчання співробітників тому, як розпізнавати та уникати фішингових атак та інших форм кібератак.
- Використання надійних паролів і двофакторної автентифікації для захисту конфіденційних даних.
- Регулярне резервне копіювання даних для захисту від втрати даних.

1.3 Категоріювання об'єкта критичної інфраструктури

Категоріювання об'єктів критичної інфраструктури є важливим аспектом національної безпеки та управління ризиками. Говорячи про процес і критерії, які використовуються для класифікації критичних об'єктів, необхідно розібратися, що є ключовим для розуміння їх важливості для функціонування суспільства та економіки. Правильне категоріювання допомагає відповідним органам у прийнятті рішень про призначення ресурсів, планування заходів захисту та розроблення стратегій відновлення після можливих інцидентів.

Категоріювання визначається на основі низки факторів, включно з соціальною значущістю об'єкту, його роллю в економіці, ступенем залежності інших критичних секторів від цього об'єкту, а також потенційними наслідками його виведення з ладу. Такий підхід не тільки сприяє ефективному розподілу ресурсів для захисту, але й формує основу для комплексної стратегії реагування на загрози, мінімізації ризиків та швидкого відновлення в кризових ситуаціях.

1. В якості об’єкта критичної інфраструктури надалі виступатиме телекомунікаційна компанія (далі - ТК). Оператор основних послуг – підприємство «ДЕЛЬТА».

2. ТК належить до об'єкта, який надає послуги з надання електронних комунікаційних послуг [22]:

- послуга з доступу до Інтернету
- послуга з передачі даних.

3. Далі в таблиці 1 знаходимо основну послугу "Електронні комунікаційні послуги", яка відповідає підсектору "електронні комунікації". Уповноважений орган - Міністерство цифрової трансформації України [22].

4. Далі визначається рівень негативного впливу об'єкта критичної інфраструктури за секторальним критерієм (додаток 1 до Методики віднесення об'єкта критичної інфраструктури до однієї з категорій критичності). Згідно з додатком 1 ТК буде оцінюватися за критерієм пункту 7 цього додатка. У разі інциденту в ТК надання електронних комунікаційних послуг буде припинено для більшості користувачів послуг. Тому за секторальним критерієм ТК отримує 4 бали [22].

Віднесення об'єкта критичної інфраструктури до однієї з категорій критичності

Таблиця 1.1

Сектор/підсектор	Рівень негативного впливу: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $РК_i$
Послуги, що надаються підсектором електронних комунікацій - у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури призведе до припинення або зменшення обсягу надання основних послуг	втрата можливості функціонування елементів електронної комунікаційної мережі або мережевої інфраструктури або інфраструктури центру обробки даних чи обміну трафіком для України або значної її частини	збій, переривання у наданні основних послуг або обмеження доступу користувачам послуг чи сервісів для великих міст чи цілих регіонів	відсутність стабільного з’єднання, переривання сесій, зниження пропускної здатності електронних комунікаційних мереж для операторів або частини користувачів	не застосовується	**4**

				Сумарна оцінка $РК_i$	**4**

5. Далі проводиться оцінка за міжсекторальними критеріям. Оцінка проводиться шляхом вибору варіанта негативного впливу за кожним критерієм та обґрунтування вибору [22]:

1) соціальна значущість об'єкта критичної інфраструктури.

У разі припинення надання послуг ТК прямої небезпеки для життя та здоров'я людей не існує, тому $РК_1 = 0$. Також за географічним критерієм небезпеки для життя та здоров'я людей не існує $РК_2 = 0$. Заподіяння шкоди навколишньому природному середовищу не має місця. Тому $РК_4 = 0$, $РК_5 = 0$;

2) суспільна значущість об'єкта критичної інфраструктури.

ТК є великим надавачем в інфраструктурі надання електронних комунікаційних послуг. У разі припинення його функціонування може бути припинено виконання основних послуг та порушено роботу органів державної влади. Тому $РК_6 = 4$. Також здійснюється значний вплив на довіру населення до державних інституцій, як наслідок - невиконання ними відповідних функцій. Тому $РК_7 = 4$. На цей час шкода іншим державам - партнерам України не може бути завдана, але можуть бути порушення міжнародних угод - $РК_8 = 2$;

3) економічна значущість об'єкта критичної інфраструктури.

Припинення надання послуг КНЕДП призведе до заподіяння збитків об'єкту критичної інфраструктури. Збитки державному бюджету посередні. Збитки місцевим бюджетам також незначні. Тому $РК_9 = 4$, $РК_{10} = 3$, $РК_{11} = 1$;

4) взаємозв'язок між об'єктами критичної інфраструктури.

Переривання надання послуг ТК може вплинути на роботу інших надавачів електронних довірчих послуг. Водночас переривання надання послуг КНЕДП призведе до порушень надання послуг в інших секторах, де діяльність пов'язана з використанням електронних комунікаційних послуг. Тому $РК_{12} = 3$, $РК_{13} = 4$;

5) значущість об'єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни.

Припинення роботи ТК може вплинути на функціонування пунктів управління (ситуаційних центрів). Тому $РК_{14} = 4$. Зниження показників державного оборонного замовлення не очікується. Тому $РК_{15} = 0$, $РК_{16} = 0$.

Методики віднесення об'єкта критичної інфраструктури до однієї з категорій критичності

Таблиця 1.2

<table>
<tr><td>Негативний вплив</td><td>Рівень негативного впливу: катастрофічні наслідки (4 бали)</td><td>Рівень негативного впливу: критичні наслідки (3 бали)</td><td>Рівень негативного впливу: значні наслідки (2 бали)</td><td>Рівень негативного впливу: незначні наслідки (1 бал)</td><td>Рівень негативного впливу: надто малий (0 балів)</td><td>Оцінка $РК_i$</td></tr>
<tr><td colspan="7">І. Соціальна значущість об'єкта критичної інфраструктури</td></tr>
<tr><td rowspan="3">Заподіяння шкоди життю та здоров'ю людей</td><td colspan="6">Кількість населення, що може постраждати</td></tr>
<tr><td>небезпека для життя або здоров'я більш як 75000 людей</td><td>небезпека для життя та здоров'я більш як 5000 людей</td><td>небезпека для життя або здоров'я більш як 50 людей</td><td>небезпека для життя або здоров'я менш як 50 людей</td><td>не критично</td><td>$РК_1 = 2$</td></tr>
<tr><td colspan="6">Географічний масштаб</td></tr>
</table>

	небезпека для життя та здоров'я мешканців на території однієї АБО більш як однієї області, АБО на території трьох та більше міст обласного значення	небезпека для життя та здоров'я мешканців на території однієї області АБО міського району міста обласного центру, АБО на всій території одного міста обласного значення	небезпека для життя та здоров'я для людей на території об'єкта та для мешканців, що проживають у безпосередній близькості до розміщення об'єкта	небезпека для життя та здоров'я людей на території об'єкта	не критично	$РК_2 = 4$
Заподіяння шкоди навколишньому природному середовищу	Економічні втрати					
	нанесені збитки більш як на 30 млн грн	нанесено збитків більш як на 18 млн грн	нанесено збитків більш як на 2 млн грн	нанесено збитків менше як на 2 млн грн	не критично	$РК_3 = 0$
	Географічний масштаб					
	шкідливий вплив розповсюджується на територію більш як однієї області	шкідливий вплив розповсюджується на територію однієї області АБО на територію більш як одного міста	шкідливий вплив розповсюджується на територію одного міста	шкідливий вплив розповсюджується на територію об'єкта	не критично	$РК_4 = 0$

	АБО на території не менш як трьох міст обласного значення	обласного значення	обласного значення	інфраструктури		
	Час					
	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом більш як одного року	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від півроку до одного року	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від одного місяця до півроку	шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом одного місяця	не критично	$РК_5 = 0$
II. Суспільна значущість об'єкта критичної інфраструктури						

Припинення або порушення функціонування державних органів	припинення або порушення функціонування Верховної Ради України, Кабінету Міністрів України, Конституційного Суду України, Верховного Суду, а також Офісу Президента України, Ради національної безпеки та оборони України	припинення або порушення функціонування центральних органів виконавчої влади та облдержадміністрацій	припинення або порушення роботи районних держадміністрацій, територіальних органів центральних органів виконавчої влади	припинення або порушення роботи органів місцевого самоврядування	не критично	$РК_6 = 4$
Негативний вплив на довіру людей до державних інституцій	матиме значний вплив	матиме великий вплив	матиме середній вплив	матиме незначний вплив	не критично	$РК_7 = 4$

Шкода інтересам інших держав - партнерів України	так, принаймні двом країнам або порушення умов міжнародного договору, укладеного від імені України	так, принаймні одній країні або порушення умов міжнародного договору, укладеного від імені Уряду України	можливі негативні наслідки для інших держав, але їх вплив навряд чи буде значним	держави не постраждають або немає порушення умов міжнародного договору, укладеного від імені міністерства, іншого центрального органу виконавчої влади, державного органу	не критично	$РК_{8}$ = 2
III. Економічна значущість об'єкта критичної інфраструктури						
Заподіяння збитків об'єкту інфраструктури (у відсотках прогнозованого обсягу річного	більш як 15 відсотків	від 10 до 15 відсотків	від 5 до 10 відсотків	менш як 5 відсотків	не критично	$РК_{9}$ = 4

доходу за всіма видами діяльності)						
Заподіяння збитків державному бюджету (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	більш як 0,1 відсотка	від 0,1 до 0,05 відсотка	від 0,05 до 0,01 відсотка	менш як 0,01 відсотка	не критично	$РК_{10} = 3$
Заподіяння збитків місцевим бюджетам (зниження прибутків бюджету у відсотках прогнозованого	більш як 0,1 відсотка	від 0,1 до 0,05 відсотка	від 0,05 до 0,01 відсотка	менш як 0,01 відсотка	не критично	$РК_{11} = 3$

річного прибутку бюджету)						
IV. Взаємозв'язок між об'єктами критичної інфраструктури						
Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує надання таких самих основних послуг	матиме негативний вплив (якщо так, вкажіть який)			не матиме впливу	не критично	$РК_{12}$ = 4

Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що надає інші основні послуги	матиме негативний вплив (якщо так, вкажіть який)			не матиме впливу	не критично	$РК_{13}$ = 4
V. Значущість об'єкта критичної інфраструктури для забезпечення оборони країни та безпеки держави						
Припинення або порушення (невиконання встановлених показників) функціон	припинення або порушення функціонування пунктів управління Верховного Головнокомандувача Збройних Сил,	припинення або порушення функціонування пунктів управління або ситуаційного центру центральних органів виконавчої влади, пунктів	припинення або порушення функціонування обласної державної адміністрації,	територіальних органів центральних органів виконавчої влади	не критично	$РК_{14}$ = 4

ування пунктів управління (ситуаційного центру), що оцінюється на рівні (значущості) пункту управління або ситуаційного центру	Головнокомандувача Збройних Сил, Начальника Генерального штабу Збройних Сил або ситуаційного центру Офісу Президента України, Кабінету Міністрів України, Ради національної безпеки та оборони України	управління Сухопутних військ, Повітряних Сил, Військово-Морських Сил, десантно-штурмових військ, сил спеціальних операцій, Національної гвардії, Держприкордонслужби	ситуаційних центрів			
Зниження показників державного оборонно	Зниження обсягів продукції (робіт, послуг) у заданий період часу (у відсотках)					
	більш як 15 відсотків	від 10 до 15 відсотків	від 5 до 10 відсотків	менш як 5 відсотків	не критично	$РК_{15}$ = 4
	Збільшення часу виготовлення продукції (робіт, послуг) із заданим обсягом (відсотків встановленого часу на виготовлення продукції)					

го замовлення	більш як 40 відсотків	від 10 до 40 відсотків	від 5 до 10 відсотків	менш як 5 відсотків	не критично	$РК_{16}$ = 0
Сумарна оцінка $РК_i$						43

6. Визначення категорії критичності.

Після проведення оцінювання необхідно хвернутися до розрахунків. Розраховується узагальнена нормована оцінка рівня критичності за наступною формулою [22]:

$$\mathbf{РК_{ОКІ} = \frac{\Sigma РК_i}{\Sigma РК_{max}}\ (1.1)}$$

де $РК_{ОКІ}$ - узагальнена нормована оцінка рівня критичності об’єкта критичної інфраструктури [22];

$РК_i$ - сума балів, які отримав об’єкт критичної інфраструктури за всіма критеріями критичності [22];

$РК_{max}$ - максимальна можлива сума балів (розраховується виходячи з того, що об’єкт отримує максимальні бали за всіма критеріями оцінки рівня негативного впливу) [22].

$РК_{ОКІ}$ = 43/68 = 0.63235294

Відповідно до правила правила визначення критичності об’єкта:

- І категорія критичності, якщо 0,8 < РК ОКІ ≤ 1;
- **ІІ категорія критичності, якщо 0,63 < РК ОКІ ≤ 0,8;**
- ІІІ категорія критичності, якщо 0,37 < РК ОКІ ≤ 0,63;
- IV категорія критичності, якщо 0,2 < РК ОКІ ≤ 0,37;
- об'єкт не є критичним, якщо РК ОКІ ≤ 0,2.

Таким чином ТК слід бути віднесено до ІІ категорії критичності. Це достатньо високий рівень критичності для об’єкту, аби говорити про важливість його стабільного функціонування.

Описаний вище процес категоріювання забезпечує не лише розуміння важливості кожного об'єкта для національної безпеки та стабільності, а й формує основу для розроблення ефективних стратегій їх захисту та відновлення.

Висновки до розділу 1

Через зростаючу залежність сучасного суспільства від функціонування різноманітних систем критичної інфраструктури, точне категоріювання є одним з ключових факторів у плануванні безпекових заходів. Воно допомагає визначити пріоритети для ресурсних асигнувань, розробки заходів захисту та реагування на кризи. Крім того, ефективна інтеграція категоріювання у загальнодержавні системи управління ризиками може значно знизити потенційні втрати від природних катастроф, техногенних аварій, або кібератак.

Слід зазначити, що зі зростанням кількості кібератак на критичні об’єкти інфраструктури, зокрема в галузі телекомунікацій, слід постійно оновлювати не лише рішення, які вроваджуються, але і підходи до оцінювання рівня критичності об’єктів для яких вроваджуються ці рішення. Це дозволить гнучкіше підходити до реалізації безпекових задач та ефективніше використовувати технології для захисту національно важливих активів у майбутньому.

РОЗДІЛ 2
МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ’ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ

У сучасному світі, де інформаційні технології стають все більш інтегрованими у всі аспекти життя суспільства, роль телекомунікаційних операторів, які управляють розподіленими інформаційними системами, значно зростає. Ці системи не тільки сприяють ефективному зв'язку та обміну даними між користувачами по всьому світу, але й становлять життєво важливу складову критичної інфраструктури нації. Вони підтримують функціонування важливих секторів економіки, від енергетики до фінансів, від охорони здоров'я до національної оборони, гарантуючи безперебійну роботу критично важливих служб.

У зв'язку з постійним зростанням різноманітних загроз, таких як несанкціонований доступ, кібератаки, технічні неполадки, а також природні катастрофи, питання захисту інформаційних систем набуває особливої актуальності. Забезпечення ефективного захисту цих систем є критично важливим для підтримки національної безпеки та загальної стабільності держави. Захист інформації від потенційних загроз стає ключовим завданням, яке вимагає розробки та впровадження комплексних заходів безпеки.

2.1 Вразливості об’єктів критичної інфраструктури

Об'єкти критичної інфраструктури представляють собою широкий спектр потенційно вразливих точок, які можуть бути використані злочинцями для нанесення шкоди цим життєво необхідним системам. Важливість проведення глибокого аналізу цих вразливостей не може бути недооцінена, оскільки наслідки таких атак можуть бути руйнівними для національної безпеки, економіки та суспільного здоров'я.

Критична інфраструктура, включно з енергетичними об'єктами, транспортними мережами, системами водопостачання, телекомунікаційними послугами та медичними установами, є фундаментом для стабільного та безпечного функціонування суспільства. Їхні потенційні слабкі місця можуть охоплювати широкий спектр від фізичних та технологічних аспектів до кібернетичних загроз та людських помилок.

Впровадження комплексних заходів безпеки, а також постійне оновлення і адаптація захисних стратегій є критично важливими для забезпечення довгострокової стійкості та надійності ОКІ.

2.1.1 Технічні вразливості

Технічні вразливості представляють собою окрему частину, до яких можна віднести наступні категорії чинників[23]:

- Недоліки мережевих протоколів - виккористання застарілих або не належним чином налаштованих мережевих протоколів може дозволити нападникам проводити атаки типу "man-in-the-middle".
- Вразливості програмного забезпечення - баги або несправності у програмному коді, які забезпечують зловмисникам можливість експлуатації системи, наприклад через SQL ін'єкції, XSS атаки або відмови в обслуговуванні (DoS).
- Застосування застарілого апаратного забезпечення - старе або не підтримуване апаратне забезпечення потенційно може містити вразливості, які не підлягають виправленню через відсутність оновлень безпеки.

Атаки «людина посередині» (MITM) - це поширений тип кібератак, що дозволяє зловмисникам перехоплювати спілкування між двома об'єктами. Ця атака відбувається під час легітимної комунікації між двома хостами, дозволяючи зловмиснику "прослуховувати" розмову, яку вони зазвичай не мають доступу прослухати, отже, вона також відома як атака "людина посередині" [23, 24б 25].

До атак «людина посередині» можна відносити наступні [23]:

- Захоплення сесії за якої зловмисник стає між комп'ютером жертви та веб-сервером, шляхом зламу мережі Wi-Fi або за допомогою спеціального програмного забезпечення. Атакувальники контролюють дані, які передаються. Якщо веб-сайт не використовує безпечне шифрування, зловмисник може легко прочитати ці дані, включаючи файли cookie, які містять ідентифікатор сесії. За допомогою цих захоплених файлів cookie зловмисник може видачі себе за жертву та отримати несанкціонований доступ до веб-додатку, обійшовши ідентифікаційні дані.
- Підробка ARP (протокол розпізнавання адрес) - метод для комп'ютерів у локальній мережі дізнатися фізичну (MAC) адресу один одного. Під час підробки ARP хакер надсилає фальшиві ARP-повідомлення, щоб обманом змусити комп'ютери пов'язувати MAC-адресу хакера з IP-адресою, якій він насправді не належить. Таким чином дані, призначені для однієї машини, замість цього потрапляють до хакера.
- Підробка DNS - хакер втручається в систему, перенаправляючи доменне ім'я на іншу IP-адресу, зазвичай на шкідливий веб-сайт або сервер. Таким чином, коли відбувається відвідування сайту, який, здавалося б, заслуговує на довіру, фактично клієнта спрямовують в інше місце. Головна мета - залучити користувачів взаємодіяти з підробленим сайтом, де вони можуть розкрити конфіденційну інформацію.
- Захоплення SSL/TLS - (Secure Sockets Layer/Transport Layer Security) - це протоколи, які шифрують дані між вашим веб-браузером і сервером. У цьому типі атаки хакер намагається взламати або обійти протоколи безпеки, які захищають зв'язок між вашим комп'ютером і сервером - SSL або його оновлену версію TLS. Роблячи це, вони можуть перехоплювати або змінювати дані, які передаються. Одним із поширених способів зробити це є використання слабких місць у налаштуваннях SSL/TLS, застосування застарілих версій або використання неправильної конфігурації.

- Підробка HTTP/HTTPS - зловмисник створює фальшиву веб-сторінку, яка точно імітує надійний сайт. Користувачі непомітно розголошують конфіденційну інформацію, вважаючи, що вони спілкуються з легітимним джерелом.

Тільки для атаки «людина посередині» можуть бути задіяні низка мережевих протоколів різних рівнів, що свідчить про необхідність відповідального ставлення до вибору та налаштування мережевих протоколів за допомогою якиї відбуватименься взаємодія елементів системи та обмін даними [27].

Критичні вразливості програмного забезпечення, слід розглядати – як слабкі місця або недоліки в програмах або операційних системах, якими можуть скористатися зловмисники, щоб отримати неавторизований доступ, пошкодити або викрасти дані або спричинити пошкодження пристрою чи мережі.

Вони можуть виникати, наприклад, через недостатню перевірку введених даних, некоректну обробку файлів, неправильно налаштовані механізми безпеки або помилки в самому програмному коді [27].

Нівелювання важливості оновлення апаратного забезпечення може призвести до низки неприємних, а деяких випадках навіть фатальних наслідків. Нижче на мою думку описані найбільш імовірні з них [28, 29]:

1. Порушення безпеки даних. Після того, як виробник оголошує про завершення життєвого циклу продукту, існує ймовірність, що виправлення безпекових уразливостей, патчі та оновлення мікропрограм для продукту будуть зменшені або скасовані. Ці прогалини в підтримці створюють значні ризики для безпеки підприємства та залишають мережу компанії відкритою для кібератак зловмисників.
2. Зниження продуктивності. Використання застарілого обладнання може значно знизити продуктивність. По-перше, старе обладнання з більшою ймовірністю вийде з ладу через свій вік, порушуючи роботу. Це може призвести до пошкоджень та дорогих перерв у роботі. По-друге, визначення відповідної заміни займає час та неодмінно впливає на середній час відновлення послуг (MTTR).

3. Вищі витрати на технічне обслуговування. У багатьох випадках, коли продукт перебуває в статусі EOL, запасні частини також припиняються. Це означає, що з часом пошук запасних частин або аксесуарів стає все складнішим і дорожчим. Іноді компанії залучають сторонніх консультантів та підтримуючі команди, які розробляють "пластирні" рішення для більш складних проблем. Це також може зробити використання EOL рішення дорожчим у довгостроковій перспективі, ніж оновлення до новішого обладнання.
4. Проблеми з масштабованістю. Обладнання EOL часто має обмежені можливості адаптуватися до змінних потреб у центрі обробки даних. IT-спеціалісти повинні використовувати нові та вдосконалені обладнання, оскільки обсяг та складність операцій центру обробки даних зростають. Це дозволяє їм використовувати технологічні інновації в таких сферах, як обробка даних, енергоефективність та модульність.
5. Невідповідність. Щоб IT-інфраструктура відповідала нормативним стандартам, обладнання повинно відповідати необхідним рівням захисту та функціональності, які вимагає кожна організація. Це особливо важливо для центрів обробки даних, що працюють у державних і фінансових установах, де порушення даних може призвести до серйозних правових наслідків і штрафів.

2.1.2 Організаційні вразливості

Неналежне управління доступом до інформаційних ресурсів і систем може призвести до того, що неавторизовані особи отримають доступ до конфіденційної інформації. Це може статися через слабке виконання політик управління доступом, відсутність сегментації мережі та неефективне використання принципу найменшого привілею. Недоліки в управлінні доступом включають в себе [30, 31]:

- Слабкі або легко вгадувані паролі. Зазвичай це паролі, які легко вгадати або зламати. Вони є серйозною вразливістю, оскільки дозволяють неавторизованим користувачам отримувати доступ до системи або даних.

- Відсутність багатофакторної аутентифікації. Вона вимагає від користувачів надання декількох форм ідентифікації (таких як пароль і відбиток пальця або маркер безпеки), може поліпшити контроль доступу, ускладнивши доступ неавторизованим користувачам.
- Неправильно налаштовані списки контролю доступу. В цій ситуації списки контролю доступу (ACL) визначають, які користувачі або групи можуть отримувати доступ до певних ресурсів, таких як файли або каталоги. Неправильно налаштовані списки управління доступом можуть дозволити неавторизованим користувачам отримати доступ до конфіденційних даних.
- Недостатні або неправильні дозволи. Користувачам повинен бути наданий найменший рівень привілеїв у системі, необхідний для їх виконання робочих функцій. Надання користувачам більшої кількості привілеїв, ніж їм необхідно, може збільшити ризик несанкціонованого доступу або випадкового витоку даних.

Ще однією причиною може бути недостатнє шифрування даних. Наявність даних, що передаються або зберігаються без адекватного шифрування, відкриває можливість для зловмисників легко отримати доступ до цих даних. Слабке шифрування або відсутність його може бути результатом застарілих технологій або недоліків в реалізації шифрувальних алгоритмів [32].

Дослідження під назвою Operationalizing Encryption and Key Management нещодавно було опубліковано Fortanix Inc. і проведено Enterprise Strategy Group (ESG). Висновки показали, що відсутність шифрування є основним фактором втрати конфіденційних даних, навіть якщо впевненість у криптографічних можливостях є високою [32].

Опитування показало, що 90% респондентів погодилися з тим, що шифрування має позитивний вплив на різні аспекти безпеки їх мережі, безпеки даних і загальної безпеки, причому понад 50% сказали, що воно має значний позитивний вплив у кожній із цих областей. У звіті також виявлено, що підприємства хочуть шифрувати свої дані, але часто не знають, як. Відсутність відповідного персоналу з кібербезпеки

та досвіду призводить до плутанини щодо того, де і коли застосовувати шифрування, ускладнює управління та труднощі з оцінкою кібербезпеки. Подібним чином відсутність шифрування залишалася головною причиною втрати даних для майже 33% респондентів, а 25% зіткнулися з втратою даних через порушення політики, наприклад малий розмір ключа [32].

Недостатній моніторинг систем може призвести до того, що інциденти безпеки не будуть виявлені або на них буде зреаговано занадто пізно. Причиною можуть стати недостатні інструменти моніторингу, відсутність аналізу логів або відсутність спеціалізованого персоналу.

І хоча критичність безперервного моніторингу безпеки не можна недооцінювати, процес побудови успішного плану постійного моніторингу непростий [33].

Нижче наведено п’ять компонентів, які слід врахувати та виконати під час складання плану постійного моніторингу безпеки [33]:

1. Визначити дані, які потрібно захистити.
2. Створити процес для регулярного виправлення вразливостей безпеки.
3. Переконатися, що постійно відстежуються всі кінцеві точки.
4. Створити процес для постійного визначення змін у стандартній поведінці користувачів в організації.
5. Встановити програмне забезпечення для безперервного моніторингу безпеки для моніторингу третіх сторін.

2.1.3 Модель загроз та порушника

Модель загроз – абстрактний структурований опис загроз. Модель порушника– це всебічна структурована характеристика порушника, яка використовується сумісно з моделлю загроз для розробки політики безпеки інформації. Ці моделі дозволяють організаціям зрозуміти, проти яких загроз вони повинні захистити свої активи, та розробити відповідні заходи захисту [34, 35, 36].

Модель загроз - документ, що використовується для [37]:

- аналізу захищеності підприємства від загроз безпеки інфокомунікаційної мережі (ІКМ) в ході організації та виконання робіт по забезпеченню безпеки;

- розробки системи захисту (ІКМ), що забезпечує нейтралізацію передбачуваних загроз з використанням методів і способів захисту мережі, передбачених для відповідного класу підприємства;

- проведення заходів, спрямованих на запобігання несанкціонованого доступу до (ІКМ) і/або передачі їх особам, які не мають права доступу до такої інформації;

- недопущення впливу на технічні засоби підприємства, в наслідок якого може бути порушено їх функціонування;

- контролю забезпечення рівня захищеності інфокомунікаційної мережі.

У моделі загроз представлено опис структури і складу підприємства, класифікацію потенційних порушників, оцінку вихідного рівня захищеності, аналіз загроз безпеки мережі [37].

Аналіз загроз безпеки системи (ЗБС) включає [37]:

- опис загроз;
- оцінку ймовірності виникнення загроз;
- оцінку можливості бути реалізованим загроз;
- оцінку небезпеки загроз;
- визначення актуальності загроз.

Зовнішними нападниками виступають:

- Кіберзлочинці – це індивідуальні хакери або організовані групи, які шукають фінансову вигоду через вимагання, крадіжку конфіденційної інформації або інші шахрайські дії.
- Державні агенти - спонсоровані державою особи, які займаються кібершпіонажем, маніпулюванням даними або саботажем для досягнення політичних, економічних чи військових цілей.

Внутрішні загрози можна поділити на 2 типи:

- Недобросовісні співробітники - особи з доступом до внутрішніх систем, які можуть свідомо або через недбалість спричинити витік або знищення даних.
- Співробітники третіх сторін – це партнери або підрядники, які мають обмежений доступ до систем та даних і можуть становити ризик через недостатній контроль або неналежне управління доступом.

Автоматизовані загрози поділяються на шкідливе програмне забезпечення та ботнети. В якості шкідливого ПЗ виступають віруси, трояни, ransomware, які можуть автоматично поширюватись і завдавати шкоди системам. Ботнети ж, - це мережі заражених пристроїв, які можуть бути використані для проведення масштабних атак типу DDoS або для розподілених зусиль злому.

Мотивація порушників може бути варіюватися від обставин, проте найбільш розповсюдженими серед них є:

- Фінансова вигода - пряме збагачення через крадіжку, шахрайство, або продаж доступу до інформації.
- Політичний, соціальний вплив – такі собі спроби змінити громадську думку або політичні процеси через маніпуляції даними чи інформаційні атаки.
- Репутаційний шкода – метою якої є завдання шкоди репутації компанії через витік даних або інші дії, які підривають довіру клієнтів та партнерів.

Розробка ефективної моделі загроз і порушників вимагає глибокого розуміння потенційних ризиків, вразливостей і мотивацій, які можуть впливати на безпеку організації. Знання цих аспектів дозволяє зосередитися на найбільш критичних точках захисту, розробляючи комплексні заходи безпеки.

Модель загроз допомагає організаціям ідентифікувати, оцінити та розробити стратегії захисту проти потенційних загроз. Нижче наведено модель загроз для PIC, розділену на різні категорії, які включають потенційних зловмисників, їхні мотиви, можливі вектори атак та ресурси, які вони можуть використовувати для реалізації своїх намірів [35].

Для ідентифікації та аналізу загроз можна використовувати таблицю 2.1:

Таблиця 2.1

Категорія	**Потенційні Загрози**	**Мотивація**	**Вектори Атаки**	**Ресурси Зловмисників**
Зовнішні нападники	Хакери/кіберзлочинці	Фінансова вигода/шпіонаж	Мережеві атаки/фішинг/веб-злfм	Просунуте програмне забезпечення/ботнети
Внутрішні загрози	Недобросовісні співробітники	Незадоволеність, особиста вигода	Інсайдерські зловживання, злам	Доступ до внутрішніх систем
Автоматизовані атаки	Віруси/трояни	Розповсюдження шкоди	Розповсюдження шкідливого ПЗ	Автоматизоване ПЗ/скрипти

Модель порушника (табл. 2.2) допомагає ідентифікувати характеристики та можливі стратегії атаки, які можуть використовувати потенційні зловмисники проти розподіленої інформаційної іистеми (РІС) на об'єкті критичної інфраструктури (ОКІ). Ця модель охоплює типи зловмисників, їхні мотивації, цілі, а також типові та можливі методи атаки [34, 35, 36].

Таблиця 2.2

Тип Зловмисника	**Опис**	**Мотивація**
Зовнішні агенти	Хакери, кіберзлочинці, спонсоровані державою агенти, які можуть використовувати складні техніки для здобуття доступу до системи.	Фінансова вигода, шпіонаж, геополітичний вплив.
Внутрішні співробітники	Співробітники організації, які мають доступ до внутрішніх ресурсів та можуть виконувати	Особиста вигода, помста, політичні

	несанкціоновані дії через особисті образи, невдоволення або намір отримати вигоду.	або соціальні переконання.
Автоматизовані загрози	Шкідливе програмне забезпечення, включаючи віруси, трояни, шпигунське ПЗ, яке автоматично розповсюджується і виконує зловмисні дії.	Розповсюдження шкоди, здобуття контролю над системами, крадіжка даних.

Нижче на рис.2 наведено модель порушника безпеки інформації залежно від мотивів, кваліфікації та озброєності [38].

Рисунок 2 - модель порушника безпеки інформації

Тим не менш, якщо говорити про мотиви, цілі і методи, дій порушників безпеки інформації можна розділити на чотири категорії [38]:

1. шукачі пригод;
2. ідейні хакери;
3. хакери-професіонали;

4. ненадійні (неблагополучні) співробітники

Шукач пригод, як правило, це студент, у якого рідко є продуманий план атаки. Він вибирає мету випадковим чином і зазвичай відступає, зіштовхнувшись із труднощами. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Своїми перемогами такий шукач пригод ділиться тільки зі своїми близькими друзями-колегами [38].

Ідейний хакер – це той же шукач пригод, але більш митецький. Він уже вибирає собі конкретні цілі (хости та ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення web-сервера або, у більш рідких випадках, блокування роботи ресурсу, що атакуються. Порівняно з шукачем пригод, ідейний хакер розповідає про успішні атаки набагато більш широкій аудиторії, звичайно розміщаючи інформацію на хакерському web-вузлі або в конференціях Usenet [38].

Хакер-професіонал має чіткий план дій і націлюється на конкретні ресурси. Його атаки добре продумані й звичайно здійснюються в кілька етапів. Спочатку він збирає попередню інформацію (тип операційної системи (ОС), сервіси, що надаються, заходи захисту, що застосовуються). Потім він становить план атаки з урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Провівши атаку, він одержує закриту інформацію, і нарешті, знищує всі сліди своїх дій. Такий атакуючий професіонал звичайно добре фінансується й може працювати самому або в складі команди професіоналів [38].

Ненадійний (неблагополучний) співробітник своїми діями може доставити стільки ж проблем (буває й більше), скільки промисловий шпигун, до того ж його присутність звичайна складніше виявити. Крім того, йому доводиться долати не зовнішній захист мережі, а тільки, як правило, менш твердий внутрішній захист. Він не так витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилки й тим самим може видати свою присутність. Однак у цьому випадку небезпека його несанкціонованого доступу до корпоративних даних багато вище, чим

будь-якого іншого зловмисника. Перераховані категорії порушників безпеки інформації можна згрупувати за їх кваліфікацією: початківець (шукач пригод), фахівець (ідейний хакер, ненадійний співробітник), професіонал (хакер-професіонал) [38].

У підсумку можна говорити про те, що вразливості ОКІ не обмежуються технічними аспектами, адже включають широкий спектр організаційних і процесуальних питань, що потребують комплексного підходу до безпеки.

Ефективне управління ризиками вимагає не лише технологічних вдосконалень, але й зміцнення організаційних процесів, поліпшення культури безпеки та навчання персоналу.

Розробка детальної моделі загроз допомагає ідентифікувати потенційні джерела інцидентів та оцінювати ризики на основі реального контексту використання об'єктів інфраструктури. Це, в свою чергу, сприяє більш цілеспрямованому застосуванню захисних заходів.

Стійкість критичної інфраструктури до сучасних загроз залежить від постійного оновлення і адаптації стратегій безпеки, враховуючи зміни у технологіях, загрозах і тактиці потенційних порушників. Таким чином слід
зміцнювати нормативну базу, залучати новітні технологічні рішення для кіберзахисту, розробляти і впроваджуватия комплексні плани навчання та реагування на інциденти, а також створювати міжвідомчі координаційні центри для керування реагуванням на кризові ситуації.

2.2 Інциденти на об’єктах критичної інфраструктури

Розглядаючи об’єкти критичної інфраструктури хотілося б окремо виділити таку сферу, як телекомунікації. Саме галузь телекомунікацій на поточний момент є однією з пріоритетних цілей хакерів. Лише в період з 2022-2024 по критичній інформаційній інфраструктурі України було завдано низку атак [39]:

- 14 січня 2022 року. Атаки на державні та банківські сайти. Приблизно 22

державні органи та 70 українських сайтів були атаковані з дефейсом, що засуджує український націоналізм. Атака була спрямована на залякування та можливе компрометування Польщі, хоча мала ознаки російського походження.

- 15 лютого 2022 року. Масштабна DDoS-атака. Сайти майже 15 банків і держорганів були недоступні протягом п’ятьох годин, що оцінювалося як найбільша кібератака в історії України.
- 23-24 лютого 2022 року. Атаки напередодні вторгнення. Масштабна кібератака порушила супутниковий доступ до інтернету. Хакери відключили модеми, які зв’язуються із супутником KA-SAT компанії Viasat, що забезпечують доступ до інтернет для клієнтів у Європі, зокрема в Україні. Відбулися атаки на державні та банківські сайти, а також на інші важливі інфраструктурні об’єкти, спричинені вірусом HermeticWiper. Атаки були спрямовані на підготовку до військового вторгнення.
- 8 квітня 2022 року. Кібератака на об’єкти енергетики України. За словами українських чиновників, атака мала початися ввечері 8 квітня, коли люди поверталися додому з роботи, і могла унеможливити їхнє повсякденне життя або отримання доступу до інформації про перебіг війни. Якби атака була успішною, вона позбавила б електроенергії приблизно 2 млн людей і ускладнила б відновлення електропостачання.
- 13 травня 2022 року. Масова кібератака на мережі львівської мерії. Під час кібератаки на мережі мерії викрали частину робочих файлів міста та опублікували її на ворожих телеграм-каналах.
- 23 червня 2022 року. Російські спецслужби атакували сервер електронної пошти Миколаївської ОДА. Внаслідок цього вони отримали доступ до поштової скриньки пресслужби облдержадміністрації.
- 1 липня 2022 року. Кібератака на ІТ-інфраструктуру групи ДТЕК. Це кібератака на найбільшу приватну енергетичну компанію України, яку здійснили разом із ракетними ударами по Криворізькій електростанції. Кібератака UAC-0056 на державні організації України з використанням Cobalt Strike Beaco.

- Фішингові атаки: розсилання фішингових листів українським військовим та їхнім родичам, а також посадовцям, які мали на меті крадіжку інформації.

Від лютого 2022 року відбулося орієнтовно 10 тис. кібератак та критичних інцидентів, які зафіксувала лише СБУ. Це 10-15 спроб здійснити щось серйозне щодня, і кібератаки стали більш витонченими [39].

Уранці 12 грудня 2023 року найбільший український оператор «Київстар» зазнав потужної хакерської атаки, внаслідок якої мільйони абонентів втратили доступ до послуг мобільного зв'язку та інтернету [39].

Відповідальність за атаку взяла на себе російська хакерська група «Солнцепек», яка, ймовірно, використала скомпрометований обліковий запис одного зі співробітників компанії. Хакери пояснили мотиви тим, що «Київстар» забезпечує зв'язком ЗСУ. Але також ця атака мала на меті завдати психологічного удару по населенню України й отримати розвідувальну інформацію, зазначили в СБУ [39].

Цифровій інфраструктурі «Київстару» завдали критичних уражень, зокрема, було знищено тисячі віртуальних серверів і ПК. На повне відновлення послуг у компанії пішло кілька тижнів [39, 40].

З огляду на вищенаведені приклади атак на об'єкти критичної інфраструктури, перед фахівцями з кібербезпеки постає завдання не тільки у відновленні об'єктів після заподіяної шкоди, але і детальному описі інцидентів, їхнього впливу та способів протидії зловмисникам.

Таким чином, кожен інцидент має бути детально описаний, включаючи:

- Дату та час інциденту - коли інцидент стався та тривалість атаки.
- Тип інциденту. Наприклад, несанкціонований доступ, витік даних, вірусна атака, атака відмови в обслуговуванні (DoS).
- Методи атаки. Тту мають описуватися техніки та методи, використані нападниками для виконання атаки.
- Вразливості, які були використані - деталі про те, які слабкі сторони системи були експлуатовані.

- Результати атаки - втрата даних, фінансові збитки, зниження продуктивності, порушення в роботі послуг.

Для кожного інциденту має проводиться аналіз причин, які могли сприяти його виникненню:

- Технічні недоліки - опис технічних помилок або вразливостей, які дозволили атаку.
- Людський фактор - роль, яку відіграли дії або бездіяльність персоналу, наприклад, помилки в налаштуваннях безпеки, недостатнє навчання персоналу або навмисні дії внутрішніх порушників.
- Організаційні недоліки - відсутність адекватних політик безпеки, неефективне управління ризиками, недоліки в процедурах реагування на інциденти.

Також необхідно провести оцінку впливу інцидентів на діяльність ОКІ. Під час такого оцінювання слід зазначити:

- Операційний вплив, тобто як інциденти вплинули на операційну діяльність, чи були перерви в наданні послуг.
- Фінансові втрати – описати прямі та непрямі фінансові збитки, включаючи втрату прибутку, штрафи за порушення договірних зобов'язань, витрати на відновлення системи.
- Репутаційні ризики – визначити вплив на репутацію компанії серед клієнтів та партнерів, розлянути таку проблему, як потенційна втрата довіри.

2.3 Методи і засоби захисту розподіленої інформаційної системи об’єкта критичної інфраструктури

У контексті застосування комплексних та ефективних методів захисту. особливо актуальними стають питання ідентифікації потенційних загроз, оцінки ризиків, а також вибору та реалізації адекватних технічних і організаційних заходів безпеки.

Особлива увага повинна приділятися сучасним методам кіберзахисту, які включають розвиток розумних аналітичних систем, застосування штучного інтелекту для прогнозування і виявлення аномалій, використання хмарних технологій та резервування для забезпечення еластичності та відновлення систем після кібератак.

Захист розподілених інформаційних систем на об’єкті критичної інфраструктури вимагає інтегрованого підходу, що поєднує технічні, організаційні та процесуальні заходи, адаптовані до конкретних вимог та умов роботи критичної інфраструктури.

Ключові методи і засоби технічного захисту інформації включають наступні підходи [41]:

- використання спеціалізованого захищеного обладнання для обробки даних;

- встановлення чітких правил роботи для користувачів, технічного персоналу, програмного забезпечення, а також для доступу до елементів баз даних і носіїв інформації, що мають обмежений доступ;

- регулювання архітектури автоматизованих систем і обладнання, що використовується в обчислювальній техніці;

- інженерне та технічне оснащення будівель та комунікацій, які використовуються для експлуатації автоматизованих систем і обчислювальних засобів;

- ідентифікація, виявлення та блокування будь-яких зовнішніх закладних пристроїв, що можуть бути використані для несанкціонованого доступу.

Різні засоби захисту інформації охоплюють широкий спектр технік та інструментів, включаючи фізичні, апаратні, програмні, апаратно-програмні засоби, а також криптографічні та організаційні методи. Фізичні засоби захисту передбачають заходи для забезпечення фізичної безпеки обладнання, територій і приміщень, де використовуються комп'ютерні системи, і мають на меті створити перепони для потенційних порушників, щоб перешкодити їх доступу до захищеної інформації і системних компонентів [41].

Апаратні засоби захисту включають різноманітні електронні, електронно-

механічні та інші пристрої, які інтегровані у стандартні модулі електронних систем для обробки та передачі даних, з метою забезпечення внутрішнього захисту обладнання обчислювальної техніки, включаючи термінали, пристрої для введення та виведення даних, процесори, комунікаційні лінії та інше. Основні завдання цих засобів захисту охоплюють [41]:

- запобігання несанкціонованому (неавторизованому) доступу віддалених користувачів ззовні;

- перешкоджання несанкціонованому (неавторизованому) внутрішньому доступу до баз даних через випадкові або умисні дії співробітників;

- захист цілісності програмного забезпечення.

Ці завдання виконуються за допомогою [41]:

- ідентифікації користувачів і співробітників, а також ресурсів системи;

- аутентифікації особи на основі поданого нею ідентифікатора;

- перевірки прав доступу, яка включає в себе затвердження дозволів на виконання певних дій;

- реєстрації (протоколювання) звернень до обмежених ресурсів;

- фіксації спроб несанкціонованого доступу.

Впровадження подібних функцій здійснюється за допомогою спеціалізованих технічних засобів. Серед них [41]:

- джерела безперебійного живлення, які гарантують неперервну роботу апаратури;

- пристрої стабілізації напруги, що захищають від перепадів напруги та пікових навантажень у мережі;

- засоби екранування апаратури, ліній зв'язку та приміщень для уникнення зовнішніх впливів;

- пристрої ідентифікації та фіксації терміналів і користувачів при спробах несанкціонованого доступу;

- засоби захисту портів та інші компоненти обчислювальної техніки, що перешкоджають неавторизованому доступу.

Програмні засоби захисту є ключовими для виконання логічних та інтелектуальних функцій безпеки, які інтегровані в програмне забезпечення системи. Ці засоби виконують кілька важливих завдань у сфері захисту інформації як от[41]:

- забезпечення контролю за завантаженням та доступом до системи через систему паролів;
- управління та контроль доступу до системних ресурсів, включаючи термінали, зовнішні ресурси, а також постійні та тимчасові набори даних;
- захист файлів від шкідливих програм та вірусів;
- автоматизований контроль діяльності користувачів шляхом детального протоколювання їхніх дій в системі.

Крім того, апаратно-програмні засоби захисту, які представляють собою комбінацію програмного та апаратного забезпечення, мають велике значення у процесі аутентифікації користувачів, особливо у складних системах, таких як автоматизовані банківські системи. Ці засоби використовуються для верифікації ідентичності користувачів, забезпечуючи високий рівень безпеки та надійності в управлінні доступом до критичних ресурсів інформаційних систем [41].

Також до технічних методів захисту інформацій слід відносити такі:

- Шифрування даних - застосування передових технологій шифрування для захисту даних, що зберігаються і передаються. Також до цього відноситься шифрування дисків, баз даних і мережевих трансмісій.
- Встановлення міжмережевих екранів для контролю доступу між різними сегментами мережі, а також систем виявлення і запобігання вторгненням для моніторингу та реагування на підозрілу активність.
- Аутентифікація та управління доступом, налаштування багатофакторної аутентифікації, політик мінімальних привілеїв та сучасних систем управління ідентифікацією для контролю доступу користувачів та пристроїв.
- Резервне копіювання та відновлення має на меті розробку та реалізацію політик резервного копіювання з використанням надійних технологій, включаючи

резервне копіювання на основі WORM (Write Once, Read Many) для запобігання втраті даних.

Організаційні методи захисту комп'ютерної інформації включають набір дій з відбору, перевірки та навчанню працівників, задіяних у кожному етапі обробки інформації [41].

Організаційні засоби захисту включають в себе:

1. Розробку і впровадження комплексних політик безпеки, які визначають стандарти і процедури для захисту інформації та IT-ресурсів.
2. Регулярне навчання співробітників з питань кібербезпеки для підвищення обізнаності щодо потенційних загроз і методів їх запобігання.
3. Проведення регулярних аудитів і перевірок безпеки для виявлення та виправлення слабких місць.

Досвід міжнародних країн показує, що ефективний спосіб захисту інформаційних систем полягає у призначенні в організаціях посади фахівця з кібербезпеки або створенні спеціалізованих відділів, як приватних, так і державних, залежно від потреби. За даними зарубіжних експертів, наявність такої структури в банках знижує ризик злочинів, пов'язаних з використанням комп'ютерних технологій, на 50% [41].

Висновки до розділу 2

Ефективність захисту РІС на ОКІ значно зростає за рахунок використання багаторівневих систем безпеки, що включають технічні, організаційні та правові засоби. Це дозволяє не тільки захищати критичну інформацію, але й забезпечувати стійкість інфраструктури до різних форм загроз.

Розвиток технологій і постійна зміна характеру загроз вимагають оновлення і адаптації методів і засобів захисту. Неперервний моніторинг стану захисту інформаційних систем і регулярна оцінка ефективності заходів безпеки є важливими для виявлення потенційних слабких місць і швидкого реагування на інциденти. Співпраця між різними агентствами та організаціями, на національному та міжнародному рівнях, сприяє підвищенню загальної захищеності ОКІ.

РОЗДІЛ 3
РОЗРОБКА ПОГРАМИ АВТОМАТИЗОВАНОГО РЕЗЕРВНОГО КОПІЮВАННЯ

В заключній частині робити увага зосереджена на описі та аналізі процесу створення програмного рішення, яке спрямоване на автоматизацію процедур резервного копіювання в лабораторному середовищі. Цей розділ описує кроки, інструменти та технології, використані для розробки та реалізації системи, що можуть ефективно забезпечувати безперервність бізнес-процесів та цілісність даних на об'єктах критичної інфраструктури.

Резервне копіювання даних є ключовим елементом стратегії з кібербезпеки будь-якої організації. Воно забезпечує наявність матеріалу для подальшого відновлення інформації після випадкових помилок, технічних збоїв або кібератак. Значення автоматизації цього процесу не можна недооцінювати, адже автоматизація дозволяє значно знизити людський фактор, збільшити регулярність та надійність створення резервних копій.

Цей розділ розглядає ключові компоненти системи автоматизованого резервного копіювання, включаючи вибір платформи, розробку алгоритмів ат програмування скрипта.

Завданням цього розділу є зображення підходу до процесу планування та розробки програми автоматизованого резервного копіювання, яка буде відповідати специфічним вимогам, встановленим для об'єктів критичної інфраструктури.

3.1 Підготовка лабораторного середовища

Для реалізації скрипта метою якого є автоматизоване резервне копіювання необхідно розгорнути лабораторне середовище.

В якості програми віртуалізації використовується VirtualBox.

За допомогою найпопулярнішого у світі кросплатформного програмного забезпечення з відкритим вихідним кодом для віртуалізації Oracle VM VirtualBox можна швидше створювати код, працюючи з кількома операційними системами на одному пристрої.

VirtualBox, розроблений Oracle, є потужним інструментом віртуалізації, який має багато переваг при використанні як основи для лабораторного середовища. Ось деякі ключові переваги використання VirtualBox [42, 43, 44, 45]:

- Відкрите програмне забезпечення - VirtualBox є безкоштовним і відкритим програмним забезпеченням, що дозволяє його використовувати без додаткових витрат на ліцензування. Це робить його доступним для студентів і дослідників, які можуть встановлювати і налаштовувати віртуальні машини без фінансових обмежень.
- Крос-платформна підтримка - VirtualBox може працювати на багатьох хост-операційних системах, включаючи Windows, macOS, Linux і Solaris. Це забезпечує велику гнучкість та зручність для користувачів, які використовують різноманітне обладнання і програмне забезпечення.
- Легке налаштування та управління - VirtualBox має інтуїтивно зрозумілий графічний користувальницький інтерфейс (GUI), що дозволяє легко створювати, налаштовувати та керувати віртуальними машинами. Він також підтримує налаштування через командний рядок, забезпечуючи гнучкість для автоматизації задач.
- Підтримка різних операційних систем - VirtualBox підтримує великий спектр гостьових операційних систем, включаючи різні версії Windows, багато дистрибутивів Linux, Solaris, BSD та інші. Це ідеально підходить для тестування програмного забезпечення та налаштування середовища під конкретні потреби проекту.
- Снапшоти та клонування - VirtualBox дозволяє робити снапшоти стану віртуальної машини, що можна використовувати для швидкого відновлення до попереднього стану. Також можливе клонування віртуальних машин, що є

корисним для масштабування тестових середовищ без необхідності повторного налаштування.

- Мережеві можливості - VirtualBox пропонує різноманітні налаштування мережі, що дозволяють інтегрувати віртуальні машини в різні мережеві конфігурації. Це може включати приватні мережі всередині VirtualBox або налаштування мережевого мосту для взаємодії з реальними мережами.
- Портативність та експорт - Віртуальні машини можуть бути легко експортовані та імпортовані у форматі OVA, що забезпечує високу портативність та легкість обміну середовищами між різними системами або користувачами.

Ці переваги роблять VirtualBox відмінним вибором для створення та управління лабораторними середовищами, особливо в академічному та дослідницькому контексті, де потрібна висока ступінь адаптивності та доступності [42, 43, 44, 45].

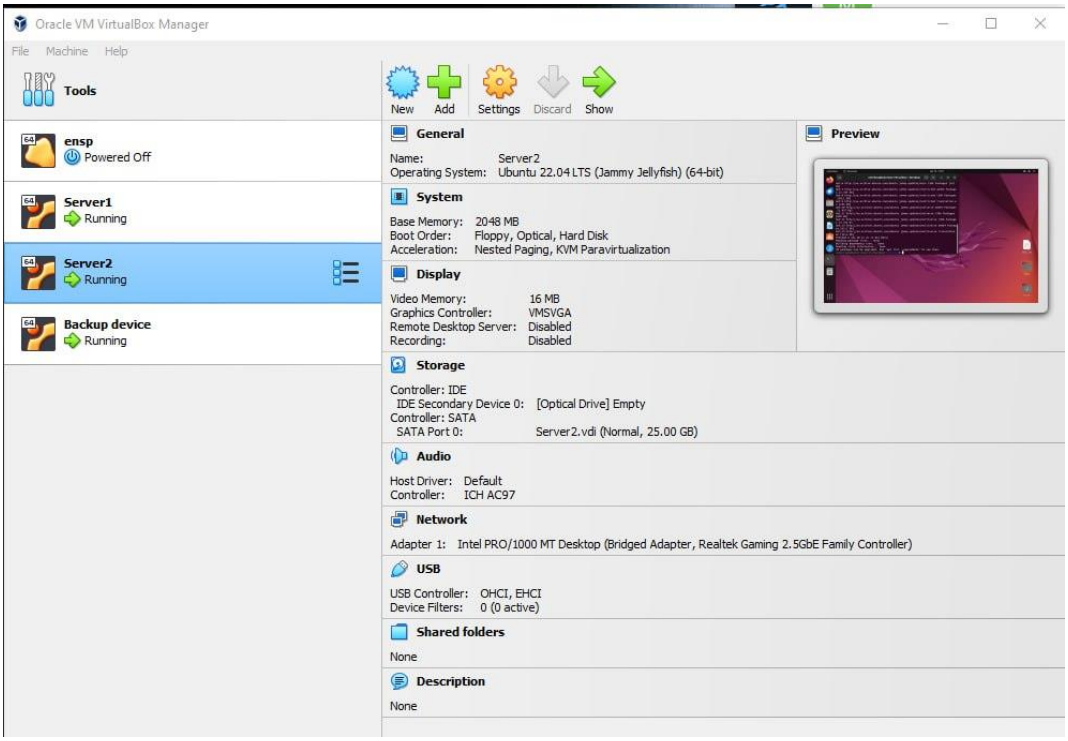

Рисунок 3 – Лабораторне середовище

Рисунок 4 – Мережеві налаштування

В цьому середовищі (рис.3) розгорнуто три віртуальні машини:

- Server1 та Server2 – серевери з даними, з яких відбуватиметься резервне копіювання
- BackupServer – сервер резервного копіювання

Для забезпечення взаємодії між VM налаштовано мережеві адаптери (рис. 4). Можна використати внутрішню мережу або мережевий міст, щоб усі VM могли спілкуватися між собою.

В якості операційної системи обрано - Linux Ubuntu 22.04 LTS. Ubuntu 22.04 LTS (Long Term Support), відома під кодовою назвою "Jammy Jellyfish", є обрано в якості віртуальної операційної системи в лабораторних умовах. Ця версія Ubuntu пропонує стабільність, широку підтримку і розширені можливості. Ключові аспекти Ubuntu 22.04 LTS, які розглядалися при виборі її, як віртуальної ОС [46]:

- Стабільність і підтримка - Ubuntu 22.04 LTS забезпечує довготривалу підтримку до квітня 2027 року, що включає оновлення безпеки і стабілізаційні патчі. Це гарантує, що система буде залишатися безпечною та оновленою протягом тривалого періоду, що є критично важливим для дослідницьких середовищ.
- Покращення продуктивності - Ubuntu 22.04 включає останні версії ядра Linux та настільного середовища GNOME, що забезпечує покращену продуктивність

і зменшене споживання ресурсів. Це робить її ідеальною для використання в віртуальних машинах, де ресурси часто обмежені.

- Розширені мережеві можливості - Ubuntu 22.04 LTS підтримує різноманітні мережеві конфігурації і може легко інтегруватися в складні мережеві інфраструктури. Це включає підтримку віртуальних мереж, інструменти для налаштування мережевого брандмауера та розширені можливості VPN, що є особливо корисним для симуляції мережевих середовищ і тестування мережевої безпеки.
- Зручність у використанні - Ubuntu 22.04 LTS забезпечує високу зручність користувача зі своїм інтуїтивно зрозумілим графічним інтерфейсом GNOME, який є особливо корисним для новачків. Вона також підтримує велику кількість програмного забезпечення, доступного через Ubuntu Software Center, що робить її відмінною платформою для розробки та тестування програм.
- Сумісність з розробкою та тестуванням - Ubuntu 22.04 LTS підтримує широкий спектр програмних мов та інструментів розробки, що робить її ідеальною для програмної інженерії і розробки веб-додатків. Система легко інтегрується з популярними IDE та інструментами для автоматизації тестування.

На серверах з даними створено директорії та тестові файли, які будуть предметом резервного копіювання.

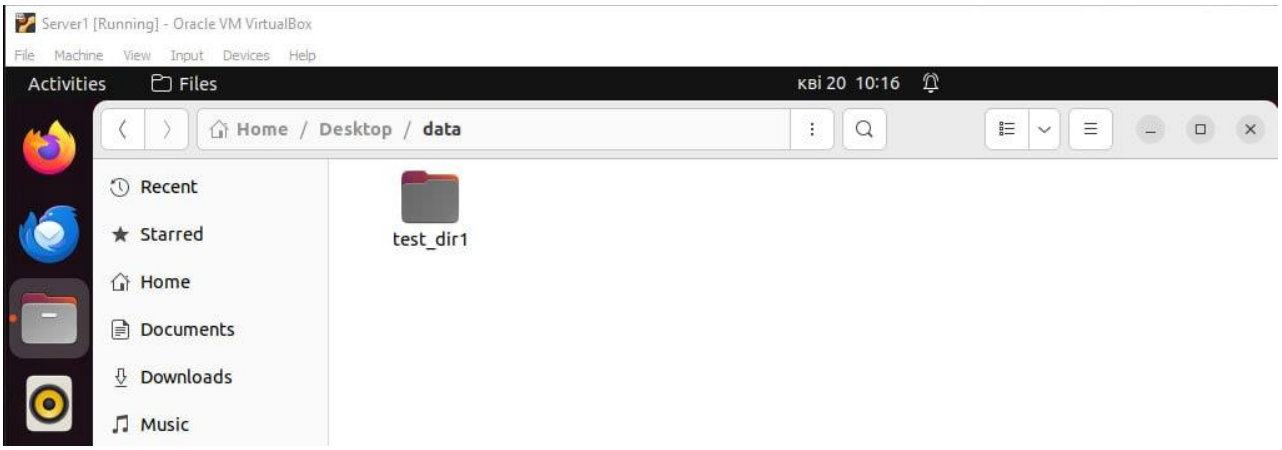

Рисунок 5 – Директорія для резервного копіювання на Server1

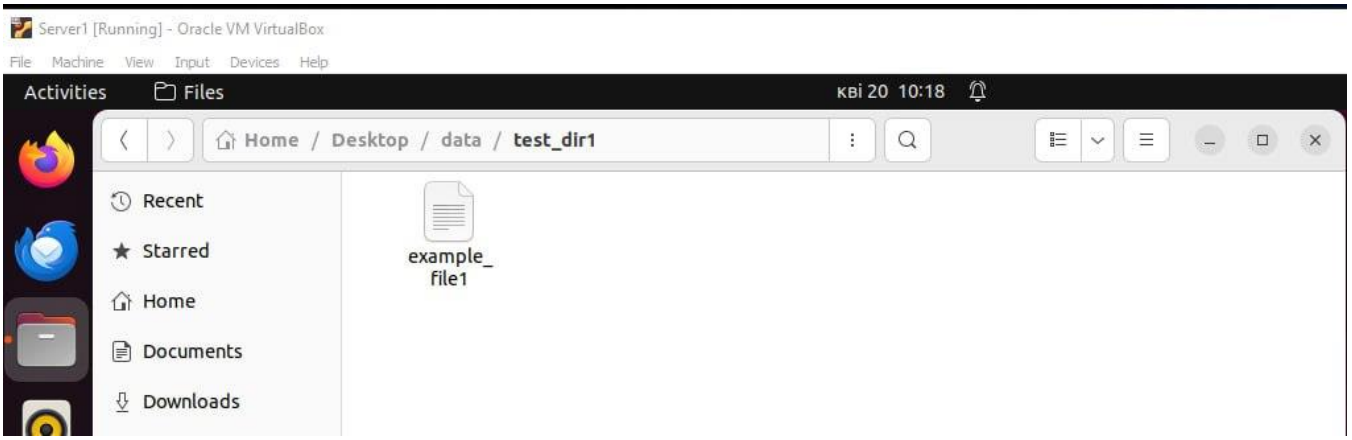

Рисунок 6 – Вміст директорії test_dir1

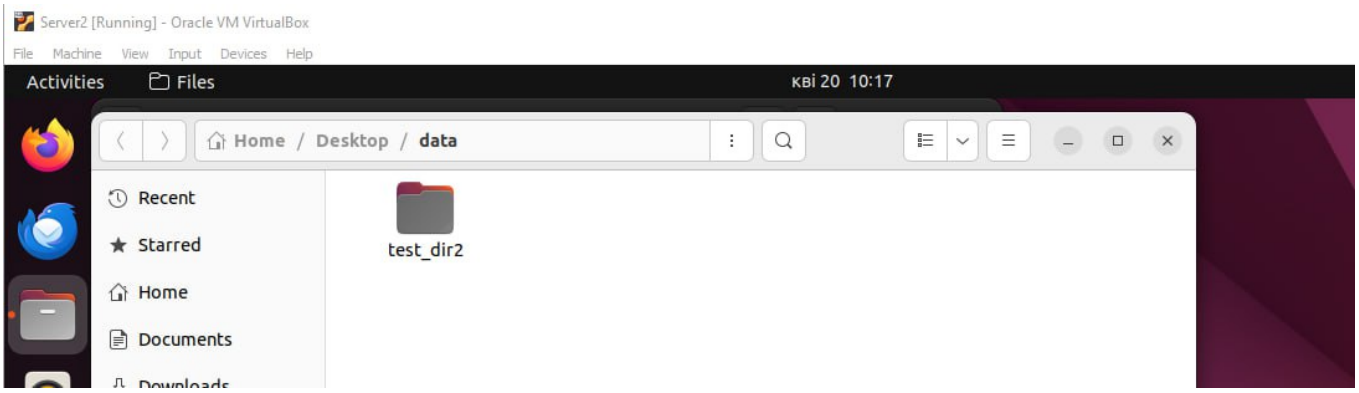

Рисунок 7 - Директорія для резервного копіювання на Server2

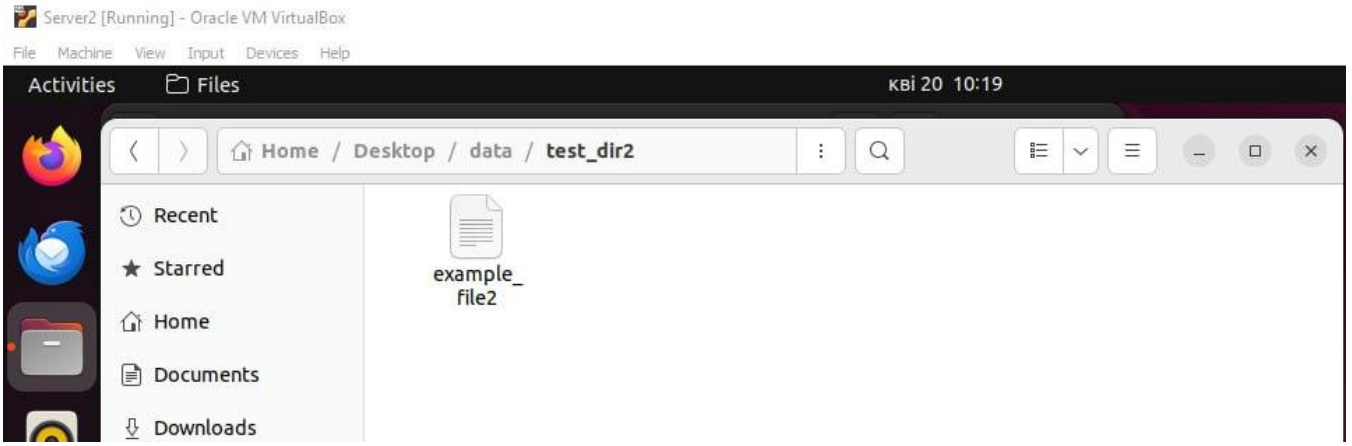

Рисунок 8 – Вміст директорії test_dir2

На сервері резервного копіювання налаштовано доступ до сховищ даних серверів через мережу (рис. 4-8).

На серверах з даними створено тестові файли та директорії, які використовуються для демонстрації резервного копіювання. Це зроблено за допомогою команд mkdir та touch в терміналі.

mkdir /data/test_dir1

touch /data/test_dir1/sample_file1.txt

На Server1 та Server2 встановлено NFS-сервер за допомогою команд:

- sudo apt update
- sudo apt install nfs-kernel-server

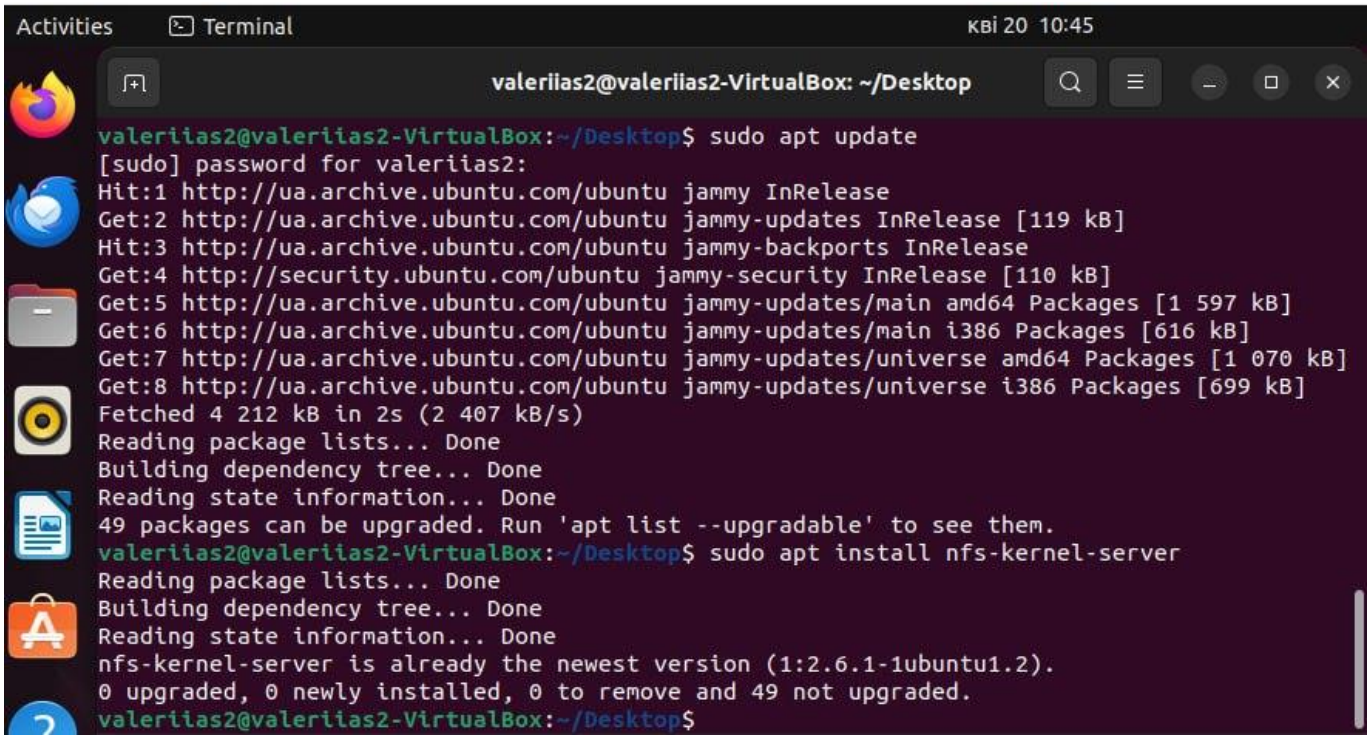

Рисунок 9 - Встановлення NFS-сервер

Конфігурація експортування файлових систем. Визначено, які директорії будуть доступні для віддаленого доступу. Відбувається редагування файлу /etc/exports. В ньому додано рядки для кожної директорії, яку буде експортовано.

Ця конфігурація дозволяє серверу резервного копіювання з IP-адресою 192.168.0.178 монтувати /home/valeriias1/Desktop/data та /home/valeriias2/Desktop/data директорії з повним доступом для читання та запису.

Тобто, /home/valeriias1/Desktop/data та /home/valeriias2/Desktop/data – шляхи до директорій, які експортуються.

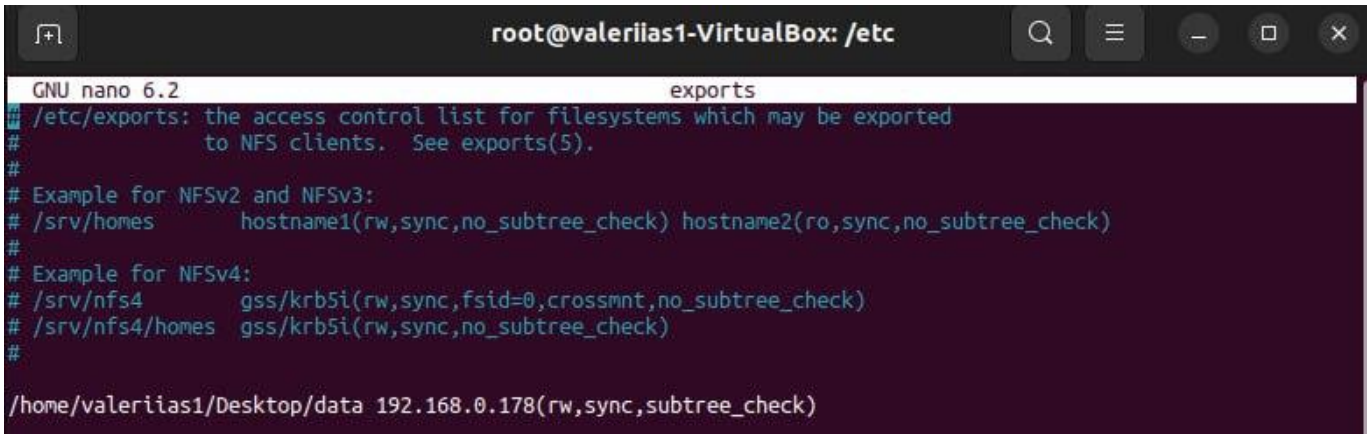

Рисунок 10 - редагування файлу /etc/exports на Server1

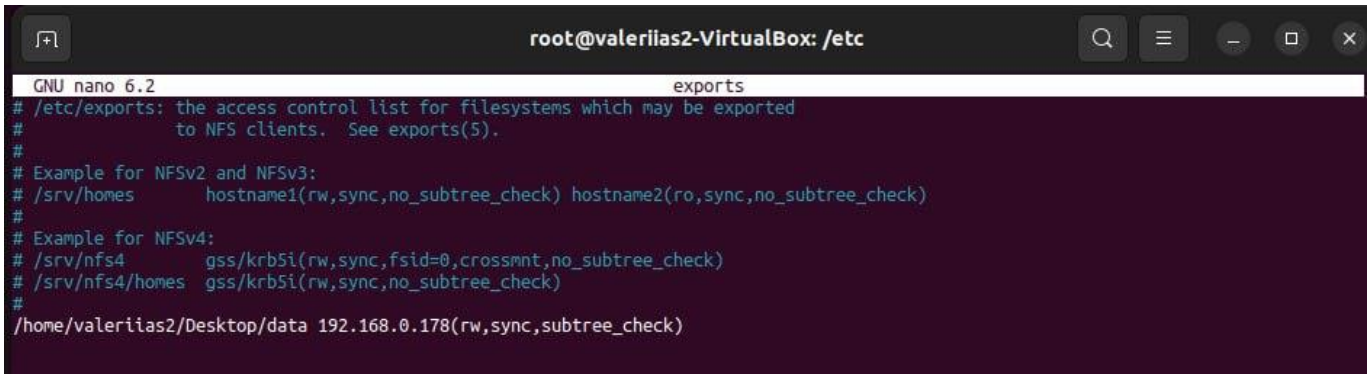

Рисунок 11 - редагування файлу /etc/exports на Server2

192.168.0.178 – IP-адреса, для якої дозволено доступ.

- rw означає, що клієнт може як читати, так і записувати у директорію.
- sync забезпечує синхронізацію даних на диск перед завершенням операції.
- subtree_check - цей параметр включає перевірку піддерева, що дозволяє серверу NFS перевіряти, чи належить файл, на який здійснюється запит, до експортованої директорії. Це може зменшити продуктивність, але збільшити безпеку.

Після конфігурації файлу /etc/exports, застосовуємо зміни:

- sudo exportfs -ra

Ця команда перечитає файл /etc/exports і застосує нові налаштування експорту без необхідності перезапуску служби NFS.

- exportfs -v

Це виведе список всіх експортованих директорій з їх параметрами доступу, допомагаючи підтвердити, що ваші налаштування були застосовані правильно.

```
root@valeriias1-VirtualBox:/etc# sudo exportfs -ra
exportfs: /etc/exports [2]: Neither 'subtree_check' or 'no_subtree_check' specified for export "192.180.0.178:
/home/valeriias1/Desktop/data".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x

root@valeriias1-VirtualBox:/etc# nano exports
root@valeriias1-VirtualBox:/etc# sudo exportfs -ra
root@valeriias1-VirtualBox:/etc# exportfs -v
/home/valeriias1/Desktop/data
                192.180.0.178(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,root_squash,no_all_squash)
root@valeriias1-VirtualBox:/etc#
```

Рисунок 12 - Експортовані директорії на Server1

Налаштування NFS-клієнта – BackupServer. На сервері резервного копіювання потрібно встановити NFS-клієнт:

- sudo apt update
- sudo apt install nfs-common

Наступним кроком є монтування NFS-директорій. Для того, аби відтворити цей процес, необхідно створіть точки монтування для експортованих директорій та змонтувати їх. Точка монтування - це директорія, у якій будуть відображатися файли з NFS-сервера. В нашому випадку:

- sudo mkdir -p /mnt/nfs/desktop_1/data
- sudo mkdir -p /mnt/nfs/desktop_2/data

Тепер відбудеться мнотування директорій з серверів на клієнтську машину. Використовуючи команду mount, вказавши IP-адресу серверів, шлях до експортованої директорії на сервері, та точку монтування на клієнті – буде виконано монтування (рис. 13):

- sudo mount 192.168.0.161:/home/valeriias1/Desktop/data /mnt/nfs/desktop_1/data
- sudo mount 192.168.0.129:/home/valeriias2/Desktop/data /mnt/nfs/desktop_2/data

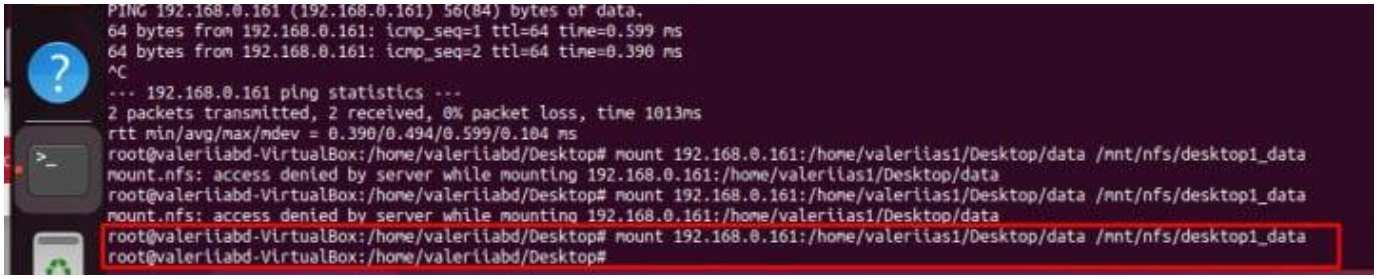

Рисунок 13 - Монтування директорії

Тут 192.168.0.161 та 192.168.0.129 - це IP-адреси серверів, /home/valeriias1/Desktop/data та /home/valeriias2/Desktop/data - шляхи до директорій на сервері, які будуть монтуватися, і /mnt/nfs/desktop_1/data та /mnt/nfs/desktop_2/data - точки монтування на клієнтській машині (рис. 14).

```
root@valeriiabd-VirtualBox:/# mkdir -p /mnt/nfs/desktop2_data
root@valeriiabd-VirtualBox:/# mount 192.168.0.129:/home/valeriias2/Desktop/data /mnt/nfs/desktop2_data
mount.nfs: access denied by server while mounting 192.168.0.129:/home/valeriias2/Desktop/data
root@valeriiabd-VirtualBox:/# cd etc
root@valeriiabd-VirtualBox:/etc# nano fstab
root@valeriiabd-VirtualBox:/etc# mount 192.168.0.129:/home/valeriias2/Desktop/data /mnt/nfs/desktop2_data
root@valeriiabd-VirtualBox:/etc# ls / mnt/nfs/desktop2_data
ls: cannot access 'mnt/nfs/desktop2_data': No such file or directory
/:
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  swapfile  tmp  var
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   sys       usr
root@valeriiabd-VirtualBox:/etc# ls /mnt/nfs/desktop1_data
test_dir1
root@valeriiabd-VirtualBox:/etc# ls /mnt/nfs/desktop2_data
test_dir2
root@valeriiabd-VirtualBox:/etc#
```

Рисунок 14 - Експортовані директорії на Server1

Також, для зручності слід впровадити автоматичне монтування при запуску системи. Для автоматичного монтування директорій при запуску системи, потрібно додати записи в /etc/fstab (рис. 15):

- 192.168.1.10:/var/www /mnt/nfs/var_www nfs defaults 0 0
- 192.168.1.10:/home /mnt/nfs/home nfs defaults 0 0

```
root@valeriiabd-VirtualBox: /etc
 GNU nano 6.2                                    fstab *
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda3 during installation
UUID=490998cd-f699-42b6-98b1-d29baded0c4a /              ext4    errors=remount-ro 0       1
# /boot/efi was on /dev/sda2 during installation
UUID=C09A-BB68  /boot/efi       vfat    umask=0077      0       1
/swapfile                                 none            swap    sw              0       0

192.168.0.161:/home/valeriias1/Desktop/data /mnt/nfs/desktop1_data nfs defaults 0 0
192.168.0.129:/home/valeriias2/Desktop/data /mnt/nfs/desktop2_data nfs defaults 0 0
```

Рисунок 15 – редагування /etc/fstab

Перевірка монтування директорій покаже файли та директорії, які знаходяться у віддаленій директорії /var/www на Backup-сервері (рис. 16, 17).

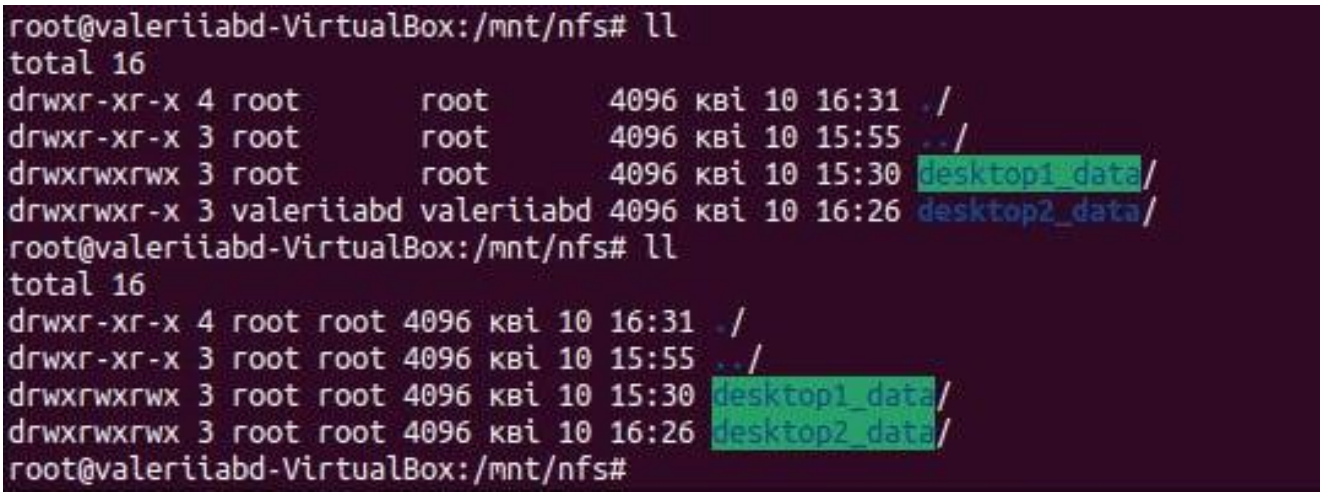

Рисунок 16 – Монтування директорій

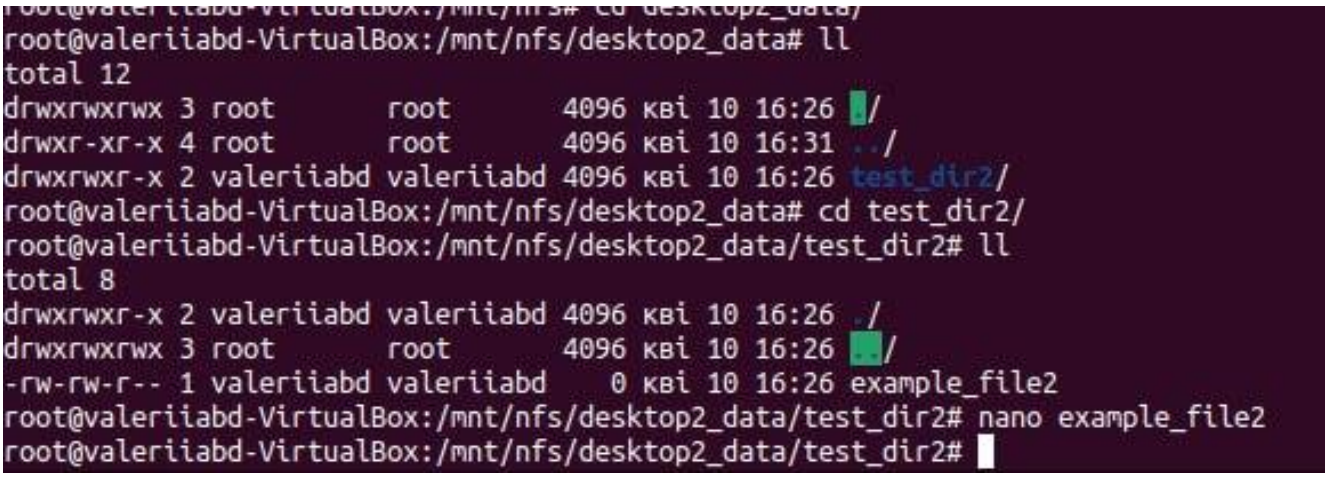

Рисунок 17 – Монтування директорій

Тепер сервер резервного копіювання має доступ до файлових систем серверів даних через мережу, що дозволяє здійснювати резервне копіювання та відновлення даних без необхідності локального доступу до дискових ресурсів серверів з даними. Монтування NFS-директорій дозволяє системі використовувати файли та директорії з віддаленого сервера так, ніби вони знаходяться локально на комп'ютері.

3.2 Програмна реалізація автоматизованого резервного копіювання

Для того, аби створити та виконати скрипт необхідно встановити середовище розробки та необхідні бібліотеки. Зробити це можна за допомогою команди - python3 –version.

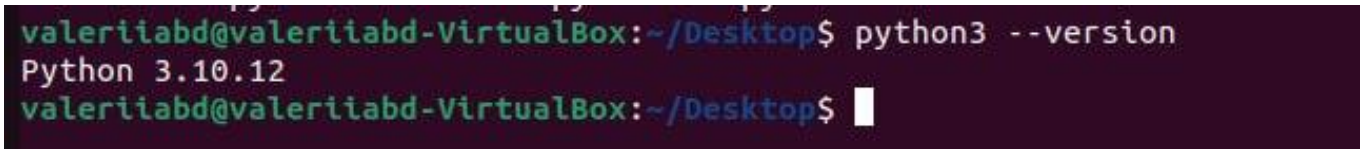

Рисунок 18 – Встановлення середовища

Структурно, Python скрипт, який автоматизує процес резервного копіювання директорій на сервері Складається з наступних частин:

1. Імпорти бібліотек

Скрипт використовує модулі `os`, `datetime`, `logging`, `subprocess`, `tkinter` і `messagebox` для реалізації своїх функцій, таких як робота з файловою системою, логування, виконання команд системи, та виведення повідомлень через графічний інтерфейс.

2. Функції

Кожна функція в коді відповідає за певну частину процесу бекапування:

- setup_logging() - ініціалізує налаштування логування, вказуючи файл, рівень і формат логів, що дозволяє зберігати історію операцій бекапування.
- create_backup_folder(base_dir) - створює директорію для зберігання бекапу, використовуючи поточну дату та час для назви папки, що забезпечує унікальність кожного бекапу.
- create_backup_filename(source_dir, date_stamp) - формує назву файлу бекапу на основі джерела і поточного часу, що дозволяє легко ідентифікувати бекапи.
- perform_backup(source_dir, backup_base_dir) - оркеструє процес бекапу, тобто створює папку, формує назву файлу бекапу, та викликає команду для архівації директорії.
- run_backup_command(command, source_dir, backup_path) - виконує команду архівації через `subprocess`, обробляє успішні та неуспішні випадки, відображає повідомлення в GUI при успіху.

- log_backup_success(source_dir, backup_path) і log_backup_failure(source_dir, error) - ці дві функції відповідають за логування результатів операцій: успішного створення бекапу та помилок при його створенні.

- show_success_message() - створює графічне вікно для відображення повідомлення про успішне створення бекапу, використовуючи `tkinter` та `messagebox`.

3. Головна функція main()

Головна функція `main()` ініціалізує логування, визначає директорії для бекапування, та оркеструє весь процес бекапу, викликаючи `perform_backup` для кожної директорії.

4. Виклик main()

Цей блок коду запускає головну функцію `main()`, якщо скрипт виконується як головна програма. Це типовий підхід для Python скриптів, які можуть бути використані як модулі або виконувати самостійно.

```
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/scripts# python3 test1.py
Backup of /mnt/nfs/desktop1_data created successfully at /home/valeriiabd/Desktop/backups/2024-04-20_11-29-00/backu
p_desktop1_data_2024-04-20_11-29-00.tar.gz
Backup of /mnt/nfs/desktop2_data created successfully at /home/valeriiabd/Desktop/backups/2024-04-20_11-29-00/backu
p_desktop2_data_2024-04-20_11-29-00.tar.gz
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/scripts#  cd ../
```

Рисунок 19 – Відпрацювання програми

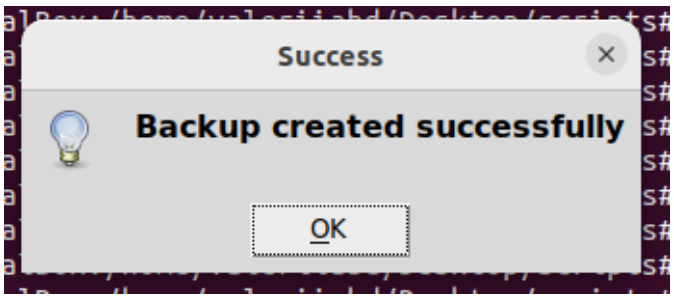

Рисунок 20 – Сповіщення про створення бекапу

```
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/scripts# python3 test1.py
Backup of /mnt/nfs/desktop1_data created successfully at /home/valeriiabd/Desktop/backups/2024-04-20_11-29-00/backu
p_desktop1_data_2024-04-20_11-29-00.tar.gz
Backup of /mnt/nfs/desktop2_data created successfully at /home/valeriiabd/Desktop/backups/2024-04-20_11-29-00/backu
p_desktop2_data_2024-04-20_11-29-00.tar.gz
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/scripts#  cd ../
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop# cd backups/
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/backups# ll
total 20
drwxr-xr-x 5 root       root       4096 кві 20 11:29 ./
drwxr-xr-x 4 valeriiabd valeriiabd 4096 кві 14 20:08 ../
drwxrwxrwx 3 valeriiabd valeriiabd 4096 кві 10 15:30 2024-04-15_22-24-17/
drwxrwxrwx 3 valeriiabd valeriiabd 4096 кві 15 11:17 2024-04-16_14-53-44/
drwxr-xr-x 2 root       root       4096 кві 20 11:29 2024-04-20_11-29-00/
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/backups# cd 2024-04-20_11-29-00/
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/backups/2024-04-20_11-29-00# ll
total 16
drwxr-xr-x 2 root root 4096 кві 20 11:29 ./
drwxr-xr-x 5 root root 4096 кві 20 11:29 ../
-rw-r--r-- 1 root root  258 кві 20 11:29 backup_desktop1_data_2024-04-20_11-29-00.tar.gz
-rw-r--r-- 1 root root  254 кві 20 11:29 backup_desktop2_data_2024-04-20_11-29-00.tar.gz
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/backups/2024-04-20_11-29-00#
```

Рисунок 21 – Перевірка результату створення резервної копії

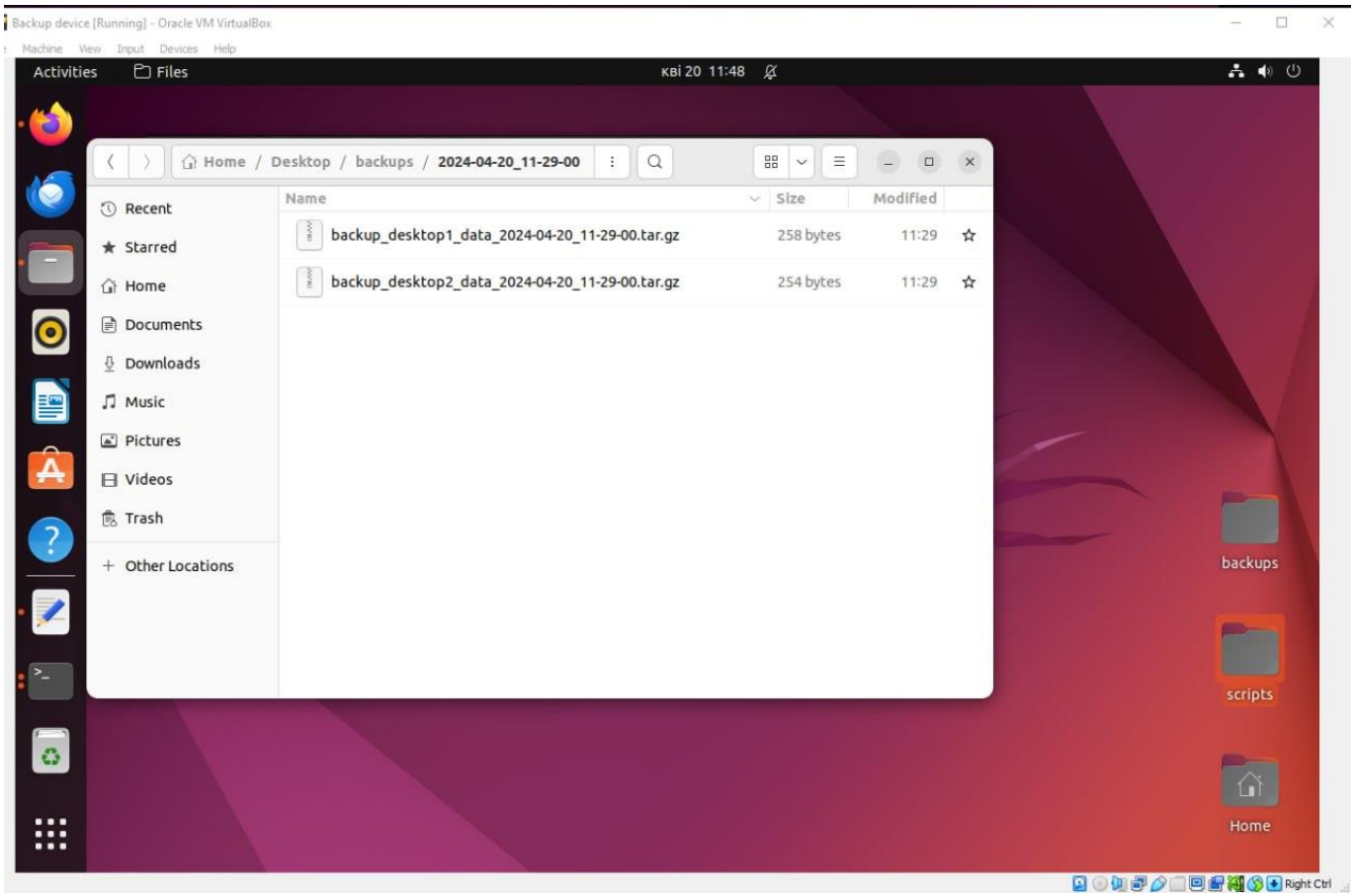

Рисунок 22 – Перевірка наявності файлів у визначеній директорії

```
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/backups/2024-04-20_11-29-00# tar -tf backup_desktop1_data_2024-
04-20_11-29-00.tar.gz
./
./backup_server1/
./test_dir1/
./test_dir1/example_file1
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/backups/2024-04-20_11-29-00# tar yf backup_desktop2_data_2024-0
4-20_11-29-00.tar.gz
tar: invalid option -- 'y'
Try 'tar --help' or 'tar --usage' for more information.
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/backups/2024-04-20_11-29-00# tar -tf backup_desktop2_data_2024-
04-20_11-29-00.tar.gz
./
./data/
./data/test_dir2/
./data/test_dir2/example_file2
root@valeriiabd-VirtualBox:/home/valeriiabd/Desktop/backups/2024-04-20_11-29-00#
```

Рисунок 23 – Перевірка змісту архівів резервних копій

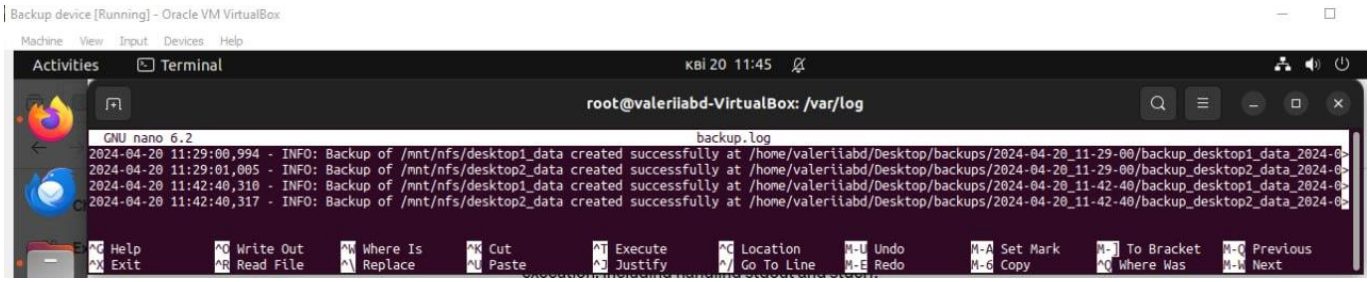

Рисунок 24 – Перевірка вмісту лог-файлу

Цей скрипт автоматизує процес резервного копіювання важливих директорій, забезпечує документування всіх дій та зберігає повну інформацію про успіхи та помилки в лог-файлі.

3.3 Перспективи впровадження та об’єднання з технологією Air-Gap

Як показує практика, одного тільки резервного копіювання часто може бути замало для забезпечення високого рівня безпеки. Для того, аби підвищити захищеність резервних копій можна застосовувати технологію Air-gap. Air-gap— це захід безпеки, який передбачає ізоляцію комп’ютера або мережі та запобігання встановленню зовнішнього з’єднання. Комп’ютер із Air-gap фізично відокремлений і не може з’єднатися бездротовим або фізичним способом з іншими комп’ютерами чи мережевими пристроями [47, 48].

Air-gap захищають критично важливі комп’ютерні системи або дані від потенційних атак, починаючи від зловмисного програмного забезпечення та програм-вимагачів до клавіатурних шпигунів чи інших атак з боку зловмисників [47, 48, 49].

Air-gap є одним із заходів безпеки в секторі критичної інфраструктури, де кібератака може порушити або призупинити основні операції. Системи, які розгортають Air-gap зазвичай включають [50]:

- військові комп'ютерні системи та мережі;
- урядові комп'ютерні системи та мережі;
- фінансові комп'ютерні системи та мережі;
- промислові системи управління;
- атомні електростанції;
- авіаційні комп'ютери;
- медичне обладнання.

Комп’ютери з Air-gap зазвичай розташовуються в безпечних місцях, наприклад, на окремому сервері з суворою охороною. В якості запобіжного заходу системи з Air-gap мають обмежений доступ, тому доступ до них мають лише кілька довірених користувачів [50].

Як можна побачити вище у цьому переліку немає телекомунікаційних операторів, як суб’єкта, який часто використовує цю технологію, проте це слід виправити.

Air Gaps в першу чергу служать двом цілям безпеки: захист від мережевих або системних вторгнень і захист цифрових активів від пошкодження, доступу або втручання. Ці цілі часто збігаються, але є різними. Наприклад, зберігання резервних стрічок у соляній шахті є методом Air Gap, який захищає дані від несанкціонованого доступу. Обґрунтування до впровадження є наступними - якщо наші системи зламано або знищено, ми можемо відновити їх, використовуючи дані, збережені в середовищі, захищеному Air-Gap.

Air Gaps сприймаються багатьма професіоналами безпеки як найкращий засіб захисту. Зрештою, якщо зловмисник навіть не може отримати доступ до системи чи мережі, як він може їй зашкодити? Air-gap поширених в секторах з високим рівнем безпеки, як-от військові, фінансові та комунальні служби.

Починаючи зі сфери IT, мереж і безпеки, Air Gap відноситься до парадигми безпеки, яка логічно і фізично розділяє IT-системи. Ці системи не підключені ні до зовнішніх мереж, як-от Інтернет чи локальні мережі, ні до інших IT-систем. Передача даних між ізольованими системами є односпрямованою, як правило, за допомогою портативних пристроїв зберігання.

Серед переваг даної технології та впровадження її є захист від програм-вимагачів. Атаки програм-вимагачів поширюються мережею для шифрування робочих хостів, серверів, підключених пристроїв зберігання даних і резервних серверів. Резервне копіювання з Air Gap гарантує, що навіть якщо інша частина інфраструктури скомпрометована, дані, що зберігаються в томах з Air-gap, залишаються доступними та залишаються доступними [51].

За допомогою цільових томів з Air Gap організації можуть захистити свої критично важливі структуровані, неструктуровані та об’єктні робочі навантаження від таких загроз, як програми-вимагачі, віруси, невдале оновлення програмного забезпечення та людські помилки [51].

Крім того, резервне копіювання Air Gap також допомагає організаціям дотримуватися галузевих норм, таких як HIPAA/HITRUST, FINRA, FISMA, GDPR тощо, оскільки запобігає витоку даних і забезпечує відновлення даних [51].

До стратегії резервного копіювання Air Gap слід віднести також правило 3-2-1-1-0. Правило 3-2-1-1-0 — це вдосконалена стратегія захисту даних, яка використовує можливості резервного копіювання та відновлення, щоб забезпечити високу доступність, можливість відновлення та майже нульовий час простою.

Правило стверджує, що потрібно мати три різні копії даних, які зберігаються на двох носіях пам’яті, з однією зовнішньою копією та однією резервною копією Air Gap [51].

У той час як традиційні методи використовують стрічкові масиви або фізичні носії для створення автономної копії, томи з Air Gap забезпечують автоматизовану, програмно визначену, просту в управлінні та доступну альтернативу. Більше того, у порівнянні зі стрічковими масивами резервне копіювання з логічним Air Gap коштує

дешевше, потребує менше часу для налаштування та керування, і на нього не впливають людські помилки [51].

Вище розглянутий скрипт пропонує зберігання резервних копій на сервері, проте можна піти далі і замість серверів для цих цілей зберігати дані на системах збереження даних. СЗД більше підходять для збереження великих об’ємів даних, які генеруються об’єктами критичної інфраструктури, зокрема телекомунікаційними операторами. Нижче наведено схему реалізації технології Air-Gap для збереження ізольованих резервних копій.

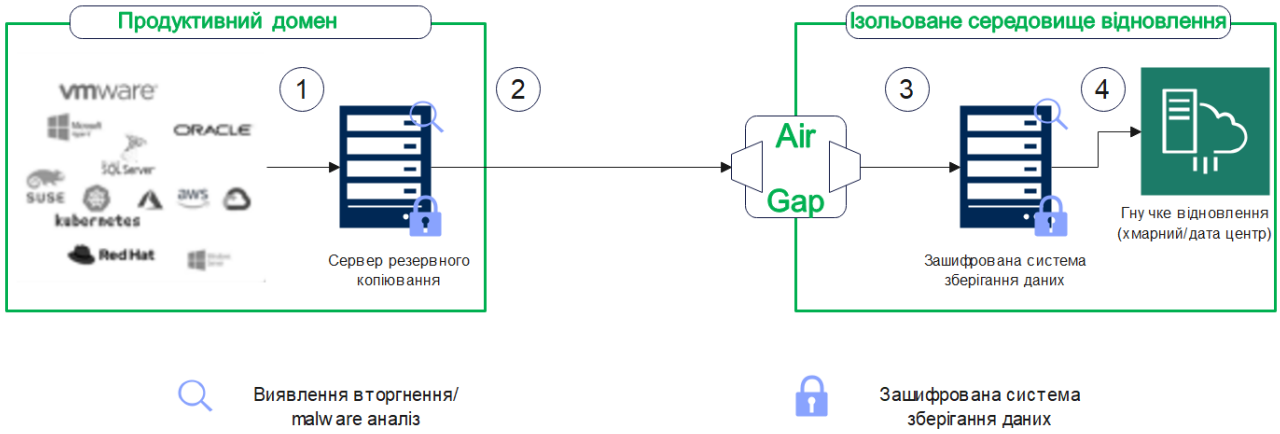

Рисунок 25 - Реалізація технології Air-Gap для збереження ізольованих резервних копій [52, 53]

Технологія Air-Gap містить в собі такі складові:

1. Виявлення аномалій в реальному часі після бекапування.
2. Ізоляція даних використанням Air-Gap.
3. Забезпечення цілісності інформації застосуванням WORM технології в сховиші даних.
4. Відновлення до нормального стану.

Технологія Air-Gap може значно покращити безпеку процесу резервного копіювання в об'єктах критичної інфраструктури, забезпечуючи високий рівень ізоляції від зовнішніх загроз. Ось як можна адаптувати зазначений скрипт до використання в умовах Air-Gap:

- Фізична ізоляція Backup Server. Слід переконатися, що сервер, який використовується для зберігання резервних копій, не має прямих мережевих з'єднань з іншими системами, крім необхідних для процесу резервного копіювання. Це може бути реалізовано шляхом відключення всіх мережевих адаптерів, окрім внутрішньої мережі, яка контролюється та захищена.
- Захист фізичних портів. Потрібно забезпечити блокування фізичних або вимкнення портів на сервері, таких як USB або зовнішних HDD порти, щоб уникнути несанкціонованого доступу через фізичні носії.
- Періодичне ручне оновлення. Оскільки Air-Gap сервер не матиме доступу до Інтернету для автоматичних оновлень, важливо регулярно вручну оновлювати програмне забезпечення та систему безпеки. Це може включати оновлення вірусних баз, патчів безпеки ОС та оновлень застосунків.
- Автоматизація процесу резервного копіювання. Скрипт має бути запланований для автоматичного виконання з певною періодичністю. Це гарантує, що дані регулярно оновлюються без втручання людини.
- Контрольована передача даних ящо передача даних забезпечується між мережами, вона має відбуватись через суворо контрольовані і захищені точки обміну. Для цього можна використовувати зашифровані пристрої зберігання або засоби передачі даних.

Говорячи про об'єкти критичної інфраструктури слід зауважити, що впровадження автоматизованого резервного копіювання у поєднанні з технологією Air-Gap наступним чином вплине на рівень безпеки системи:

- Знизится рівеня ризику кібератак, адже оскільки Air-Gap сервери відокремлені від зовнішніх мереж, ризик інфекцій вірусами або зламів значно знижується.
- Відбудеться підвищення рівня захисту від витоку даних. Неможливість прямого доступу до серверів ззовні знижує ризик несанкціонованого доступу та витоку даних.
- Буде гарантія доступності даних. Тобто, навіть у випадку масштабних мережевих атак, дані залишатимуться доступними для відновлення системи.

- Процеси оновлення будуть контрольованими. Ручне оновлення елемента з Air Gap забезпечує, що всі зміни в системі можуть бути уважно перевірені на предмет безпеки перед їх впровадженням.

За допомогою цих підходів об'єкти критичної інфраструктури можуть забезпечити високий рівень захисту своїх даних, що є критично важливим для їх стабільної та безпечної роботи.

Висновки до розділу 3

В третьому розділі створено лабраторні умови для проведення розробки програми автоматизованого резервного коіювання. Розроблено програму для автоматизації створення резервних копій з пристроїв задля забезпечення стійкості інформаційних систем до знищення інформації. Досліджено перспективи впровадження автоматизованого підходу до створення резервних копій з пристроїв прозподіленої інформаційної системи на віддалений ізольваний пристрій із застосуванням Air-Gap технології. Викладений вище погляд на проблему бекапування та способи її вирішення, можуть дати поштовх до активнішого застосування описаних підходів до зберігання даних та зміцнення кібербезпеки на об'єктах критичної інфраструктури.

ВИСНОВКИ

Ми кожного дня стикаємося із втратою або пошкодженням інформації. Це свого роду стало нормою сучасності, проте не для систем, які забезпечують критично важливі галузі функціонування держави. Втрата або пошкодження даних в системах таких об’єктів часто призводить до фінансових, репутаційних та інших збитків. Для того, аби унеможливити повну втрату важливих даних резервне копіювання є одним із ключових підходів для вирішення цієї проблеми. Проте в класичному варіанті навіть цього вже не достатньо. Саме тому реалізація нових підходів та об’єднання з іншими технологіями може підвищити рівень забезпечення безпеки на об’єктах критичної інфраструктури.

Дана робота структурована на основі трьох ключових розділів, кожен з яких вносить свій вклад у комплексний підхід до забезпечення безпеки критичної інфраструктури.

У першому розділі проаналізовано законодавче забезпечення, надано визначення та розглянута організаційна структура розподілених інформаційних систем, а також прокласифіковано об'єкти інфраструктури. Ефективне законодавче забезпечення, яке гнучко адаптується до нових умов та підтримує комплексний підхід до управління ризиками, служить основою для захисту стратегічних активів країни та зміцнення стійкості критичної інфраструктури. Це сприяє не лише безпеці окремих об'єктів, а й гарантує високий рівень забезпечення національної безпеки та стабільності загалом. Важливість адекватного правового регулювання та класифікації критичних активів має ключове значення для їх оборони, що обумовлює стратегії протидії загрозам і розподіл ресурсів.

У другому розділі детально розглянуто вразливості об'єктів критичної інфраструктури, включаючи технічні, організаційні аспекти та модель загроз і порушника. Аналіз інцидентів та огляд сучасних методів і засобів захисту відкрив нові перспективи для розуміння та покращення механізмів захисту. Набуті знання

стосовно протидії загрозам і кіберзахисту розподілених систем засвідчили потребу у постійному оновленні та адаптації захисних стратегій.

У третьому розділі увагу буо сфокусовано на створенні та впровадженні автоматизованої системи резервного копіювання з подальшою можливістю використанням технології Air-Gap. Розробка такої системи в лабораторних умовах показала, як можна підвищити стійкість інформаційних систем до знищення інформації. Вивчення перспектив впровадження та можливостей інтеграції з іншими захисними технологіями надало бачення для майбутнього розвитку та зміцнення кібербезпеки на об'єктах критичної інфраструктури.

На основі проведеного аналізу стало очевидним те, що захист розподілених інформаційних систем критичної інфраструктури вимагає інтегрованого підходу, який включає застосування передових технологій, ретельну підготовку персоналу, впровадження стандартизованих процедур і постійне оновлення захисних механізмів. Такий підхід дозволяє не тільки ефективно реагувати на поточні загрози, але й адаптуватися до майбутніх викликів у сфері кібербезпеки.

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ЗАКОН УКРАЇНИ Про національну безпеку України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text

2. Підтримка парламентом законопроекту «Про національну безпеку» стала важливим кроком на шляху зміцнення оборони і безпеки нашої держави [Електронний ресурс]. – Режим доступу: https://www.rnbo.gov.ua/ua/Diialnist/2996.html?PRINT

3. ЗАКОН УКРАЇНИ Про критичну інфраструктуру [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text

4. Про критичну інфраструктуру || від 16.11.2021р. - № 1882-IX(редакція 01.01.2024р.) [Електронний ресурс]. – Режим доступу: https://protocol.ua/ua/pro_kritichnu_infrastrukturu/

5. ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. Основні засади забезпечення кібербезпеки в Україні [Електронний ресурс]. – Режим доступу : https://vseosvita.ua/lesson/osnovni-zasady-zabezpechennia-kiberbezpeky-v-ukraini-263564.html

7. ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

8. Про захист інформації в інформаційно-комунікаційних системах || від 05.07.1994р. - № 80/94-ВР(редакція 04.04.2024р.) [Електронний ресурс]. – Режим доступу: https://protocol.ua/ua/pro_zahist_informatsii_v_informatsiyno_telekomunikatsiynih_sistemah/

9. ЗАКОН УКРАЇНИ Про захист персональних даних [Електронний ресурс]. –

Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

10. Захист персональних даних в умовах воєнного стану [Електронний ресурс]. – Режим доступу: https://ombudsman.gov.ua/storage/app/media/%D0%92%D0%BE%D1%94%D0%BD%D0%BD%D0%B8%D0%B9%20%D1%81%D1%82%D0%B0%D0%BD/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85%20%D0%B2%20%D1%83%D0%BC%D0%BE%D0%B2%D0%B0%D1%85%20%D0%B2%D0%BE%D1%94%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%81%D1%82%D0%B0%D0%BD%D1%83.pdf

11. ЗАКОН УКРАЇНИ Про інформацію [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

12. Закон України Про інформацію. Реферат [Електронний ресурс]. – Режим доступу: https://osvita.ua/vnz/reports/journalism/25499/#google_vignette

13. What is a Distributed System? [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/what-is-a-distributed-system/

14. Distributed System vs. Distributed Computing? [Електронний ресурс]. – Режим доступу: https://www.baeldung.com/cs/distributed-system-vs-distributed-computing

15. What is a Distributed System? [Definition + Benefits] [Електронний ресурс]. – Режим доступу: https://www.spaceotechnologies.com/glossary/tech-terms/what-is-distributed-system/

16. Guide to Distributed Systems (With Definition and Examples) [Електронний ресурс]. – Режим доступу: https://ca.indeed.com/career-advice/career-development/distributed-system

17. Солодовник В. О. Засоби захисту розподіленої інформаційної системи

державного підприємства. – Київ, 2022 – 63 с.

18. Features of Distributed Operating System [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/features-of-distributed-operating-system/?ref=lbp

19. What is a Distributed System? Definition, Examples, Benefits, and Challenges of Distributed Systems [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=NKsySmuM81o

20. Distributed Systems Explained [Електронний ресурс]. – Режим доступу: https://www.splunk.com/en_us/blog/learn/distributed-systems.html

21. Types of Cyber Attacks [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/types-of-cyber-attacks/?ref=lbp

22. МЕТОДИКА категоризації об’єктів критичної інфраструктури. ВИЗНАЧЕННЯ РІВНЯ негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури (секторальні критерії) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#n91

23. Man-in-the-Middle Attack [Електронний ресурс]. – Режим доступу: https://sosafe-awareness.com/glossary/man-in-the-middle-attack/

24. Man in the middle (MITM) attack [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

25. Man-in-the-Middle [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle

26. Man in the Middle (MITM) Attacks [Електронний ресурс]. – Режим доступу: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

27. Критичні Вразливості Програмного Забезпечення [Електронний ресурс]. – Режим доступу: https://ru.scribd.com/document/707361322/%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D1%96-%D0%92%D1%80%D0%B0%D0%B7%D0%BB%D0%B8%D0%B2%D0%BE%D1%81

%D1%82%D1%96-
%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE-
%D0%97%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F

28. Five Problems with Using End of Life (EOL) Hardware in the Data Center [Електронний ресурс]. – Режим доступу: https://www.lantronix.com/blog/five-problems-with-using-end-of-life-eol-hardware-in-the-data-center/

29. END OF LIFE SERVERS | RISKS, COSTS, AND SOLUTIONS [Електронний ресурс]. – Режим доступу: https://www.webitservices.com/blog/end-of-life-servers-risks-costs-solutions/

30. СЛАБКІ МІСЦЯ КОНТРОЛЮ ДОСТУПУ [Електронний ресурс]. – Режим доступу: https://cqr.company/ua/web-vulnerabilities/access-control-weaknesses/

31. Контроль доступу (Access control) до інформації як один із ключових елементів інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://bsoprivacygroup.com/gdpr-personal-data-access-control/

32. Lack of encryption the primary reason for sensitive data loss [Електронний ресурс]. – Режим доступу: https://www.securitymagazine.com/articles/100227-lack-of-encryption-the-primary-reason-for-sensitive-data-loss

33. Cyber Security Monitoring (5 Key Components) [Електронний ресурс]. – Режим доступу: https://www.bitsight.com/blog/5-things-to-consider-building-continuous-security-monitoring-strategy

34. Модель Загроз Та Модель Порушника [Електронний ресурс]. – Режим доступу:
https://ru.scribd.com/document/600094249/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C-%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7-%D0%A2%D0%B0-%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C-%D0%9F%D0%BE%D1%80%D1%83%D1%88%D0%BD%D0%B8%D0%BA%D0%B0

35. Моделі загроз та моделі порушника [Електронний ресурс]. – Режим

доступу: https://e-tk.lntu.edu.ua/pluginfile.php/25376/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2017.pdf

36. Поняття про модель загроз та модель порушника [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/5992570/page:5/

37. Побудова моделі загроз інфокомунікаційної мережі підприємства [Електронний ресурс]. – Режим доступу: https://openarchive.nure.ua/bitstreams/5ac338d2-b62e-4580-97b8-2e7901d8bb82/download

38. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.) [Електронний ресурс]. – Режим доступу: http://kist.ntu.edu.ua/textPhD/tzi.pdf

39. Кібервійна росії проти України [Електронний ресурс]. – Режим доступу: https://speka.media/kiberviina-rosiyi-proti-ukrayini-9qy4ok

40. Russian cyber and information warfare in practice [Електронний ресурс]. – Режим доступу: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice

41. Технічні методи і засоби захисту інформації [Електронний ресурс]. – Режим доступу: https://e-tk.lntu.edu.ua/mod/resource/view.php?id=3266

42. Welcome to VirtualBox.org! [Електронний ресурс]. – Режим доступу: https://www.virtualbox.org/

43. Можливості Oracle VM VirtualBox [Електронний ресурс]. – Режим доступу: https://www.oracle.com/ua/virtualization/virtualbox/#rc30p3

44. How to Use VirtualBox: Quick Overview [Електронний ресурс]. – Режим доступу: https://www.nakivo.com/blog/use-virtualbox-quick-overview/

45. How to run an Ubuntu Desktop virtual machine using VirtualBox 7 [Електронний ресурс]. – Режим доступу: https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox#1-overview

46. Open Source Edge: Secure & Fast [Електронний ресурс]. – Режим доступу:

https://ubuntu.com/

47. Air gap (air gapping) [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/whatis/definition/air-gapping#:~:text=An%20air%20gap%20is%20a,other%20computers%20or%20network%20devices.

48. What is an Air Gap? Air Gapping and Cybersecurity [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=rh3yG8fsYA8

49. Air Gapping: Offline Backups Ensure Recovery [Електронний ресурс]. – Режим доступу: https://www.arcserve.com/blog/air-gapping-offline-backups-ensure-recovery

50. What Is Air Gap and How Does It Impact Your Cybersecurity? [Електронний ресурс]. – Режим доступу: https://softteco.com/blog/what-is-air-gap#what-is-an-air-gap

51. What are Air-Gapped Backups? How Air-Gapped Backups Work [Електронний ресурс]. – Режим доступу: https://stonefly.com/resources/what-are-air-gapped-backups/

52. Flex Appliance Isolated Recovery Environment (IRE) Air Gap Solution Deployment Guide [Електронний ресурс]. – Режим доступу: https://sort.veritas.com/DocPortal/pdf/FlexAirGapIRE

53. Кібербезпека: актуальні загрози та методи захисту [Електронний ресурс]. – Режим доступу: https://lemon.school/blog/kiberbezpeka-aktualni-zagrozy-ta-metody-zahystu

ДОДАТОК А

Тези наукових доповідей

1. IX International Conference of Students, PhD Students and Young Scientists "Engineer of XXI Century" 10th December 2021 - "Research of methods and means of protection of centralized and distributed information systems" Valeriia Solodovnyk, Yuliia Stepanenko, Larysa Myrytenko, Andrii Fesenko, Natalia Lukova-Chuiko

Статті в іноземних виданнях

2. IX International Conference of Students, PhD Students and Young Scientists "Engineer of XXI Century" 6th December 2019 - "Analysis of SDN network management by software" Dakov Serhiy, Valeriia Solodovnyk
3. 2nd International Conference of Cuber Hygiene & Conflict Management in Global Information Networks - "Assessment of the introduction of agents to detect the impact of system level cyber attacs on increasing the data processing center security level«Serhii Toliupa, Yanina Shestak, Ogbu James Onyigwang, Valeriia Solodovnyk
4. "IT&I 2020 Information Technology and Interactions". Тема: "RF Signals Encryption with AES in WDID96-105 Serhii Toliupa, Volodymyr Nakonechnyi, Maksym Kotov, Valeriia Solodovnyk".
5. IX International Conference of Students, PhD Students and Young Scientists "Engineer of XXI Century" 11th December 2020 - "Algorithm of load Balance optimization on hardware resources of information systems» Larysa Murytenko, Valeriia Solodovnyk, Yanina Shestak
6. IX International Conference of Students, PhD Students and Young Scientists "Engineer of XXI Century" 10th December 2021 - "Secure password storage with

cryptographic hash function" Yuliia Stepanenko, Valeriia Solodovnyk, Andrii Fesenko, Larysa Myrytenko

7. IT&I 2023 Information Technology and Interactions 21 листопада 2023 «VULNERABILITY SCANNER FOR BLOCKCHAIN SMART CONTRACTS» Serhii Toliupa Yaroslav Kulaha Valeriia Solodovnyk
8. Міжнародна наукова конференція молодих учених, аспірантів і здобувачів освіти «Інформаційні системи та технології — науковий та практичний підхід» 06 березня 2024 «Fortifying Telecommunications: The Strategic Role of Network Function Virtualization in Enhancing Cybersecurity Valeriia Solodovnyk, Serhii Toliupa, Yaroslav Kulaha

Статті в індексованих міжнарожних виданнях

1. Scopus indexed publication: "RF signals encryption with AES in WDID Toliupa, S., Nakonechnyi, V., Kotov, M., Solodovnyk, V. CEUR Workshop Proceedingsthis link is disabled, 2021, 2845, pp. 96–105".

ДОДАТОК Б

Лістинг коду програми

```
#!/usr/bin/env python3
import os
import datetime
import logging
import subprocess
import tkinter as tk
from tkinter import messagebox
# Налаштування логування
def setup_logging():
# Конфігурація логування, включаючи шлях до файлу логу, рівень логування і формат повідомлень
log_file = '/var/log/backup.log'
log_level = logging.DEBUG
log_format = '%(asctime)s - %(levelname)s: %(message)s'
logging.basicConfig(filename=log_file, level=log_level, format=log_format)
# Створення директорії для бекапу
def create_backup_folder(base_dir):
#Створюється директорія для збереження бекапу на основі поточного часу.
date_stamp = datetime.datetime.now().strftime("%Y-%m-%d_%H-%M-%S")
backup_folder = os.path.join(base_dir, date_stamp)
os.makedirs(backup_folder, exist_ok=True)
return backup_folder
# Генерація назви файлу бекапу
def create_backup_filename(source_dir, date_stamp):
#Формування назви файлу резервної копії на основі назви директорії і дати.
```

```
return f"backup_{os.path.basename(source_dir)}_{date_stamp}.tar.gz"
# Виконання бекапу
def perform_backup(source_dir, backup_base_dir):
backup_folder = create_backup_folder(backup_base_dir)
date_stamp = datetime.datetime.now().strftime("%Y-%m-%d_%H-%M-%S")
backup_filename = create_backup_filename(source_dir, date_stamp)
backup_full_path = os.path.join(backup_folder, backup_filename)
tar_command = ["tar", "-czf", backup_full_path, "-C", source_dir, "."]
run_backup_command(tar_command, source_dir, backup_full_path)
# Виконання команди tar
def run_backup_command(command, source_dir, backup_path):
#Виконує команду для створення архіву і обробляє результати виконання.
try:
subprocess.run(command, check=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)
log_backup_success(source_dir, backup_path)
show_success_message()
except subprocess.CalledProcessError as e:
log_backup_failure(source_dir, e)
# Логування успішного бекапу
def log_backup_success(source_dir, backup_path):
#Логування успішного створення бекапу.
success_message = f"Backup of {source_dir} created successfully at {backup_path}"
print(success_message)
logging.info(success_message)
# Логування помилки бекапу
def log_backup_failure(source_dir, error):
#Логування помилки при створенні бекапу.
error_message = f"Failed to create backup of {source_dir}: {error.stderr.decode()}"
print(error_message)
```

```
logging.error(error_message)
# Відображення повідомлення про успіх у GUI
def show_success_message():
#Відобаження GUI повідомлення про успішне створення резервної копії.
msg = tk.Tk()
msg.withdraw()
messagebox.showinfo("Success", "Backup created successfully")
msg.destroy()
root->msg (can it be changed?)
# Основна функція
def main():
#Головна функція для ініціалізації логування та запуску процесу бекапу.
setup_logging()
source_dirs = ["/mnt/nfs/desktop1_data", "/mnt/nfs/desktop2_data"]
backup_base_dir = "/home/valeriiabd/Desktop/backups"
for source_dir in source_dirs:
perform_backup(source_dir, backup_base_dir)
if __name__ == "__main__":
main()
```