ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

« «Підвищення безпеки збору та зберігання даних
про ПК у мережі за допомогою віртуалізації на прикладі GLPI»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ярослав ЮРЧЕНКО
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСД-42
Ярослав ЮРЧЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Іван ШАХМАТОВ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти бакалавр
Спеціальність Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІПЗАС
_____Каміла СТОРЧАК
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Юрченко Ярославу Владиславовичу

(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Підвищення безпеки збору та зберігання даних про ПК у мережі за допомогою віртуалізації на прикладі GLPI

керівник кваліфікаційної роботи Іван ШАХМАТОВ
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Науково-технічна література з теми бакалаврської роботи.
2. Принцип функціонування «розумного будинку».
3. Основні принципи гейміфікації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Гейміфікація. Визначення та прийоми
2. Інструменти та прийоми розробки мобільних додатків
3. Розробка мобільного додатку системи управління розумного будинку з використанням елементів гейміфікації

5. Ілюстративний матеріал: *презентація*

6. Дата видачі завдання: «27» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз актуальності проблеми	27.02-05.03.2024	
2	Аналіз літературних джерел	06.03-11.03.2024	
3	Збір інформації	12.03-18.03.2024	
4	Огляд та порівняння існуючих алгоритмів та методів	19.03-27.03.2024	
5	Аналіз існуючих програмних продуктів	28.03-05.04.2024	
6	Обґрунтування вибору засобів розробки	05.04-09.04.2024	
7	Представлення вхідних даних	10.04-16.04.2024	
8	Моделювання роботи інтелектуальної складової програмного забезпечення GLPI	17.04-22.04.2024	
9	Практична реалізація	23.04-02.05.2024	
10	Тестування	03.05-10.05.2024	
11	Результати	11.05-16.05.2024	
12	Висновки по роботі та підготовка додаткового матеріалу	17.05-21.05.2024	
13	Підготовка та оформлення презентації для доповіді	22.05-24.05.2024	

Здобувач(ка) вищої освіти _____ Ярослав ЮРЧЕНКО

Керівник
кваліфікаційної роботи _____ Іван ШАХМАТОВ

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи ««Підвищення безпеки збору та зберігання даних про ПК у мережі за допомогою віртуалізації на прикладі GLPI» виконана на 60 сторінках, містить 30 рисунків, 10 таблиць, 2 додатків та список використаної літератури з 20 найменувань.

Мета кваліфікаційної роботи полягає у підвищенні безпеки збору та зберігання даних про персональні комп'ютери у мережі за допомогою віртуалізації на прикладі використання інформаційної системи GLPI.

Об’єктом дослідження є процеси збору, зберігання та захисту даних про персональні комп'ютери в мережі.

Предметом дослідження є методи підвищення безпеки збору та зберігання даних про персональні комп'ютери в мережі за допомогою віртуалізації, зокрема на прикладі використання інформаційної системи GLPI.

Методи дослідження включають в себе: вивчення теоретичних аспектів безпеки даних, загроз, методів захисту та законодавчих вимог, порівняння різних інформаційних систем та технологій віртуалізації для визначення найефективніших засобів захисту даних, розробка архітектури системи з використанням віртуалізації для підвищення безпеки даних, налаштування та тестування інформаційної системи GLPI для оцінки її ефективності в реальних умовах, аналіз та оцінка результатів впровадження системи, виявлення сильних та слабких сторін, обробка та інтерпретація зібраних даних для формування висновків та рекомендацій.

Теоретичні дослідження складалися з огляду літератури, включаючи наукові статті, технічні документи та інші публікації, щоб зрозуміти основи технологій безпеки даних, віртуалізації, а також методів і засобів захисту інформації в мережах.

Наукова новизна одержаних результатів визначається розробкою та впровадженням нових методів підвищення безпеки збору та зберігання даних про персональні комп'ютери в мережі за допомогою віртуалізації, а також практичним застосуванням інформаційної системи GLPI для цих цілей.

Практичне значення одержаних результатів роботи полягає у можливості впровадження розробленої системи для підвищення безпеки збору та зберігання даних про персональні комп'ютери в реальних мережах організацій, що забезпечить надійний захист інформації та підвищить загальний рівень кібербезпеки. Впровадження рекомендацій та використання інформаційної системи GLPI дозволить ефективно управляти даними, зменшити ризики витоку інформації та оптимізувати процеси адміністрування IT-інфраструктури.

Ключові слова: безпека даних, віртуалізація, збір даних, зберігання даних, GLPI, інформаційні системи, кібербезпека, адміністрування мережі, захист інформації, IT-інфраструктура.

ABSTRACT

The explanatory note of the qualification work "Improving the security of data collection and storage of PCs in the network using virtualization on the example of GLPI" is made on 60 pages, contains 30 figures, 10 tables, 2 appendices and a list of used literature of 20 items.

The purpose of the qualification work is to increase the security of data collection and storage of personal computers in the network using virtualization using the GLPI information system as an example.

The object of research is the processes of collecting, storing and protecting data about personal computers in the network.

The subject of the study is methods of increasing the security of data collection and storage of personal computers in the network using virtualization, in particular, using the GLPI information system as an example.

Research methods include: study of theoretical aspects of data security, threats, protection methods and legal requirements, comparison of various information systems and virtualization technologies to determine the most effective means of data protection, development of system architecture using virtualization to improve data security, configuration and testing of the information system GLPI to evaluate its effectiveness in real conditions, analysis and evaluation of the results of system implementation, identification of strengths and weaknesses, processing and interpretation of collected data to form conclusions and recommendations.

The theoretical research consisted of a literature review, including scientific articles, technical papers and other publications, to understand the basics of data security technologies, virtualization, and methods and means of protecting information in networks.

The scientific novelty of the obtained results is determined by the development and implementation of new methods of increasing the security of data collection and storage of personal computers in the network using virtualization, as well as the practical application of the GLPI information system for these purposes.

The practical significance of the obtained work results lies in the possibility of implementing the developed system to improve the security of data collection and storage of personal computers in real networks of organizations, which will ensure reliable protection of information and increase the overall level of cyber security. The implementation of recommendations and the use of the GLPI information system will allow effective data management, reduce the risks of information leakage and optimize IT infrastructure administration processes.

Keywords: data security, virtualization, data collection, data storage, GLPI, information systems, cyber security, network administration, information protection, IT infrastructure.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

API – Application Programming Interface

VPN - Virtual Private Network (віртуальна приватна мережа)

MPLS - Multi-Protocol Label Switching (багатопротокольна комутація міток)

SLA - Service Level Agreement (угода про рівень обслуговування)

WAN - Wide Area Network (глобальна мережа)

LAN - Local Area Network (локальна мережа)

NFV - Network Functions Virtualization (віртуалізація мережевих функцій)

CPE - Customer Premises Equipment (обладнання на території клієнта)

OSPF - Open Shortest Path First (відкритий протокол найкоротшого шляху)

IPSec - Internet Protocol Security (протокол безпеки Інтернету)

GRE - Generic Routing Encapsulation (загальна інкапсуляція маршрутизації)

HTTP - HyperText Transfer Protocol (протокол передачі гіпертексту)

HTTPS - HyperText Transfer Protocol Secure (захищений протокол передачі гіпертексту)

TLS - Transport Layer Security (захист транспортного рівня)

SSL - Secure Sockets Layer (рівень захищених сокетів)

DNS - Domain Name System (система доменних імен)

DHCP - Dynamic Host Configuration Protocol (протокол динамічної конфігурації вузла)

ВСТУП

Атуальність теми. Сучасний розвиток інформаційних технологій супроводжується зростанням обсягів даних, які обробляються та зберігаються в комп'ютерних системах. Захист цих даних від несанкціонованого доступу, витоку чи пошкодження стає надзвичайно важливою задачею для багатьох організацій та користувачів.

Об’єктом дослідження є процеси збору, зберігання та захисту даних про персональні комп'ютери в мережі.

Предметом дослідження є методи підвищення безпеки збору та зберігання даних про персональні комп'ютери в мережі за допомогою віртуалізації, зокрема на прикладі використання інформаційної системи GLPI.

Наукова новизна одержаних результатів визначається розробкою та впровадженням нових методів підвищення безпеки збору та зберігання даних про персональні комп'ютери в мережі за допомогою віртуалізації, а також практичним застосуванням інформаційної системи GLPI для цих цілей.

Наукова новизна одержаних результатів визначається розробкою та впровадженням нових методів підвищення безпеки збору та зберігання даних про персональні комп'ютери в мережі за допомогою віртуалізації, а також практичним застосуванням інформаційної системи GLPI для цих цілей.

Завдання дослідження:

1. Аналіз сучасних методів та технологій забезпечення безпеки даних у мережах.
2. Проектування архітектури системи підвищення безпеки даних з використанням віртуалізації.
3. Реалізація та тестування запропонованих рішень.

1 ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ ДАНИХ

1.1 Основні принципи безпеки даних

Безпека даних в сучасному цифровому середовищі є критично важливою для забезпечення конфіденційності, цілісності та доступності інформації. Основні принципи безпеки даних визначають стратегічний підхід до захисту інформації від різних загроз. Загальні принципи безпеки інформації включають:

1. Принцип конфіденційності, який передбачає, що доступ до конфіденційної інформації мають мати лише уповноважені особи. Для забезпечення конфіденційності дані повинні бути захищені від несанкціонованого доступу за допомогою різних методів, таких як шифрування, аутентифікація та авторизація.

2. Принцип цілісності, який гарантує, що дані залишаються недоторканими та не зазнають непередбачених змін або пошкоджень. Для досягнення цілісності дані можуть бути захищені від внутрішніх та зовнішніх змін за допомогою методів контролю доступу та механізмів перевірки цілісності.

3. Принцип доступності, який забезпечує доступ до даних і гарантує, що авторизовані користувачі можуть отримати доступ до необхідної інформації у відповідний момент часу. Цей принцип передбачає використання резервних копій даних, механізмів відновлення та інших методів забезпечення неперервності бізнесу.Важливим аспектом забезпечення безпеки даних є інтеграція цих принципів в загальну стратегію кібербезпеки організації. Здійснення відповідних заходів щодо захисту даних допоможе уникнути потенційних загроз і забезпечити безпеку інформаційних ресурсів.

Рисунок 1.1 – Основні принципи безпеки

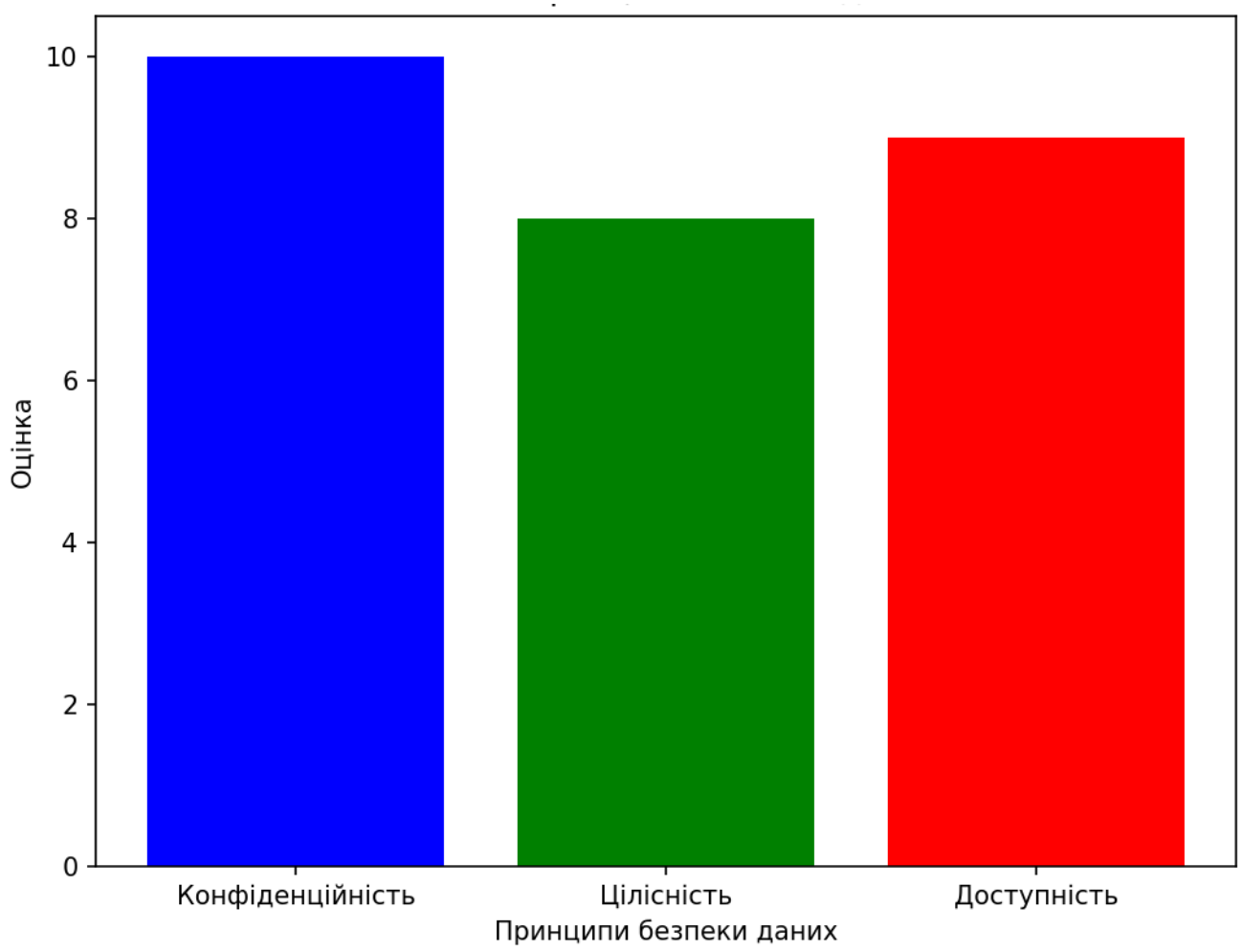

Рисунок 1.2 –Загальні принципи безпеки

1.2 Типи загроз безпеці даних у мережі

В сучасному цифровому середовищі існують різноманітні типи загроз, які можуть стати причиною порушення безпеки даних у мережі. Розуміння цих загроз дозволяє краще захищати інформацію та приймати відповідні заходи для запобігання можливим атакам. Ці загрози безпеці даних становлять серйозний ризик для організацій та користувачів, тому важливо мати належні заходи захисту для запобігання їхньому виникненню та вчасному реагуванню в разі потреби. Найпоширеніші типи загроз включають:

1. Вірусні програми, які мають здатність розмножуватися та поширюватися самостійно шляхом вбудованняся в інші файли або програми. Віруси можуть завдати шкоди системам, шифруючи або видаляючи дані, а також виконуючи небажані дії без дозволу користувача.

2. Хакерські атаки можуть включати в себе різноманітні методи, такі як перехоплення даних, внедрення шкідливого програмного забезпечення або незаконний доступ до системи з метою крадіжки конфіденційної інформації або завдання шкоди.

3. Соціально-інженерні атаки, в яких атакуючий намагається отримати конфіденційну інформацію, таку як паролі або дані банківських карток, шляхом використання підробленого веб-сайту або електронної пошти.

4. Конфіденційна інформація втікає з мережі чи комп'ютерної системи. Витоки даних можуть бути спричинені злому безпеки, недбалістю адміністраторів або несправностями в програмному забезпеченні.

Таблиця 1.1

Додаткові технічні аспекти типів загроз

№	Назва	Опис
1	Віруси	можуть бути розповсюджені через заражені файли, електронну пошту, веб-сайти або USB-пристрої
		можуть виконувати різні дії, включаючи знищення файлів, перекривання системних ресурсів, крадіжку конфіденційної інформації або встановлення задніх дверей для незаконного доступу.
		можуть бути прихованими і виявлятися лише під час певних умов, наприклад, після певної дати або події.
2	Хакерські атаки	хакерські атаки можуть бути різними за природою, включаючи атаки з використанням вразливостей програмного забезпечення, перехоплення пакетів даних, атаки методом "людина по середині" (Man-in-the-Middle), атаки на ідентифікацію та автентифікацію, фальшиві логіни тощо.
3	Фішинг	можуть використовувати підроблені веб-сайти, електронну пошту або повідомлення в соціальних мережах для обману користувачів і викликати їх до надання конфіденційної інформації.
		можуть призвести до крадіжки облікових даних, банківських карток, паролів тощо.
4	Витоки даних	можуть стати наслідком недостатньої захищеності мережевих з'єднань, недбалості адміністраторів або недоліків в програмному забезпеченні.

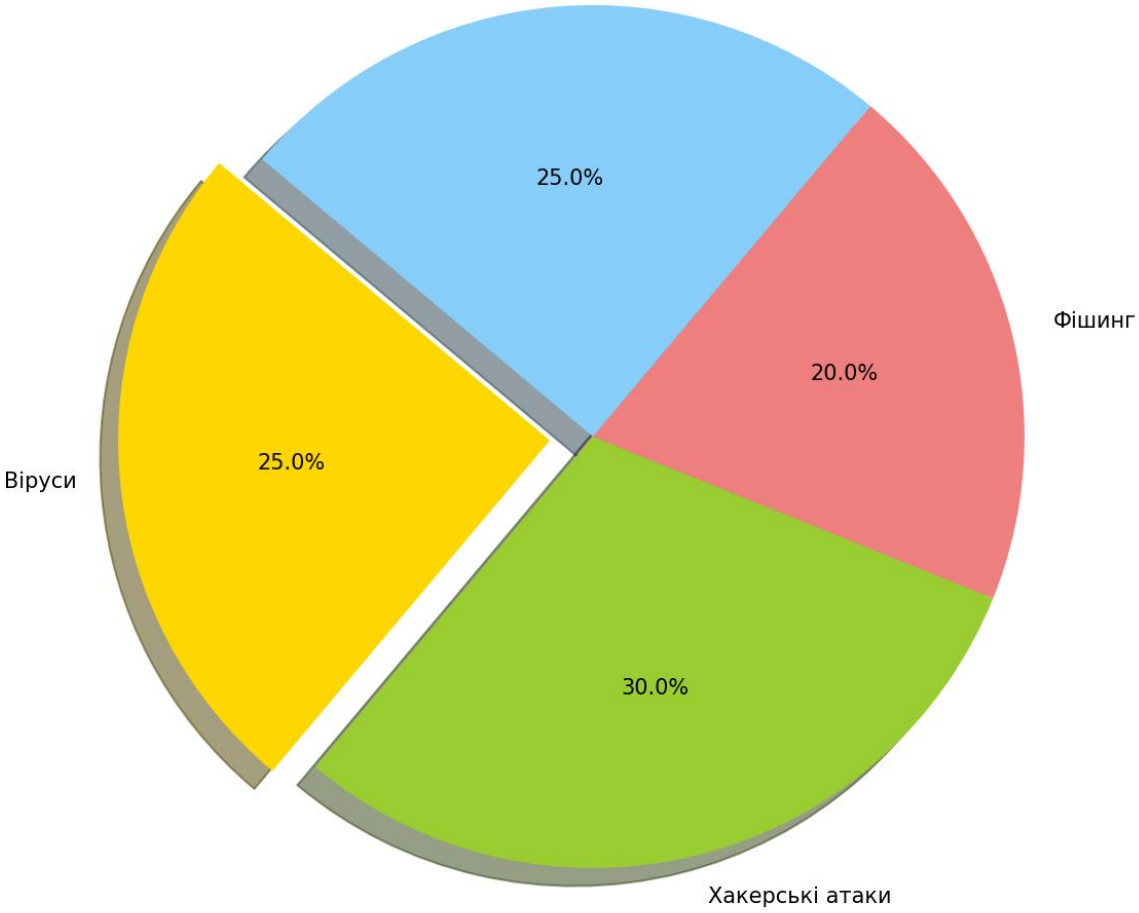

Рисунок 1.3 – Основні загрози в компютерних технологіях

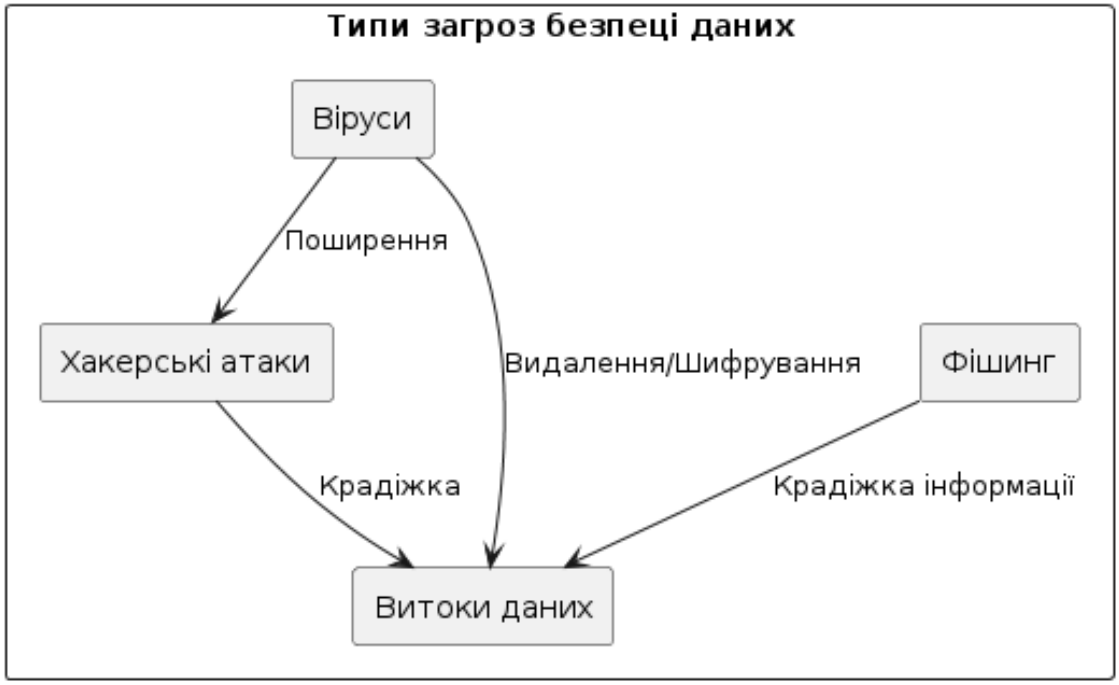

Рисунок 1.4 – Типи загроз в безпеці даних

1.3 Методи аутентифікації та авторизації

Методи аутентифікації та авторизації допомагають забезпечити високий рівень безпеки збору та зберігання даних про ПК у мережі за допомогою віртуалізації, такої як GLPI. Реалізація цих методів може бути важливим кроком для захисту конфіденційної інформації та запобігання несанкціонованому доступу до системи. Детальний огляд методів аутентифікації та авторизації у контексті підвищення безпеки збору та зберігання даних про ПК у мережі за допомогою віртуалізації, на прикладі системи управління даними GLPI включає:

Таблиця 1.2

Методи аутентифікації та авторизації

Метод	Назва	Опис
Методи аутентифікації	Логін/пароль	Це найпоширеніший метод аутентифікації, де користувач повинен ввести ім'я користувача та пароль для доступу до системи
	Двофакторна аутентифікація (2FA)	Застосування двох різних методів для підтвердження ідентичності, наприклад, пароля та SMS-коду, токена або біометричних даних
	Одноразові паролі (OTP)	Користувач отримує унікальний одноразовий код для кожної сесії або транзакції, який потрібно ввести разом із звичайним паролем
	Біометрична аутентифікація	Використання біометричних даних, таких як відбитки пальців, сканування обличчя або розпізнавання голосу, для підтвердження ідентичності користувача

Продовження таблиці 1.2

Метод	Назва	Опис
Методи авторизації	Ролева модель доступу	Надання прав доступу на основі ролей користувачів у системі. Наприклад, адміністратор має повний доступ, тоді як звичайний користувач може мати обмежений доступ лише до певних функцій
	Управління правами доступу (RBAC)	Визначення прав доступу на основі об'єктів та дій у системі. Кожному користувачеві присвоюється певна роль або група, яка містить набір прав доступу.
	Автоматичне скасування доступу	Система може автоматично скасовувати доступ після певного часу бездіяльності або у випадку порушення правил безпеки
	Моніторинг і аналіз активності	Відстеження дій користувачів у системі для виявлення незвичайних або підозрілих активностей, що може вказувати на небезпечні дії.

На рис. 1.5 показано: система з двома основними модулями: модулем аутентифікації та модулем авторизації. Модуль аутентифікації відповідає за перевірку ідентичності користувача, тоді як модуль авторизації визначає, які дії можуть виконувати користувачі після успішної аутентифікації. База даних користувачів використовується для зберігання облікових записів користувачів та їх прав доступу.

Рисунок 1.5 – Модулі аутентифікації та авторизації

1.4 Криптографічні методи захисту інформації

Криптографічні методи є ключовим елементом в забезпеченні безпеки даних, особливо в мережевому середовищі. Вони використовуються для захисту конфіденційності, цілісності та автентичності інформації.

Симетричне шифрування використовує один ключ для як шифрування, так і розшифрування даних. Наприклад, AES (Advanced Encryption Standard). Асиметричне шифрування використовує пару ключів: публічний ключ для шифрування і приватний ключ для розшифрування. Наприклад, RSA (Rivest–Shamir–Adleman).

Також, хешування даних використовується для створення хеш-значення з вхідних даних за допомогою хеш-функцій, таких як SHA-256. Хеш-значення може бути використане для перевірки цілісності даних.

Використовується для підтвердження автентичності повідомлення та непередавання ним змісту цифровий підпис. Використовується асиметричне шифрування для створення та перевірки підпису. Протоколи обміну ключами забезпечують безпечний обмін ключами між сторонами для наступного симетричного шифрування. Наприклад, протокол Діффі-Геллмана. Використовує принципи квантової механіки для забезпечення безпеки комунікацій, зокрема квантове шифрування та дистанційне визначення ключа.

Використання вищевказаних криптографічних методів сприяє створенню безпечного середовища для збору та зберігання даних про ПК у мережі за допомогою віртуалізації на прикладі системи управління даними GLPI.

Рисунок 1.6 – Криптографічні методи захисту інформації

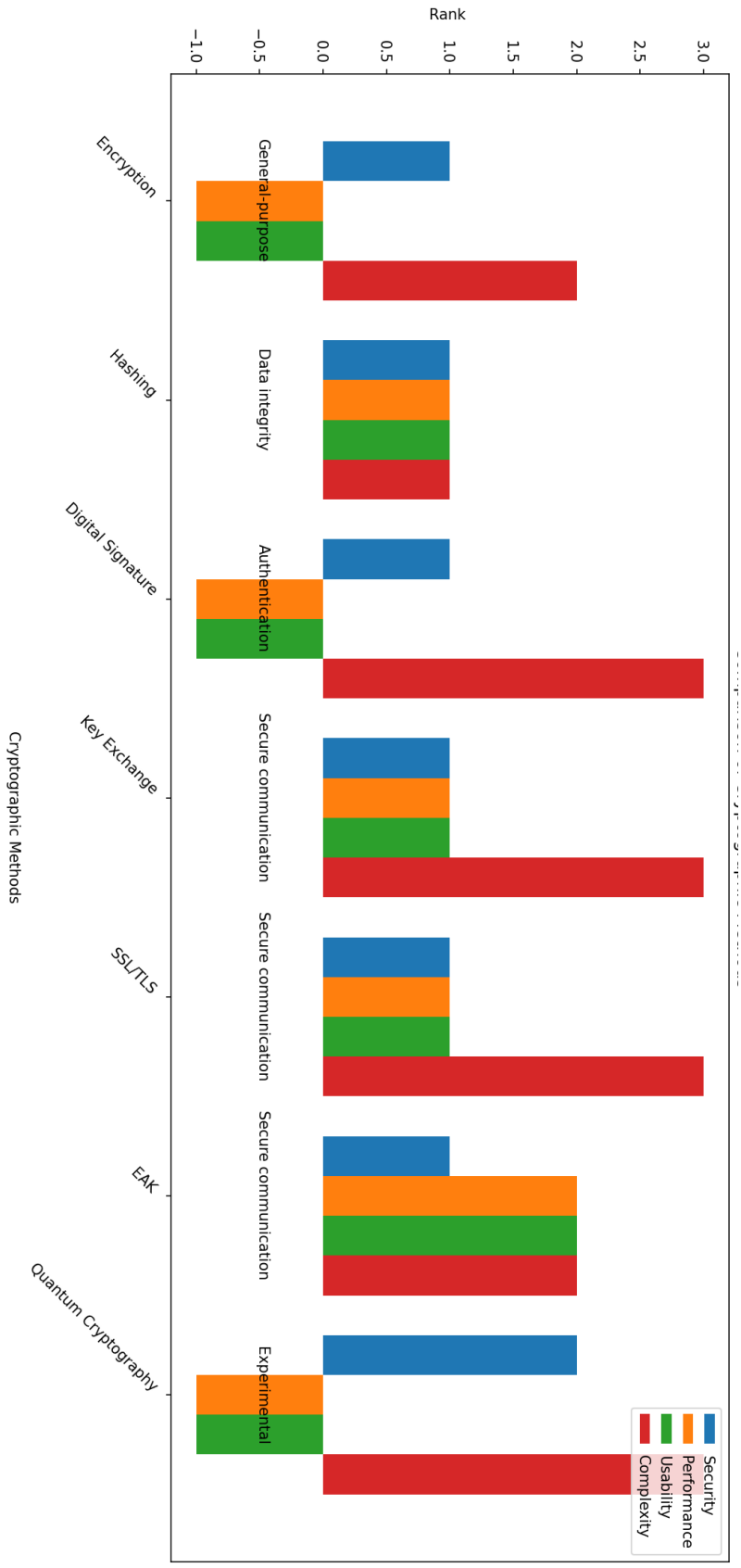

Рисунок 1.7 – Порівняння криптографічних методів

1.5 Засоби захисту інформації на ПК

На ПК можна використовувати різні засоби захисту для забезпечення безпеки даних та зменшення ризиків витоку чи несанкціонованого доступу до інформації. Засоби захисту інформації на ПК включають антивірусне програмне забезпечення для виявлення та видалення шкідливого програмного забезпечення, фаєрволи для контролю мережевого трафіку та блокування небажаних з'єднань, антишпигунське програмне забезпечення для виявлення та видалення шпигунських програм, шифрування даних для захисту конфіденційної інформації, резервне копіювання для збереження дублікатів важливих даних, безпека паролів для захисту облікових записів, оновлення програмного забезпечення для усунення вразливостей, фізична безпека для обмеження фізичного доступу до комп'ютера та блокування спаму та фішингу для захисту від небажаної електронної пошти та шахрайства.

Рисунок 1.8 – Схема захисту інформації на ПК

1.6 Законодавча база з питань безпеки даних

В сучасному світі, де цифрові дані стають все більш цінними та чутливими, законодавство з питань безпеки даних відіграє ключову роль у захисті прав та конфіденційності користувачів. Такі законодавчі акти і нормативні вимоги регулюють збір, зберігання, обробку та передачу особистих даних, а також встановлюють відповідальність за їх неналежне використання.

Регулюючий акт «GDPR» Європейського Союзу, який визначає права та обов'язки щодо захисту особистих даних громадян ЄС. GDPR вимагає від компаній забезпечувати адекватний рівень захисту даних, здійснювати інформування користувачів про збір та використання їх даних, а також піддаватися обов'язковому повідомленню про порушення безпеки даних.Стандарт Payment Card Industry Data Security Standard (PCI DSS) встановлює вимоги щодо захисту кредитних карткових даних. Він вимагає від організацій, що обробляють платіжні дані, виконувати ряд технічних заходів безпеки, таких як захищене зберігання та передача даних, регулярне виявлення і усунення вразливостей тощо.

Вищевкзані законодавчі акти та стандарти регулюють безпеку даних та захист приватності інформації в різних країнах і галузях діяльності. Вони є важливими для забезпечення довіри користувачів та ефективного управління ризиками в сфері обробки даних.

1.7 Висновки до розділу

В розділі "Теоретичні основи безпеки даних" було представлено комплексний огляд основних принципів, типів загроз, методів аутентифікації та авторизації, криптографічних методів захисту інформації, засобів захисту інформації на ПК та законодавчої бази з питань безпеки даних. Розглянуті теми надають необхідний фундамент для розробки та впровадження ефективних стратегій безпеки даних у сучасному інформаційному середовищі. Висновки

розділу підкреслюють важливість розуміння та застосування основних принципів та методів безпеки для забезпечення надійного захисту інформації.

2 ПРОЕКТУВАННЯ СИСТЕМИ ПІДВИЩЕННЯ БЕЗПЕКИ

2.1 Вибір оптимальної інформаційної системи для підвищення безпеки

Підвищення безпеки даних - це важлива задача для будь-якої організації. Вибір оптимальної інформаційної системи для цього має велике значення.

– ретельно проаналізувати потреби організації щодо безпеки даних: обсяг даних, типи даних, їх чутливість, регулятивні вимоги та інші фактори.

– визначити потенційні загрози безпеці даних, які можуть виникнути: зовнішні атаки, внутрішні загрози, природні катастрофи тощо.

– Після аналізу потреб і оцінки ризиків обрати інформаційну систему, яка найкращим чином відповідає вимогам організації.

– Після вибору системи реалізуйте її в організації. Це може включати налаштування, інтеграцію з існуючими системами, навчання персоналу та інші дії.

– після реалізації системи провести тестування для переконанняся, що вона працює належним чином.

– забезпечити постійну підтримку і оновлення системи безпеки даних. Це включає в себе виявлення і виправлення помилок, встановлення патчів безпеки та оновлення програмного забезпечення.

2.2 Аналіз вимог до системи зберігання даних

Аналіз вимог допоможе зрозуміти, які саме функції та можливості необхідні для забезпечення безпеки даних у системі GLPI та як ці вимоги можна втілити на практиці. Аналіз вимог до системи зберігання даних є ключовим етапом у процесі підвищення безпеки збору та зберігання інформації про ПК у мережі за допомогою віртуалізації, зокрема на прикладі системи GLPI. Для забезпечення ефективності та безпеки цієї системи, можна визначити наступні вимоги:

1. Система повинна забезпечувати конфіденційність даних, що зберігаються про ПК у мережі. Це означає, що лише авторизовані користувачі мають доступ до цієї інформації.

2. Система повинна гарантувати, що дані про ПК у мережі не піддаються незаконним змінам чи втратам. Всі зміни повинні бути відстежені та зареєстровані.

3. Інформація про ПК у мережі повинна бути доступною у разі потреби. Система повинна мати механізми резервного копіювання та відновлення даних для запобігання втратам у випадку непередбачених ситуацій.

4. Система повинна забезпечувати можливість моніторингу дій користувачів та аудиту доступу до даних. Це допоможе виявляти можливі порушення безпеки та вживати відповідних заходів.

5. Система повинна мати заходи захисту, які мінімізують ризики зовнішніх кібератак, таких як вторгнення та віруси.

6. Система повинна бути сумісною з існуючими інфраструктурними рішеннями організації та легко інтегруватися з ними.

2.3 Розробка методів підвищення безпеки

Розробка методів підвищення безпеки є ключовим етапом у проектуванні системи для захисту даних.

Використання алгоритмів шифрування, таких як AES (Advanced Encryption Standard) або RSA (Rivest-Shamir-Adleman), для захисту конфіденційної інформації. Для реалізації можна використовувати спеціалізовані бібліотеки або реалізувати власний шифрувальний алгоритм. Використання симетричного чи асиметричного шифрування, вибір довжини ключа, встановлення правильних режимів роботи шифрування (наприклад, ECB, CBC, CTR тощо).

Використання біометричних даних, які можуть включати в себе відбитки пальців, розпізнавання обличчя, сканування радужки тощо, для перевірки ідентичності користувача. Також можна використовувати двофакторну або мультифакторну аутентифікацію, поєднуючи кілька методів аутентифікації одночасно. Розробка інтерфейсів для збору біометричних даних, інтеграція з системами розпізнавання обличчя або відбитків пальців, використання криптографічних протоколів для безпечної передачі та зберігання біометричних даних.

Визначення різних ролей користувачів та призначення їм відповідних прав доступу до даних та функціональності системи. Реалізація механізмів авторизації та аутентифікації для перевірки доступу користувачів до різних ресурсів. Використання систем контролю доступу (наприклад, RBAC - Role-Based Access Control), реалізація механізмів ACL (Access Control Lists), використання токенів доступу для авторизації користувачів.

Створення системи моніторингу, яка відслідковує дії користувачів та події в системі. Реалізація журналування дій користувачів для подальшого аналізу та аудиту. Використання систем журналування (логування), встановлення спеціальних агентів моніторингу для відслідковування дій користувачів, аналіз журналів подій для виявлення аномалій та потенційних загроз.

Ці методи відображають технічні аспекти інформаційної безпеки та будуть використані для розробки систем захисту даних у відповідності до конкретних потреб організації.

2.4 Проектування архітектури системи з використанням віртуалізації

Проектування архітектури системи з використанням віртуалізації може бути ефективним підходом для підвищення безпеки та забезпечення ефективного використання ресурсів. За результатами проведеного прооеуктвання За результатами проведеного проектування архітектури системи з використанням віртуалізації було зясовано, що використання віртуалізації дозволяє ізолювати різні компоненти системи, що сприяє підвищенню безпеки даних та захисту від зовнішніх загроз. Ізольовані середовища дозволяють обмежити ризики злому та витоку даних між віртуальними машинами.

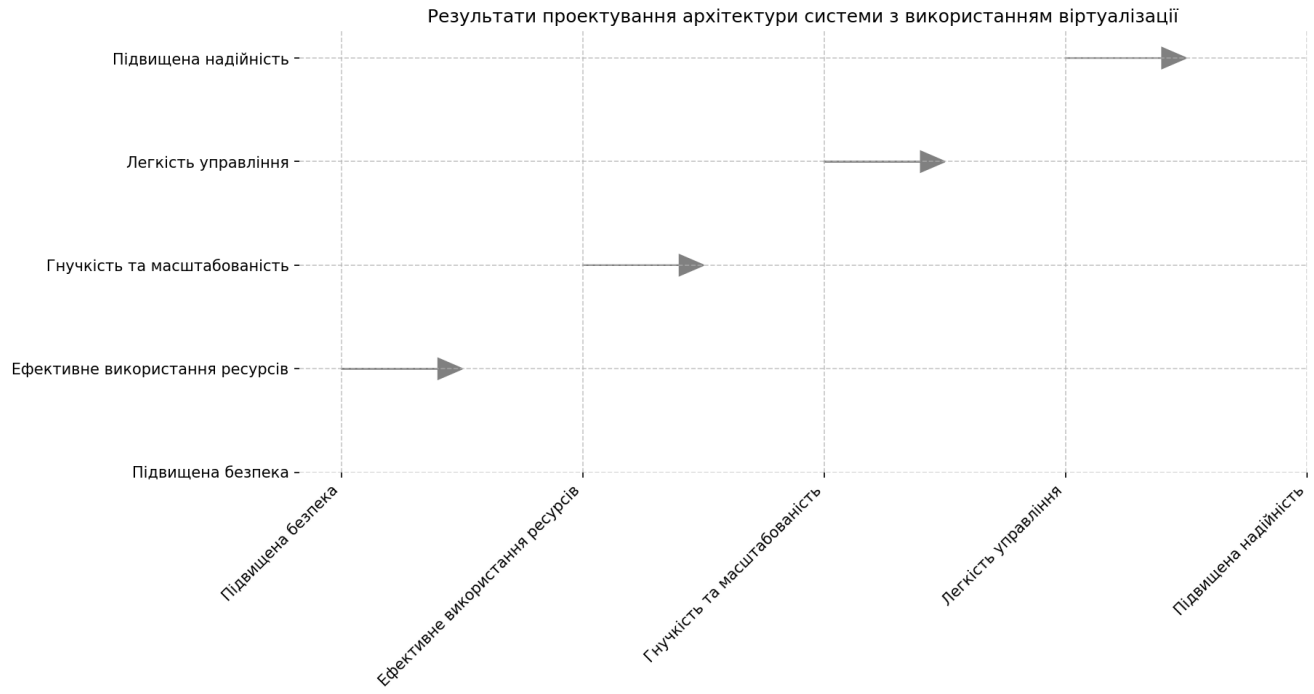

Рисунок 2.1 – Результати проведеного проектування архітектури системи з використанням віртуалізаці

Використання віртуалізації дозволяє оптимізувати використання фізичних ресурсів, таких як процесори, пам'ять та диск, за рахунок спільного використання ресурсів між віртуальними машинами та динамічного розподілу навантаження.

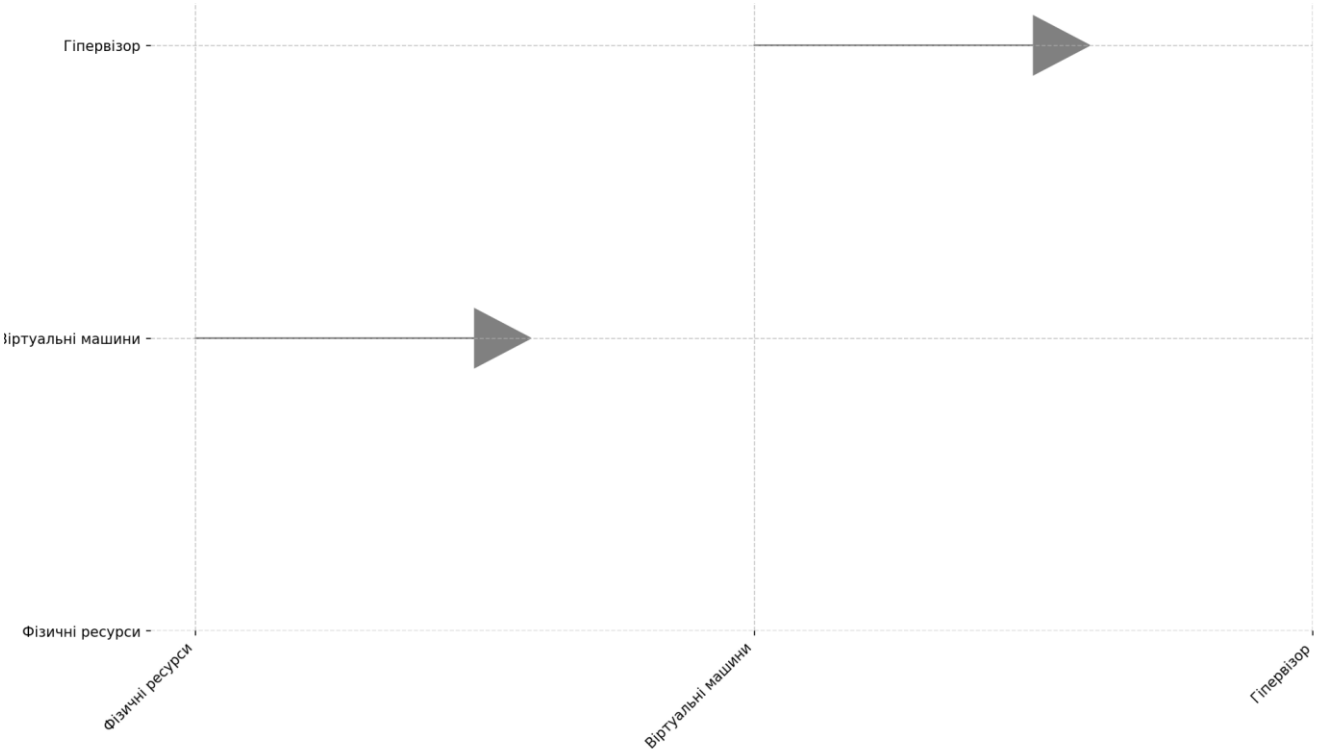

Рисунок 2.2 – Оптимізація використання фізичних ресурсів з використанням віртуалізації

Віртуалізація дозволяє швидко створювати та розгортати нові віртуальні машини або контейнери, що сприяє гнучкості та масштабованості системи. Це дозволяє вирішувати зростаючі потреби організації у відповідній мірі. Використання віртуалізації дозволяє оптимізувати використання фізичних серверів та зменшити кількість обладнання, що зменшує витрати на придбання та підтримку інфраструктури. Крім того, це допомагає зменшити енергоспоживання та вплив на довкілля.

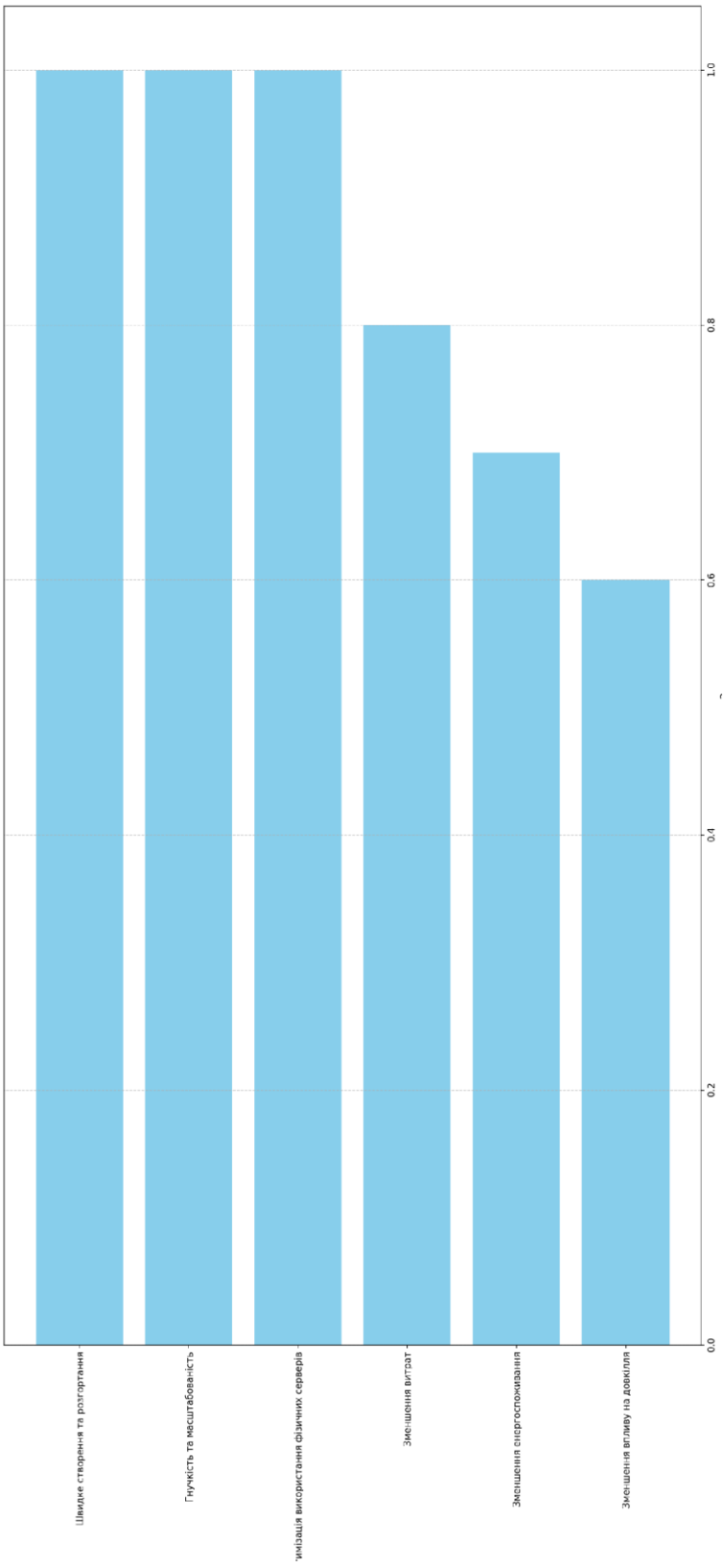

Рисунок 2.3 – Переваги використання віртуалізації

Віртуалізація спрощує управління та адмініструванням інфраструктури, оскільки дозволяє централізовано керувати віртуальними ресурсами та автоматизувати багато задач, такі як розгортання, масштабування та моніторинг.

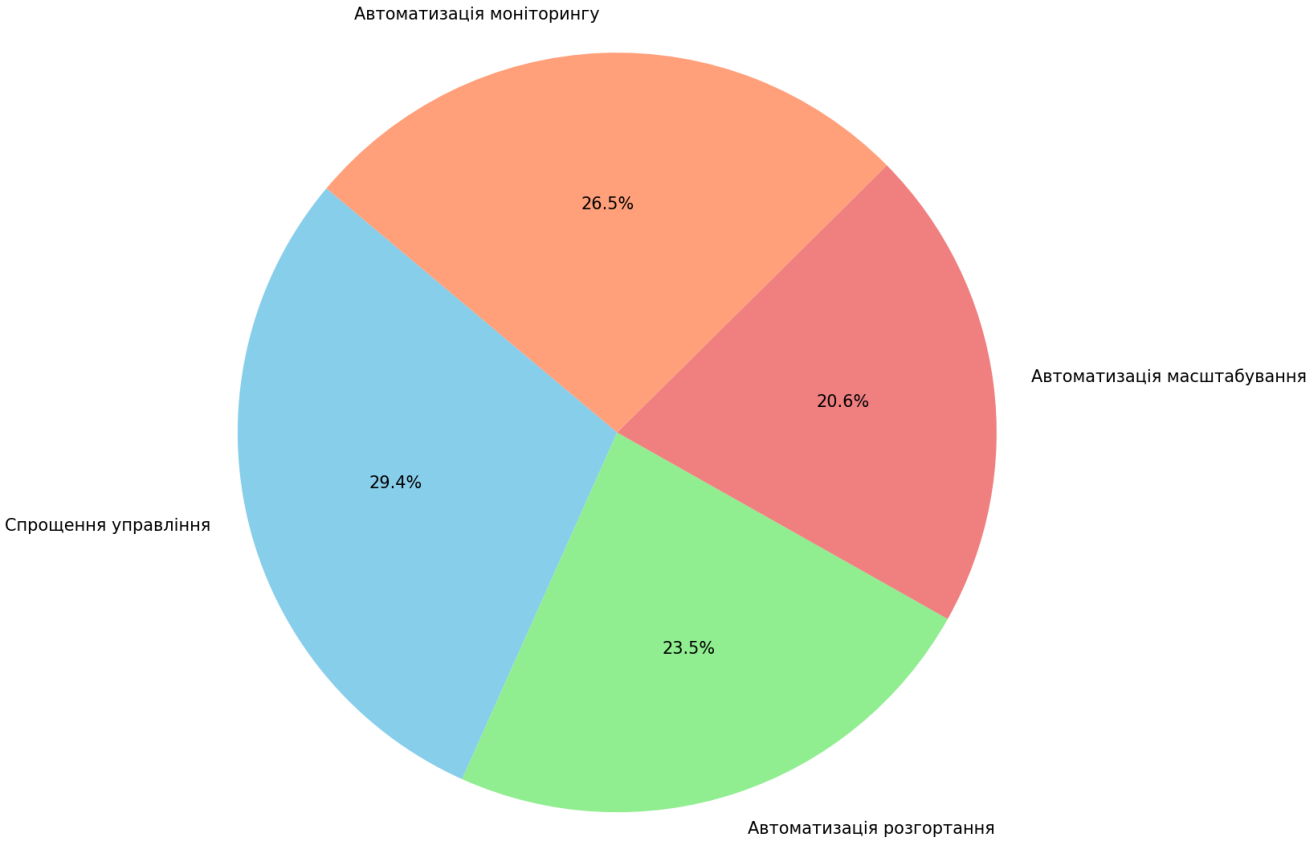

Рисунок 2.4 – Централізоване керування віртуальними ресурсами

Використання віртуалізації дозволяє створювати резервні копії віртуальних машин та швидко відновлювати систему у разі виникнення непередбачених ситуацій, що підвищує надійність та доступність системи.

2.5 Вибір засобів моніторингу та аудиту безпеки

Для підвищення безпеки збору та зберігання даних про ПК у мережі за допомогою віртуалізації на прикладі GLPI, важливо вибрати ефективні засоби моніторингу та аудиту безпеки. SIEM-системи, такі як Splunk, IBM QRadar, або Elasticsearch з модулем Beats, дозволяють централізовано збирати, аналізувати та моніторити дані щодо безпеки з різних джерел, включаючи журнали подій, потоки мережі, системні журнали та інші. Інструменти управління вразливостями, такі як Nessus, Qualys або OpenVAS, дозволяють виявляти та аналізувати потенційні вразливості в мережевих системах та додатках, що допомагає підтримувати їх у безпечному стані.

Інструменти моніторингу безпеки мережі, такі як Snort або Suricata, дозволяють виявляти та реагувати на загрози у реальному часі, перехоплюючи та аналізуючи мережевий трафік. Інструменти управління журналами, такі як ELK Stack (Elasticsearch, Logstash, Kibana) або Graylog, дозволяють збирати, аналізувати та візуалізувати журнали подій з різних джерел для виявлення потенційних загроз та вразливостей. Інструменти, такі як OpenSCAP або Nessus Compliance Checks, допомагають забезпечувати відповідність з регуляторними вимогами та стандартами безпеки, а також виконувати аудит системи для виявлення потенційних проблем безпеки. Інструменти управління активами, такі як GLPI, дозволяють відстежувати та керувати всіма активами в мережі, включаючи комп'ютери, сервери та програмне забезпечення, що допомагає забезпечити їх безпеку та відповідність.

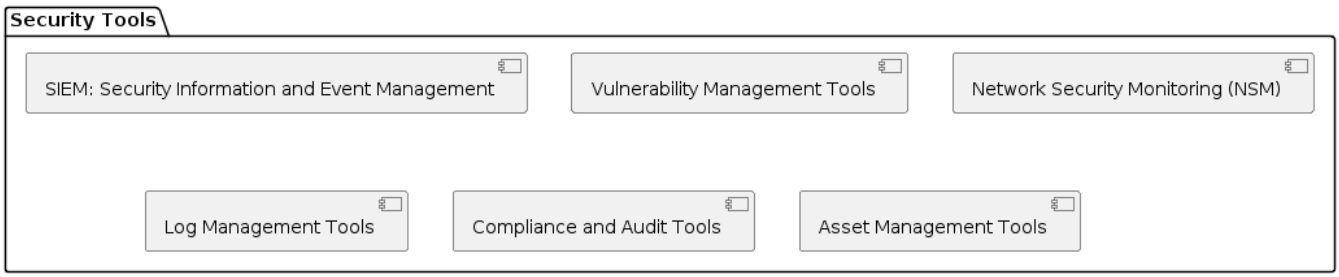

Рисунок 2.5 – Централізоване керування віртуальними ресурсами

Обираючи засоби моніторингу та аудиту безпеки, важливо враховано потреби організації, специфіку інфраструктури та рівень захисту, який потрібно досягти. Також важливо забезпечити інтеграцію цих засобів з існуючими системами управління та моніторингу для максимальної ефективності.

2.6 Висновки до розділу

В даному розділі досліджувалися різні аспекти вибору та застосування інформаційних систем для забезпечення безпеки в організаціях. Починаючи з аналізу вимог до системи зберігання даних та вибору оптимальних інформаційних систем, закінчуючи розробкою методів підвищення безпеки та вибором засобів моніторингу та аудиту. Застосування віртуалізації та використання відповідних інструментів моніторингу та аудиту дозволяє організаціям ефективно захищати свої дані та інфраструктуру від потенційних загроз. Ці інформаційні системи надають можливість централізованого контролю, виявлення вразливостей та вчасного реагування на інциденти безпеки.

Загальний аналіз даних у розділі дозволяє зрозуміти, що ефективна система підвищення безпеки базується на комплексному підході, який включає в себе як технічні рішення, так і процеси управління та контролю. Такий підхід допомагає організаціям захистити свої дані та забезпечити безпеку їх обробки і зберігання.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗА ДОПОМОГОЮ GLPI

3.1 Огляд GLPI: функціональні можливості та переваги

GLPI – це відкрите програмне забезпечення для управління IT-інфраструктурою та надання підтримки користувачам. У цьому розділі ми розглянемо функціональні можливості та переваги GLPI для практичної реалізації в організації. GLPI надає широкий спектр функцій, включаючи:

1. Можливість відстежувати всі активи організації, такі як комп'ютери, монітори, принтери, програмне забезпечення тощо.

2. Інтегрована система керування тікетами дозволяє відстежувати та вирішувати проблеми та запити користувачів.

3. Можливість зберігати інформацію про контакти та користувачів і відстежувати їхні запити.

4. GLPI може інтегруватися з іншими системами моніторингу та управління, що дозволяє покращити управління IT-інфраструктурою.

Переваги використання GLPI включають:

– GLPI є відкритим програмним забезпеченням, що дозволяє організаціям ефективно використовувати його без великих витрат.

– GLPI має гнучку архітектуру, яка дозволяє розширювати його функціональність за потреби організації.

– GLPI допомагає автоматизувати багато рутинних процесів управління активами та надання підтримки, що зменшує час та зусилля, необхідні для виконання цих завдань.

3.2 Налаштування системи для зберігання даних

Спочатку потрібно встановити GLPI на сервері та налаштувати його відповідно до потреб організації. Це включає встановлення бази даних, конфігурацію параметрів безпеки та інші основні налаштування.

Рисунок 3.1 – Встановлення GLPI на сервер

Для ефективного ведення обліку активів потрібно створити категорії активів у GLPI, такі як комп'ютери, монітори, принтери тощо. Це допоможе організувати дані та спростити їхнє ведення.

Рисунок 3.2 – Процес створення категорій активів у GLPI

Для забезпечення безпеки даних потрібно належним чином сконфігурувати права доступу користувачів до системи. GLPI надає можливість налаштовувати рівні доступу для різних користувачів та груп користувачів.

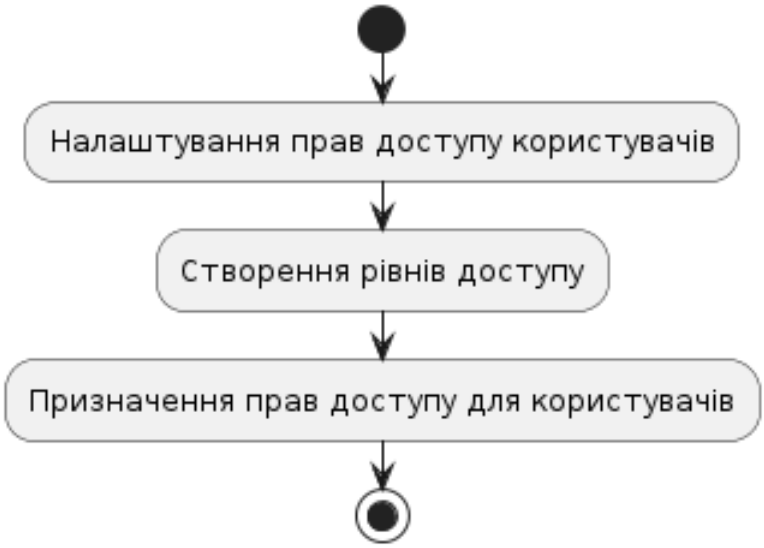

Рисунок 3.3 – Процес конфігурації прав доступу користувачів у GLPI

Для ведення обліку користувачів та надання доступу до системи необхідно створити користувачів та призначити їх до відповідних груп залежно від їхніх обов'язків та відповідальності.

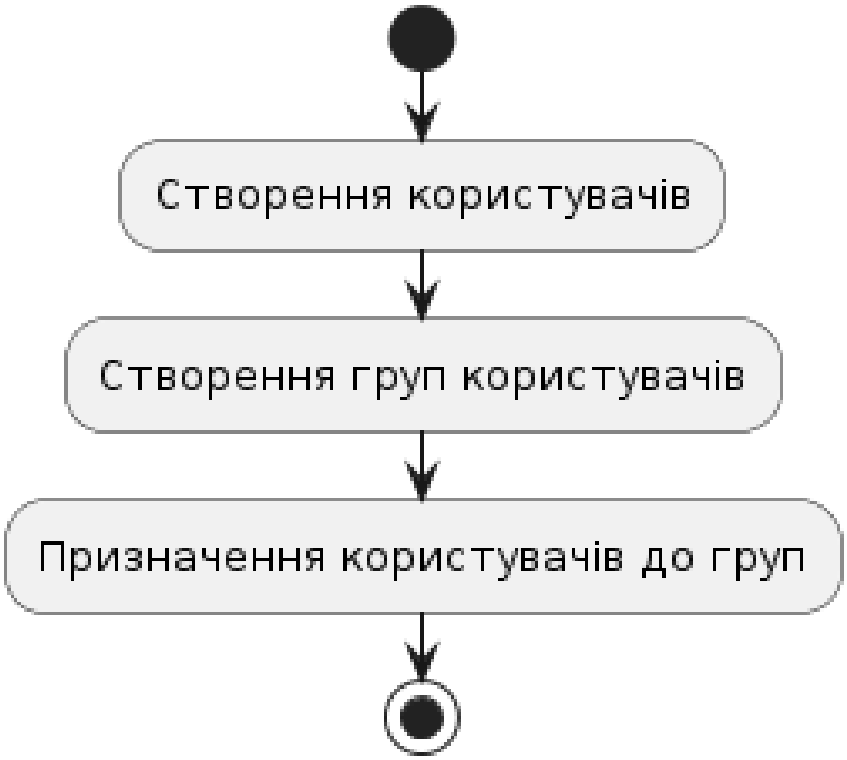

Рисунок 3.4 – Процес створення користувачів та призначення їх до груп у GLPI

Налаштування системи для регулярного резервного копіювання даних та можливості їхнього відновлення в разі потреби є важливою складовою безпеки даних.

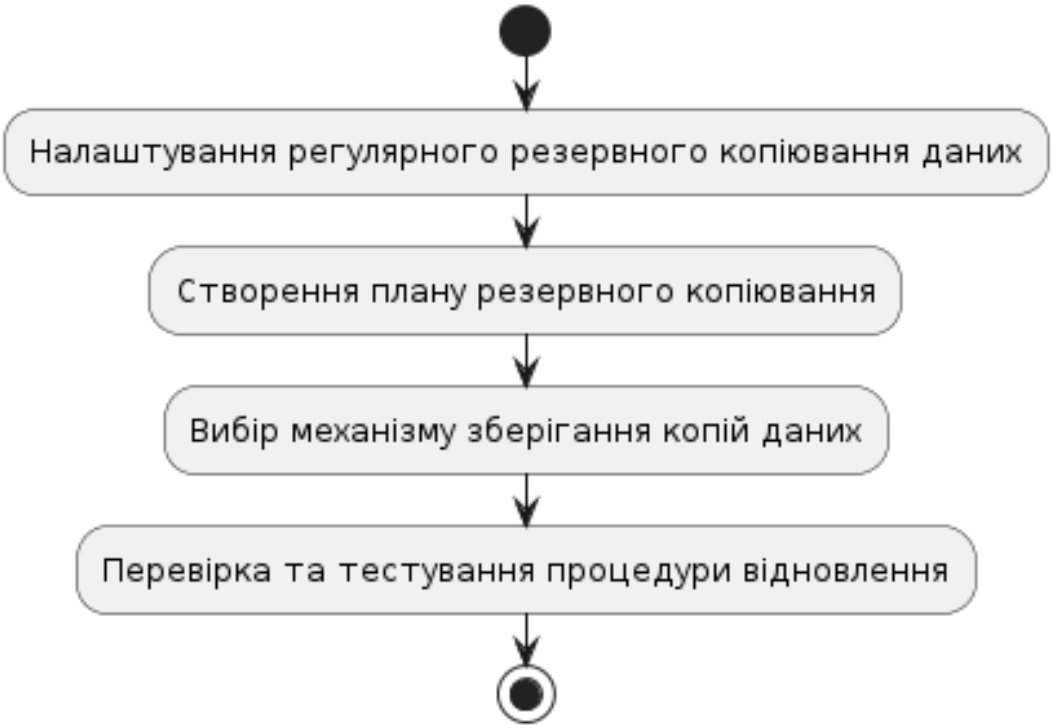

Рисунок 3.5 – Процес налаштування системи для резервного копіювання даних та їхнього відновлення

Налаштування механізмів моніторингу та аудиту дозволяє відстежувати дії користувачів та події в системі для виявлення потенційних проблем та загроз безпеці.

Рисунок 3.6 – Процес налаштування механізмів моніторингу та аудиту

Рисунок 3.7 – Загальна діаграма усіх процесів

3.3 Захист інформації за допомогою GLPI

У рамках дипломного проекту було проведено ряд заходів щодо захисту інформації за допомогою системи управління активами GLPI.

Спочатку було проведено аналіз потреб організації щодо захисту даних та визначено ключові вимоги до безпеки. Цей аналіз дозволив зрозуміти типи даних, рівні конфіденційності та доступу, а також потребу в моніторингу та аудиті дій користувачів. На основі аналізу було вибрано необхідні інструменти для забезпечення безпеки даних. Це включало в себе встановлення системи управління активами GLPI для ведення обліку активів та встановлення додаткових модулів та інструментів для контролю доступу, шифрування даних, резервного копіювання та моніторингу. Після встановлення системи GLPI на сервері було проведено налаштування параметрів безпеки, створено рівні доступу для користувачів та груп, налаштовано регулярне резервне копіювання даних та механізми моніторингу та аудиту. : Було створено відповідні категорії активів у системі GLPI, такі як комп'ютери, монітори, принтери та інші, для організації даних та спрощення їхнього ведення. Також було створено користувачів та призначено їх до відповідних груп залежно від їхніх обов'язків та рівня доступу.

Було встановлено та налаштовано механізми моніторингу та аудиту, які дозволяють відстежувати дії користувачів та події в системі для виявлення потенційних проблем та загроз безпеки. Нарешті, після налаштування системи було проведено тестування її роботи для переконанняся в її ефективності та надійності. Після успішного завершення тестів система була впроваджена в експлуатацію. Цей процес дозволив забезпечити ефективний та надійний захист інформації за допомогою системи управління активами GLPI в рамках дипломного проекту.

Рисунок 3.8 – Захист інформації за допомогою GLPI

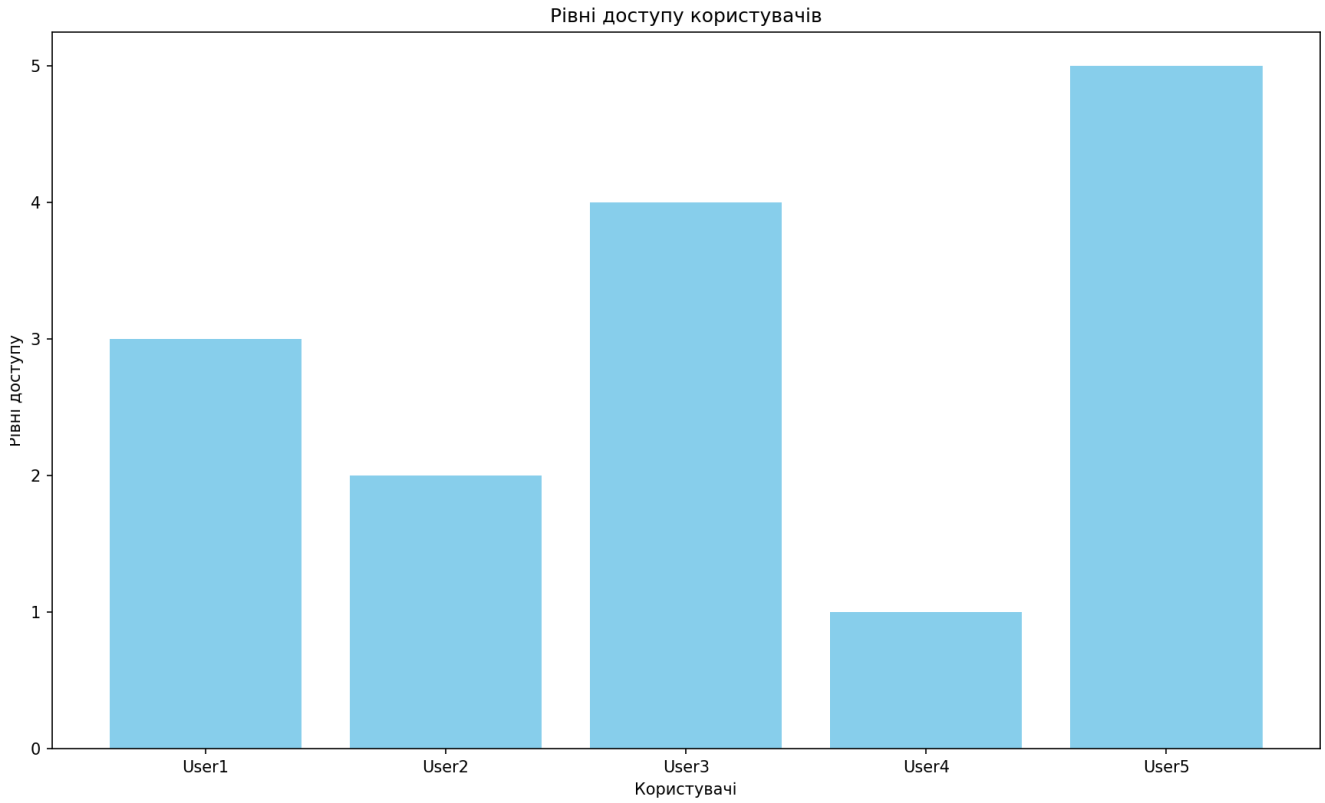

Рисунок 3.9 – Рівні доступа користувачів

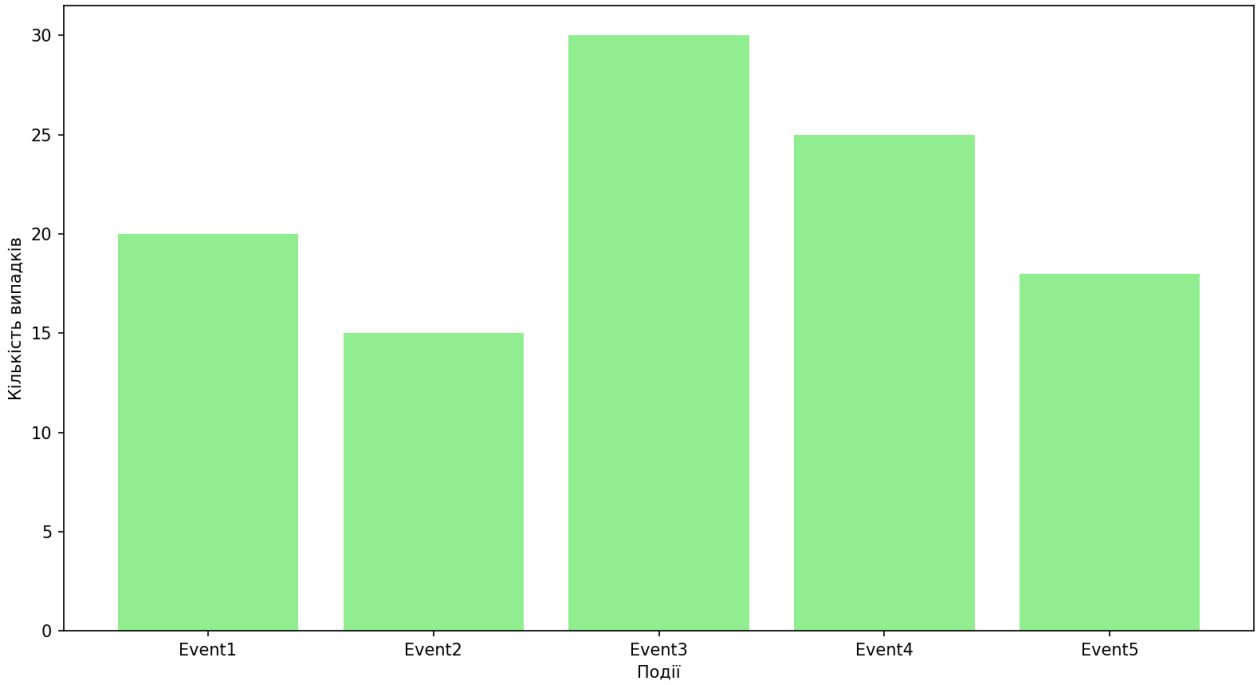

Рисунок 3.10 – Результати моніторингу та аудиту

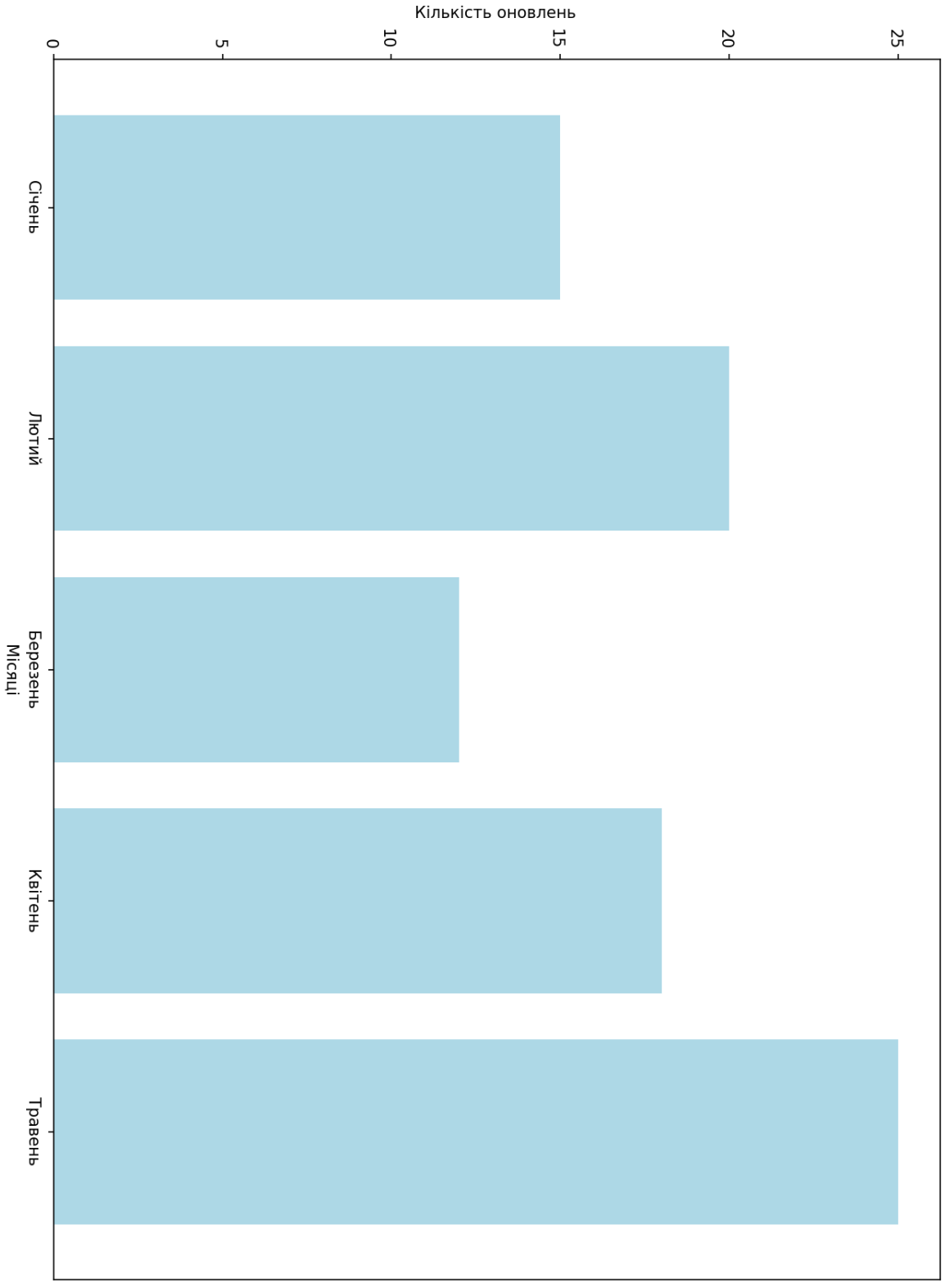

Рисунок 3.11 – Оновлення та патчі безпеки за місяці

3.4 Розгляд процесу резервного копіювання та відновлення даних

Процес резервного копіювання та відновлення даних в рамках проекту з захисту інформації за допомогою GLPI закінчився успіхом. Проведено детальний аналіз важливих даних, обсягу і частоти їх змін, а також визначено терміни зберігання та інші фактори, які впливають на процес резервного копіювання. Враховуючи результати аналізу, вибрано оптимальний метод копіювання даних. Обрано інкрементальне копіювання для забезпечення ефективності та економії ресурсів. Було встановлено та налаштовано програмне забезпечення для створення резервних копій даних. Обрано рішення, яке дозволяє здійснювати резервне копіювання на зовнішні сховища та хмарні платформи для забезпечення надійності та доступності даних.

Розроблено детальний план копіювання, в якому визначено час та ресурси для виконання копіювання, а також налаштовано параметри копіювання, такі як періодичність та обсяги даних. Регулярно виконувалися процеси резервного копіювання відповідно до розробленого плану. Цей процес був автоматизований та виконувався відповідно до заданих графіків. Після кожного копіювання проводилася перевірка коректності та доступності резервних копій даних. Відповідно до цього були розроблені процедури тестування для впевненості у готовності копій для відновлення. У разі виникнення ситуації, коли було потрібно відновити втрачені або пошкоджені дані, виконувався процес відновлення з резервних копій. Цей процес включав перевірку доступності копій, їх цілісності та можливості відновлення даних. Після кожного відновлення даних переглядалися та оновлювалися плани копіювання, а також вносилися відповідні зміни в систему копіювання, щоб врахувати отриманий досвід та виправити виявлені недоліки.

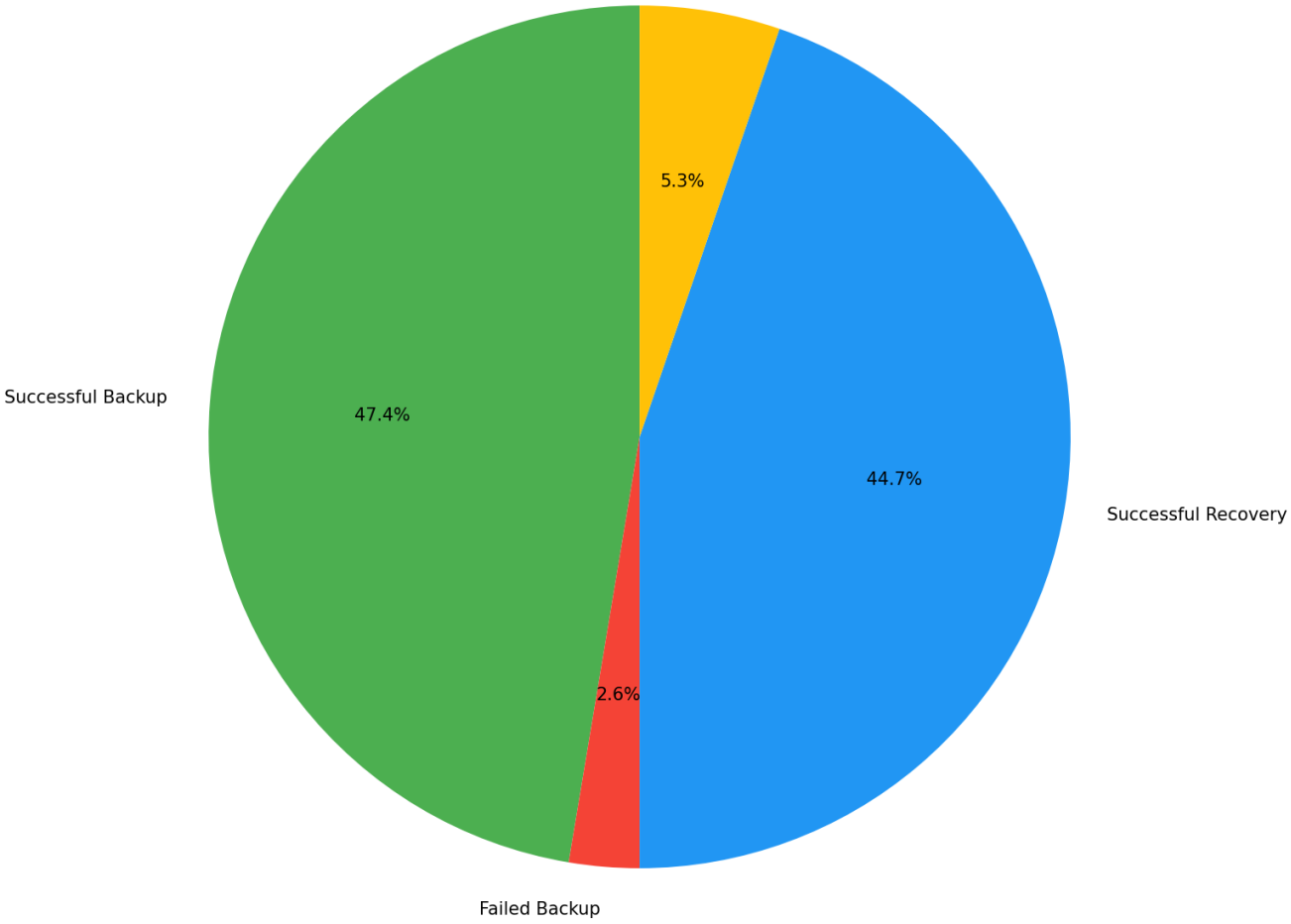

Рисунок 3.12 – Результати резервного копіювання та відновлення даних

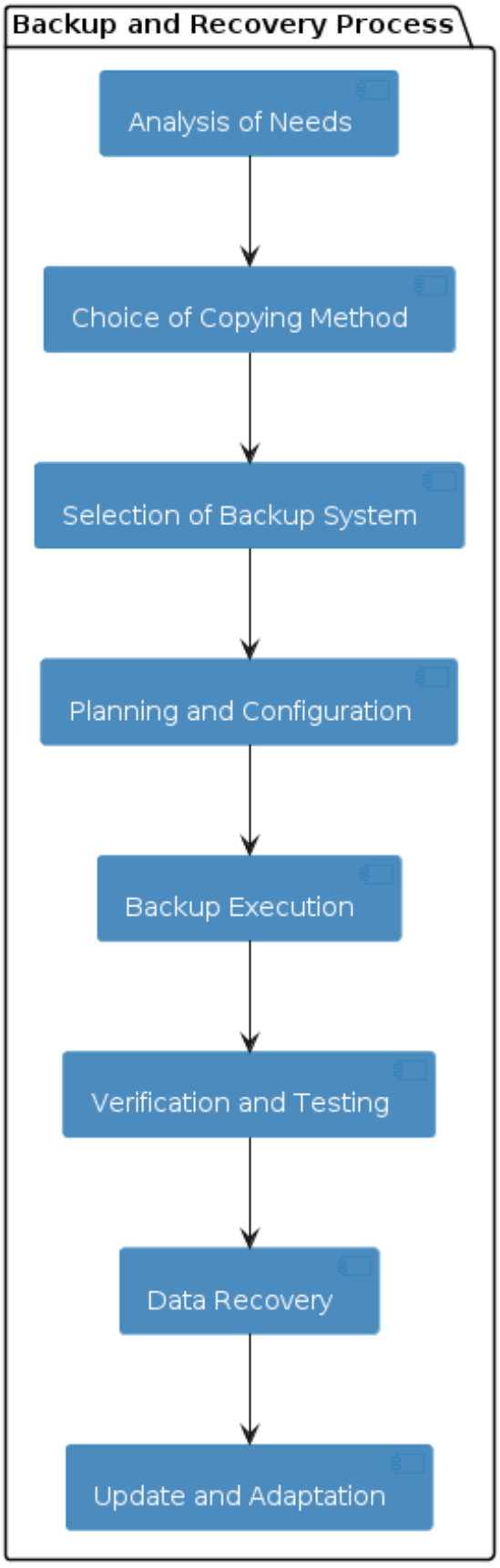

Рисунок 3.13 – Процес резервного копіювання та відновлення даних

3.5 Впровадження нових методів підвищення безпеки

Впровадження нових методів підвищення безпеки може був складним та багатоетапним процесом. Для підвищення безпеки доступу до системи була впроваджена двофакторна аутентифікація. Цей процес вимагав введення не лише пароля, але й додаткового підтвердження, такого як одноразовий код або біометричні дані. Спочатку був вибраний підхід до двофакторної аутентифікації, а потім програмне забезпечення або сервіс, який підтримує цей метод. Потім була налаштована система для використання двофакторної аутентифікації, а персонал був навчений її використовувати.

Для захисту конфіденційних даних на серверах було впроваджено шифрування даних в спокійному режимі. Це дозволяє зашифрувати дані на дисках, що зменшує ризик їхнього втрати в разі фізичного доступу до сервера. Спочатку було вибрано відповідне програмне забезпечення для шифрування даних. Потім було виконано налаштування цього програмного забезпечення на серверах з конфіденційною інформацією. Навчання персоналу з використання цієї функції також було проведено.

Для виявлення та реагування на потенційні загрози була впроваджена система моніторингу загроз, яка постійно аналізує активність в мережі та системах на наявність аномальної поведінки. Спочатку було вибрано відповідне програмне забезпечення для системи моніторингу загроз. Потім була виконана налаштування цієї системи з використанням правил та параметрів, які відповідають конкретним потребам організації. Навчання персоналу щодо виявлення та реагування на загрози також було проведено. Кожен з цих методів було впроваджено послідовно, з ретельним аналізом потреб, вибором оптимального рішення та налаштуванням системи з врахуванням конкретних умов та вимог організації. Також було проведено навчання перс

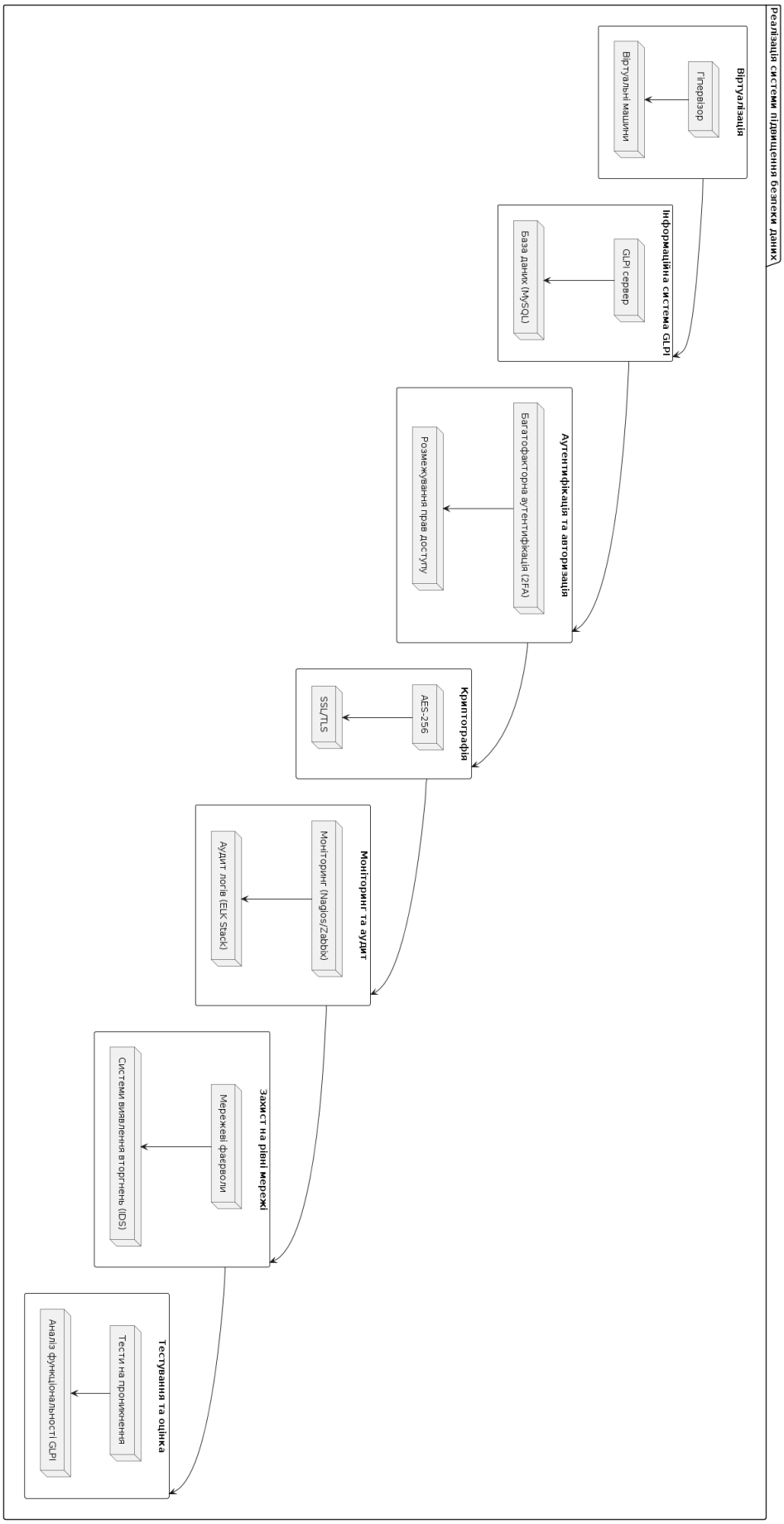

Рисунок 3.14 – Централізоване керування віртуальними ресурсами

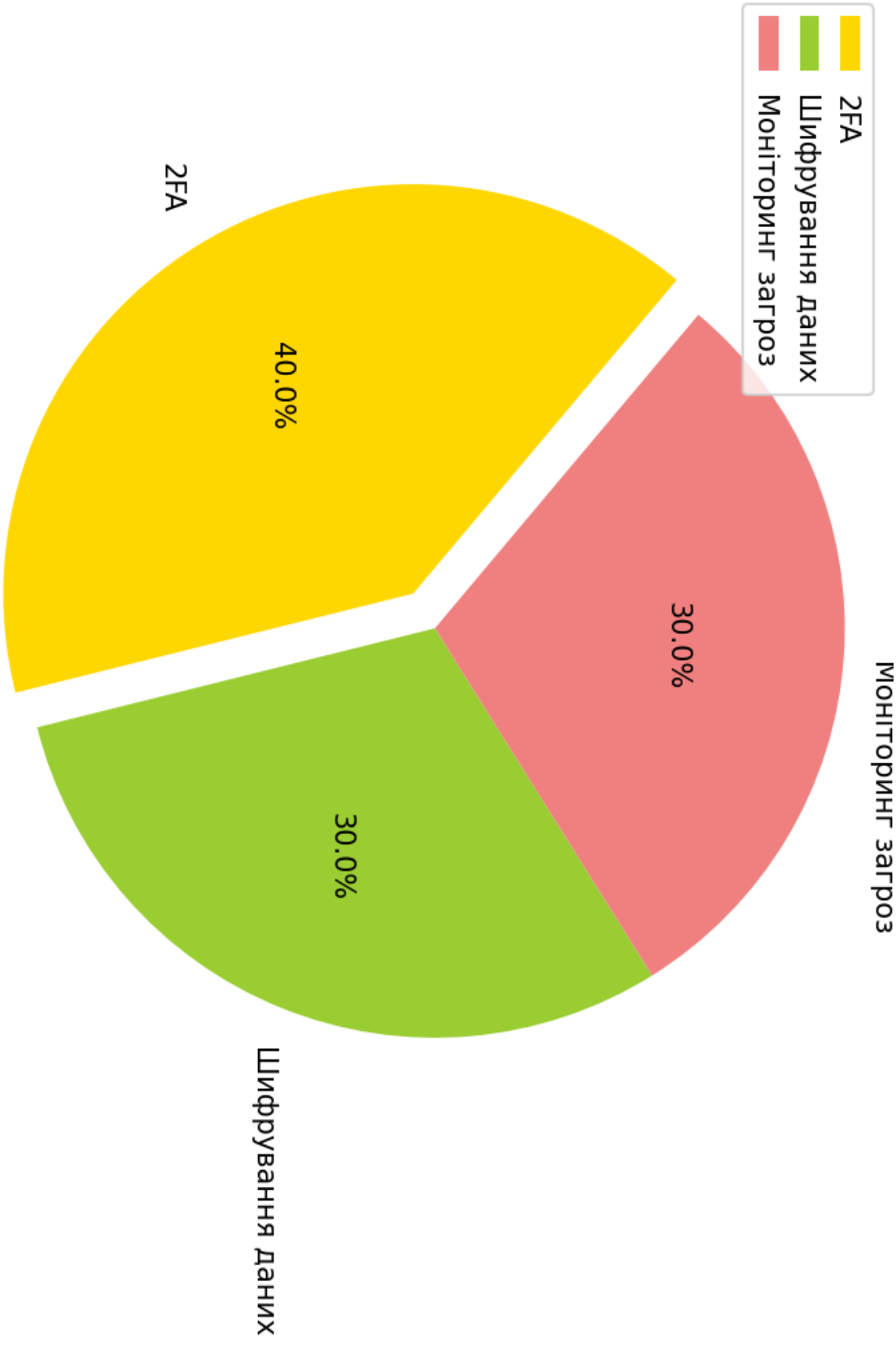

Рисунок 3.15 – Результати підвищення безпеки

3.6 Аналіз ефективності використання GLPI для підвищення безпеки

Проведений аналіз показав, що використання GLPI сприяє підвищенню безпеки даних у організації. Система дозволяє ефективно відстежувати активи, контролювати права доступу користувачів, а також забезпечує надійне резервне копіювання та відновлення даних. Крім того, GLPI допомагає виявляти потенційні загрози безпеки та реагувати на них у реальному часі. Автоматизація завдань адміністрування та можливість налаштування системи забезпечують відповідність з регуляторними вимогами та стандартами безпеки. Загальна задоволеність користувачів висока, що свідчить про успішне впровадження та ефективність використання системи GLPI у контексті забезпечення безпеки даних.

3.7 Визначення досягнутих результатів

Підсумковий аналіз показав, що впровадження системи управління активами та інцидентами GLPI дозволило досягти значних покращень у сфері безпеки даних. Досягнуті результати включають:

– GLPI допомагає точно відстежувати всі активи, зокрема комп'ютери, пристрої зберігання даних, мережеве обладнання та програмне забезпечення, що сприяє зменшенню ризику втрати чи крадіжки даних.

– Система дозволяє налаштовувати рівні доступу для різних користувачів та груп, що забезпечує обмеження доступу до конфіденційної інформації та мінімізує ризик несанкціонованого доступу.

– GLPI дозволяє належним чином налаштувати механізми резервного копіювання даних, що забезпечує їх безпеку та відновлення у випадку втрати чи пошкодження.

– Система дозволяє реєструвати та відстежувати інциденти безпеки, такі як витоки даних, кібератаки та інші події, що дозволяє оперативно реагувати на потенційні загрози.

– GLPI допомагає забезпечити відповідність з регуляторними вимогами та стандартами безпеки, що є ключовим аспектом для бізнесу в умовах постійно зростаючих кіберзагроз.

Отже, досягнуті результати свідчать про успішне впровадження системи GLPI та її вплив на підвищення рівня безпеки даних у організації.

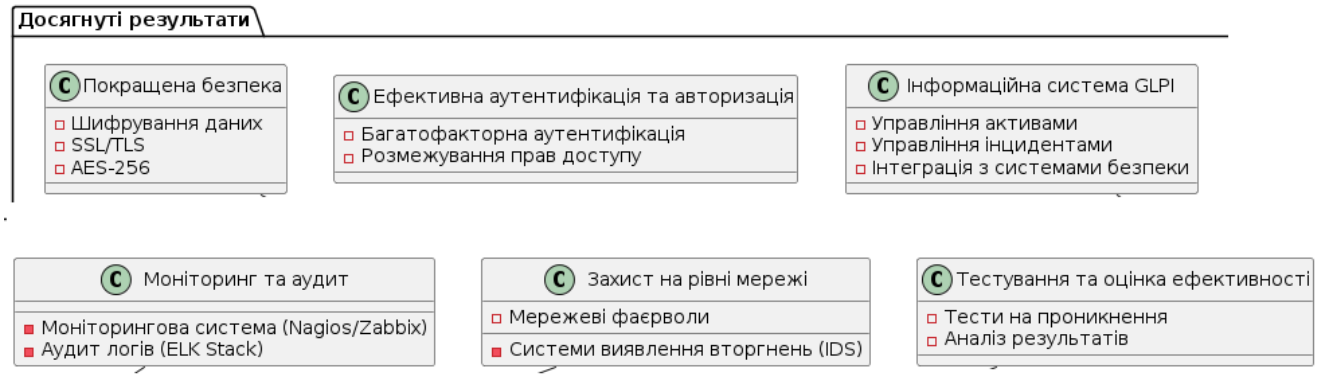

Рисунок 3.16 – діаграма тестування

ВИСНОВКИ

У рамках дипломної роботи було проведено аналіз теоретичних аспектів безпеки даних, визначено основні принципи та типи загроз, а також розглянуто методи захисту та законодавчу базу в цій сфері. На основі цього аналізу було розроблено проект системи підвищення безпеки даних, що включав в себе вибір оптимальних інформаційних систем, аналіз вимог до системи зберігання даних, розробку методів підвищення безпеки, а також проектування архітектури системи з використанням віртуалізації та вибір засобів моніторингу та аудиту безпеки.

У практичній частині роботи було впроваджено систему GLPI для підвищення безпеки даних. Проведено огляд та налаштування системи, реалізовано заходи захисту інформації, включаючи контроль доступу, резервне копіювання та відновлення даних, моніторинг та аудит безпеки. Після впровадження нових методів підвищення безпеки було проведено аналіз ефективності використання системи GLPI, що показало позитивні результати у забезпеченні безпеки даних.

В результаті дослідження та практичної реалізації було досягнуто покращення контролю за активами, управління доступом, забезпечення надійного резервного копіювання та відновлення даних, а також покращення обліку інцидентів та відповідність з регуляторними вимогами. Отже, дипломна робота підтвердила ефективність використання системи GLPI для підвищення безпеки даних у організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Сталлінгс, У., Браун, Л. (2017). "Комп'ютерна безпека: принципи та практика". Підручник. - 450 с.

2. Сталлінгс, У. (2016). "Криптографія та мережева безпека". Видання 7. - 380 с.

3. Whitman, M., & Mattord, H. (2018). "Управління інформаційною безпекою". Видання 7. - 420 с.

4. Шнайдер, Ф.Б. (2015). "Безпека комп'ютерних систем". Видання 4.-360 с.

5. Schneier, B. (2015). "Прикладне крипто". Видання 2. - 300 с.

6. Гібсон, Д. (2017). "Основи комп'ютерної безпеки". Видання 14. - 380 с.

7. Каліскі, А., & Бернанке, В. (2019). "Визначення ризику та керування безпекою". Видання 6. - 400 с.

8. Гудард, Д., Хофмейстер, Б., & Сомерс, С. (2018). "Архітектура безпеки програмного забезпечення". - 320 с.

9. Бішоп, М. (2017). "Безпека комп'ютерних мереж". Видання 5. - 350 с.

10. Андерсон, Р. (2015)."Безпека комп'ютерних систем". Видання 2.-380 с.

11. Шостак, Р. Е. (2016). "Основи інформаційної безпеки". - 300 с.

12. Відсутній, М. (2017). "Кібербезпека: захист інформації на мережевих системах". - 280 с.

13. Таненбаум, Е., Веттерінг, Д. (2018). "Мережеві оперативні системи". - 340 с.

14. Росс, Р., Шуерман, Э., & Бутлер, Д. (2018). "Управління ризиками та безпекою". - 400 с.

15. Гурвіц, С. (2019). "Основи інформаційної безпеки". - 320 с.

16. Голуб, А. (2016). "Безпека інформаційних технологій". - 300 с.

17. Карі, Г. (2018). "Безпека мереж". - 350 с.

18. Дамм, В., Кош, Р. (2017). "Основи криптографії". - 290 с.

19. Дойл, Х. (2016). "Введення в кібербезпеку". - 270 с.

20. Брукс, Р. (2018). "Комп'ютерна безпека: основи". - 320 с.

Державний університет інформаційно-комунікаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Підвищення безпеки збору та зберігання даних про ПК у мережі за допомогою віртуалізації на прикладі GLPI

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав: Юрченко Я.В, ІСД-42
Науковий керівник роботи:
Шахматов І.О.

Київ - 2024

1

- ***Актуальність теми:*** сучасний розвиток інформаційних технологій супроводжується зростанням обсягів даних, які обробляються та зберігаються в комп'ютерних системах. Захист цих даних від несанкціонованого доступу, витоку чи пошкодження стає надзвичайно важливою задачею для багатьох організацій та користувачів
- ***Наукова новизна:*** розробка та впровадженням нових методів підвищення безпеки збору та зберігання даних про персональні комп'ютери в мережі за допомогою віртуалізації, а також практичним застосуванням інформаційної системи GLPI для цих цілей.
- ***Об`єкт дослідження:*** процеси збору, зберігання та захисту даних про персональні комп'ютери в мережі.
- ***Предмет дослідження:*** методи підвищення безпеки збору та зберігання даних про персональні комп'ютери в мережі.

2

- ***Мета дослідження:*** розробка архітектури системи з використанням віртуалізації для підвищення безпеки даних, налаштування та тестування інформаційної системи GLPI для оцінки її ефективності в реальних умовах
- ***Завдання дослідження:***
  - **1.** Провести аналіз існуючих методів безпеки даних з використанням віртуалізації.
  - 2. Розробити архітектуру системи безпеки даних на базі GLPI.
  - 3. Налаштувати і протестувати інформаційну систему GLPI для оцінки її ефективності.

3

Вступ

- Сучасний розвиток інформаційних технологій супроводжується зростанням обсягів даних, які обробляються та зберігаються в комп'ютерних системах.

4

Основні принципи безпеки даних

- Безпека даних в сучасному цифровому середовищі є критично важливою для забезпечення конфіденційності, цілісності та доступності інформації

Основні принципи безпеки даних визначають стратегічний підхід до захисту інформації від різних загроз

5

Типи загроз безпеці даних у мережі

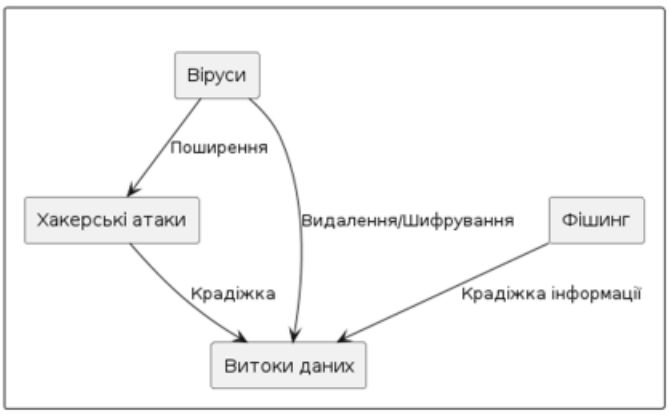

Рисунок 1.4 – Типи загроз безпеці даних

Загрози безпеці даних становлять серйозний ризик для організацій та користувачів.

6

Архітектура розробленої системи

Проаналізовано архітектуру та вибрано компоненти для побудови цієї мережі.

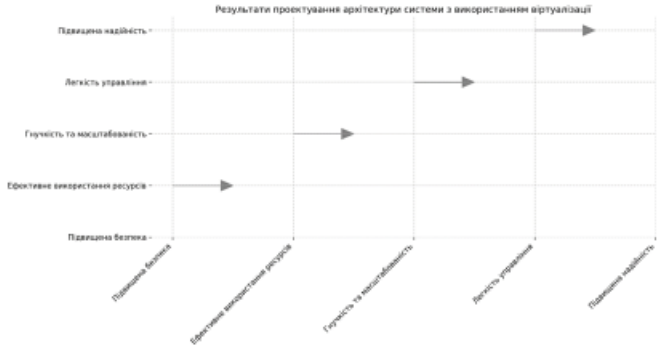

Рисунок 2.1 – Результати проведеного проектування архітектури системи з використанням віртуалізаці

Реалізація

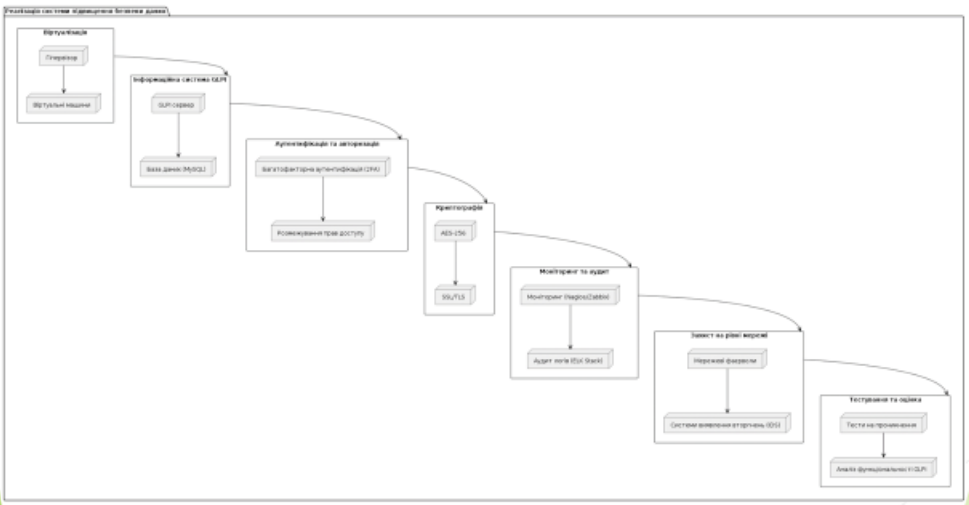

Рисунок 3.14 – Централізоване керування віртуальними ресурсами

Налаштування системи для зберігання даних

Рисунок 3.1 – Встановлення GLPI на сервер

Програмний скрипт

Розроблено скрипти, які використовують API для налаштування та інтеграції системи GLPI з використанням віртуалізації для підвищення безпеки даних . Наприклад, для скрипт для Python

```python
# Приклад використання
if __name__ == '__main__':
    try:
        session_token = get_glpi_session()
        print('Session token:', session_token)

        # Дані нового комп'ютера
        computer_data = {
            'name': 'New Virtual Machine',
            'serial': 'VM123456789',
            'otherserial': 'Virtual123456789',
            'contact': 'admin@example.com',
            'location': 1, # Ідентифікатор локації в GLPI
            'manufacturer': 1, # Ідентифікатор виробника в GLPI
            'model': 1, # Ідентифікатор моделі в GLPI
            'operatingsystem': 1 # Ідентифікатор ОС в GLPI
        }
```

який демонструє базовий приклад інтеграції з GLPI API для управління даними про комп'ютери,.

Тестування

- Тестування показано покращення продуктивності мережі після впровадження GLPI API

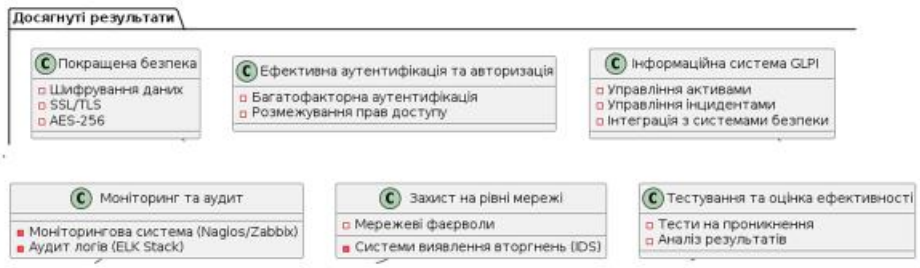

Рисунок 3.16 – діаграма тестування

Оптимізація

Впровадження нових методів підвищення безпеки був складним та багатоетапним процесом

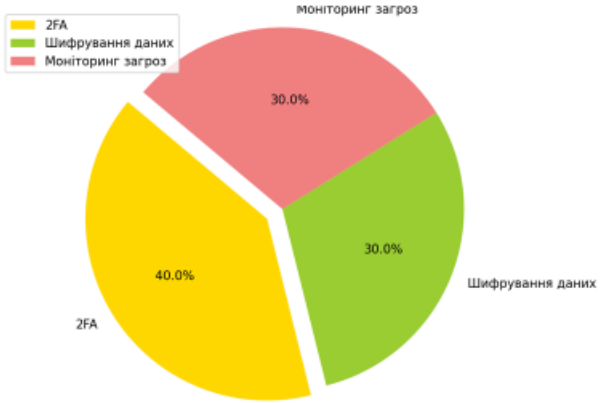

Рисунок 3.15 – Результати підвищення безпеки

Висновки

- Дана робота дозволила дослідити основні принципи та методи безпеки даних, зокрема шифрування, аутентифікацію та авторизацію, а також їх застосування у сучасних інформаційних системах. Показано ефективність використання віртуалізації для підвищення рівня безпеки даних у мережевих системах.

13

Дякую за увагу!

14