Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Якушевського Романа В'ячеславовича

на здобуття ступеня вищої освіти Бакалавра

Система оцінювання рівня захищеності корпоративної мережі приватного підприємства

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.220256.22.02.37 ПЗ

Виконав студент 4 курсу група КБ-22-2 Роман ЯКУШЕВСЬКИЙ

Керівник канд. техн. наук, доцент Віра ТІТОВА

Нормоконтролер д-р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

8 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

9 січня 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Якушевському Роману В'ячеславовичу

1 Тема роботи Система оцінювання рівня захищеності корпоративної мережі приватного підприємства

Керівник роботи канд. техн. наук, доцент Тітова Віра Юріївна

Затверджено наказом ректора університету від 8 січня 2026 р. № 7

2 Строк подання студентом кваліфікаційної роботи на кафедру 27 травня 2026р.

3 Вихідні дані до роботи розробити систему оцінювання рівня захищеності корпоративної мережі приватного підприємства на основі технічного сканування та аналізу організаційних заходів безпеки.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз загроз інформаційній безпеці та методів оцінювання захищеності корпоративних мереж приватних підприємств. Розроблення математичної моделі та алгоритму оцінювання рівня захищеності мережі. Програмна реалізація системи оцінювання та аналіз результатів тестування.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Розподіл пріоритетів математичної моделі оцінювання. Алгоритм роботи програмного комплексу. Структура програмного комплексу і модульна організація файлів.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Петляк Н.С., д-р філософії, доцент кафедри кібербезпеки		

7 Дата видачі завдання 12 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	лютий	
Ознайомлення з предметною областю	лютий	
Дослідження існуючих рішень	лютий	
Постановка задачі	березень	
Визначення загальних принципів рішення задачі	березень	
Деталізація принципів рішення задачі	квітень	
Розробка проєктних рішень	квітень	
Апробація проєктних рішень	травень	
Оформлення пояснювальної записки згідно вимог	травень	
Оформлення графічної частини	червень	
Захист КР	червень	

Студент _____ Роман ЯКУШЕВСЬКИЙ

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система оцінювання рівня захищеності корпоративної мережі приватного підприємства.

Автор роботи: Якушевський Роман В'ячеславович

Керівник роботи: канд. техн. наук, доцент Тітова Віра Юріївна.

Пояснювальна записка: 67 с., 1 додаток, 7 рисунків, 5 таблиць, 45 джерел.

Графічна частина: 3 плакати.

Ключові слова: кібербезпека, інтегральний показник, стоп-фактор, nmap, flask.

У кваліфікаційній роботі проведено комплексний аналіз стану інформаційної безпеки та методів оцінювання захищеності корпоративних мереж приватних підприємств. На основі ризик-орієнтованого підходу визначено ключові домени безпеки, сформовано систему критеріїв та обґрунтовано вагові коефіцієнти параметрів захисту. Побудовано математичну модель розрахунку підсумкового інтегрального показника з урахуванням логічних «стоп-факторів» для критичних вразливостей (відсутності резервного копіювання).

Розроблено та протезовано автономний програмний комплекс на базі мови Python 3.12, мікрофреймворку Flask та мережевого ядра Nmap 7.98. Програма забезпечує автоматизоване сканування TCP-портів, інтерактивне анкетування та динамічну візуалізацію результатів у вигляді радіальної діаграми. Практична апробація системи на базі реального мережевого шлюзу довела її точність та ефективність для використання в секторі малого бізнесу.

27 . 05 .2026 Якушевський Р.В

ABSTRACT

Subject of qualification work: System for assessing the security level of a private enterprise corporate network.

Author: Yakushevskyi Roman Viacheslavovych.

Head of work: Candidate of Technical Sciences, Associate Professor Titova Vira Yuriivna.

Explanatory note: 67 p., 1 appendix, 7 figures, 5 tables, 45 sources.

Graphic part: 3 posters.

Keywords: cybersecurity, integral score, stop-factor, nmap, flask.

The bachelor's qualification work is devoted to the development and implementation of an automated system for assessing the security level of a private enterprise corporate network. Based on a risk-oriented approach, the key security domains were identified, a system of single metrics was formed, and the weights of security parameters were justified using expert evaluation methods. A mathematical additive model for calculating the final integral score was constructed, incorporating logical "stop-factors" for critical vulnerabilities such as the absence of a backup policy.

A portable software package was developed and tested using Python 3.12, Flask microframework, and Nmap 7.98 engine. The system provides automated scanning of TCP ports, interactive checklists, and dynamic risk visualization via radar charts implemented through Chart.js. Experimental testing on a real network gateway verified the model's adaptability and high efficiency for independent internal security audits in small and medium-sized business environments.

27.05.2026 Якушевський Р.В.

ЗМІСТ

ВСТУП

У сучасних умовах цифрової трансформації бізнес-процесів корпоративна мережа стає критично важливим активом будь-якого приватного підприємства (ПП). Розвиток хмарних технологій, впровадження концепції віддаленої роботи та активне використання мобільних пристроїв значно розширили периметр мережі. Це, у свою чергу, призвело до появи нових векторів кібератак та збільшення ризиків несанкціонованого доступу до конфіденційних даних. Статистика останніх років свідчить про стрімке зростання кількості інцидентів інформаційної безпеки, спрямованих саме на малий та середній бізнес, оскільки такі підприємства часто не мають достатніх фінансових та кадрових ресурсів для утримання повноцінних відділів кібербезпеки.

Аналіз статистичних даних за 2024-2025 роки вказує на те, що вектор атак змістився з простих вірусів на складні багаторівневі загрози, такі як фішинг, соціальна інженерія та експлуатація вразливостей у застарілому мережевому програмному забезпеченні [1], а також цілеспрямовані тривалі атаки [2]. Для приватних підприємств, які часто використовують бюджетне або вживане мережеве обладнання (роутери, комутатори, точки доступу), ризик компрометації внутрішньої мережі зростає в геометричній прогресії. Відсутність автоматизованих засобів регулярної перевірки призводить до того, що критичні порти залишаються відкритими протягом тривалого часу, що створює ідеальні умови для проникнення зловмисників та розгортання вірусів-шифрувальників.

Проблема оцінювання рівня захищеності корпоративної мережі приватного підприємства є надзвичайно гострою через постійну динаміку ландшафту загроз. Традиційні методи захисту, такі як використання лише міжмережевих екранів та антивірусного програмного забезпечення, вже не забезпечують комплексного захисту. Необхідним стає системний підхід, який базується на періодичній оцінці ефективності впроваджених технічних і організаційних засобів захисту. Особливого значення це набуває в умовах обмеженого бюджету, коли адміністратор мережі повинен чітко розуміти пріоритетність оновлення обладнання або зміни налаштувань безпеки.

Додатковим фактором ризику є недотримання співробітниками підприємства елементарних правил кібергігієни. Використання слабких паролів, ігнорування політик резервного копіювання та робота через незахищені публічні канали зв'язку формують значну кількість вразливостей організаційного характеру. Таким чином, виникає гостра потреба у розробці комплексного підходу, який дозволив би не лише технічно сканувати мережеву інфраструктуру, а й оцінювати загальний рівень організаційної стійкості бізнесу до актуальних кіберзагроз.

Більшість існуючих систем оцінювання захищеності або орієнтовані на великі корпорації з відповідними бюджетами, або є занадто вузькоспеціалізованими професійними інструментами, що потребують тривалого налаштування. Для приватного підприємства актуальною є розробка інструментарію, який дозволив би інтегрально оцінити стан безпеки, враховуючи як технічні конфігурації обладнання, так і дотримання базових вимог безпеки персоналом. Незважаючи на наявність на ринку потужних комерційних сканерів вразливостей, більшість із них потребують високої кваліфікації персоналу для інтерпретації результатів. Саме тому розробка доступного, автономного та візуально зрозумілого програмного засобу оцінювання є своєчасним завданням для вітчизняного IT-сектору.

Мета роботи полягає у розробці методу та програмного засобу для комплексної оцінки рівня захищеності корпоративної мережі приватного підприємства, що дозволить оперативно виявляти слабкі місця в інфраструктурі та приймати обґрунтовані рішення щодо її вдосконалення без залучення дороговартісних зовнішніх консультантів.

Об’єкт дослідження - процес забезпечення інформаційної безпеки в корпоративних мережах приватних підприємств.

Предмет дослідження - методи, моделі та програмні інструменти оцінювання рівня захищеності об’єктів мережевої інфраструктури.

Завдання роботи:

1. проаналізувати типову структуру мережі приватного підприємства та

ідентифікувати найбільш ймовірні загрози інформаційній безпеці в сучасних умовах;

2. провести порівняльний огляд існуючих методів та програмних засобів оцінювання рівня захищеності інформаційних систем;

3. визначити перелік критеріїв і показників, що найбільш повно характеризують стан безпеки мережі приватного підприємства, враховуючи специфіку його функціонування;

4. розробити алгоритм розрахунку інтегрального показника захищеності мережі з використанням системи вагових коефіцієнтів та спеціальних “стоп-факторів”;

5. створити програмну реалізацію системи оцінювання на базі мови Python з використанням мережевого ядра Nmap та веб-інтерфейсу Flask;

6. провести тестування розробленої системи на прикладі моделі мережі реального підприємства та сформулювати практичні рекомендації щодо її застосування.

Практичне значення отриманих результатів. Розроблена система може бути впроваджена в повсякденну роботу системних адміністраторів для проведення регулярного внутрішнього аудиту, виявлення критичних помилок у налаштуваннях серверів та роутерів, а також для формування обґрунтованих звітів керівництву щодо необхідності інвестицій у засоби кіберзахисту. Запропонований підхід, що поєднує автоматизований аналіз технічних параметрів (стани портів, доступність сервісів) з оцінкою ключових організаційних заходів безпеки, дозволяє отримати більш повну картину стану захищеності підприємства порівняно з класичними безкоштовними сканерами вразливостей.

1 ОГЛЯД ПІДХОДІВ ДО ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Аналіз структури корпоративної мережі приватного підприємства та основних загроз її безпеці

1.1.1 Типова архітектура мережі малого та середнього бізнесу

Функціонування сучасного приватного підприємства неможливе без створення надійної та продуктивної інформаційно-комунікаційної інфраструктури. Типова архітектура мережі малого та середнього бізнесу зазвичай будується на базі стека протоколів TCP/IP та використовує клієнт-серверну модель взаємодії [3]. На відміну від великих корпоративних мереж, інфраструктура приватного підприємства часто має плоску або двохорівневу ієрархічну структуру, що зумовлено необхідністю мінімізації витрат на придбання та обслуговування обладнання.

Основним вузлом такої мережі є маршрутизатор периметра. Саме цей пристрій забезпечує зв’язок локальної мережі з глобальною мережею Інтернет та виконує функції первинного захисту. У практиці вітчизняних підприємств часто використовується обладнання таких виробників як MikroTik або Cisco серій для малого бізнесу [4, 5]. Маршрутизатор виконує роль шлюзу за замовчуванням для всіх внутрішніх пристроїв та здійснює маршрутизацію трафіку між різними сегментами мережі. Важливою характеристикою такого пристрою є наявність апаратного прискорення шифрування та підтримка створення захищених тунелів.

Фізичний рівень архітектури зазвичай представлений структурованою кабельною системою на основі витої пари категорії 5e або 6, що забезпечує швидкість передачі даних до 1 Гбіт/с [6]. Для підключення великої кількості робочих станцій використовуються комутатори другого рівня. У сучасних архітектурах перевага надається керованим комутаторам, оскільки вони дозволяють реалізовувати функції безпеки на рівні портів та підтримують технологію віртуальних локальних мереж. Це дозволяє уникнути проблем із широкомовними штормами та підвищити загальну стабільність роботи мережевих сервісів.

Логічна структура мережі приватного підприємства часто включає такі основні сегменти:

– сегмент управління та адміністрації, де розташовані комп’ютери керівництва та бухгалтерські системи;

– сегмент загального користування для основної маси співробітників;

– серверний сегмент, де розміщуються локальні сервери баз даних, файлові сховища або сервери для розміщення внутрішніх веб-ресурсів та панелей керування;

– бездротовий сегмент для підключення мобільних пристроїв через точки доступу Wi-Fi.

При проектуванні архітектури ПП найчастіше використовується топологія типу зірка. У центрі такої топології знаходиться центральний комутатор або маршрутизатор, до якого підключаються всі інші вузли. Перевагою такої схеми є простота діагностики та висока відмовостійкість - вихід з ладу однієї робочої станції або кабелю не впливає на роботу всієї мережі в цілому. Однак критичною точкою відмови стає центральний пристрій, тому до його вибору та захисту висуваються підвищені вимоги.

Окрему увагу в типовій архітектурі приділяють організації серверної частини. Навіть у невеликих підприємствах спостерігається тенденція до використання технологій віртуалізації [7]. Це дозволяє на одному фізичному сервері розгортати кілька ізольованих віртуальних машин під управлінням різних операційних систем. Такий підхід не тільки оптимізує використання заліза, але й підвищує рівень захищеності за рахунок ізоляції критичних сервісів один від одного. Наприклад, поштовий сервер може функціонувати в одній віртуальній машині, а база даних в іншій, що обмежує можливості зловмисника у разі зламу одного з сервісів.

Бездротова інфраструктура в архітектурі приватного підприємства часто є найбільш вразливою ланкою [8]. У правильних конфігураціях вона обов’язково відокремлюється від основної дротової мережі. Використання сучасних стандартів шифрування стає промисловим стандартом, проте на багатьох

підприємствах все ще зустрічаються застарілі пристрої, що потребує додаткового контролю. Для великих офісів використовується архітектура з централізованим контролером точок доступу, що дозволяє реалізувати безшовний роумінг та централізовано керувати політиками безпеки.

Периферичне обладнання, таке як мережеві принтери, камери відеоспостереження та пристрої контролю доступу, також інтегруються в загальну архітектуру мережі. Часто вони виділяються в окремий підсегмент, щоб мінімізувати ризики втручання в їх роботу з боку звичайних користувачів мережі або зовнішніх зловмисників. Це особливо важливо для систем IP-відеонагляду, трафік яких може створювати значне навантаження на загальні канали зв’язку.

Завершальним елементом архітектури є організація зовнішніх підключень. Окрім основного каналу від провайдера, приватні підприємства часто використовують резервний канал зв’язку. Маршрутизатор на периферії налаштовується таким чином, щоб автоматично перемикати трафік на резервну лінію у разі аварії на основній. Це забезпечує безперервність бізнес-процесів, що є однією з головних цілей інформаційної безпеки [9].

Таким чином, типова архітектура мережі приватного підприємства є компромісом між продуктивністю, вартістю та необхідним рівнем безпеки. Вона базується на перевірених мережевих рішеннях, але вимагає постійної уваги до налаштувань кожного активного пристрою. Розуміння особливостей цієї побудови є ключовим етапом для подальшого аналізу загроз та розроблення системи оцінювання рівня захищеності в рамках даної дипломної роботи.

1.1.2 Логічна сегментація та VLAN

Важливою складовою забезпечення безпеки корпоративної мережі приватного підприємства є впровадження механізмів логічної сегментації трафіку. У плоских мережах, де всі пристрої знаходяться в одному широкомовному домені, виникає значна кількість ризиків. Зокрема, у разі зараження одного робочого місця шкідливим програмним забезпеченням, воно може безперешкодно поширюватися на сервери баз даних, касові апарати або комп’ютери адміністрації. Логічна сегментація дозволяє обмежити область

розповсюдження загроз та значно спростити контроль за переміщенням даних всередині компанії.

Основним інструментом для вирішення цієї проблеми є технологія віртуальних локальних мереж (VLAN), що базується на міжнародному стандарті IEEE 802.1Q [10]. Використання цієї технології дозволяє розділити одну фізичну мережеву інфраструктуру на кілька незалежних логічних мереж на другому рівні моделі OSI. Кожен пакет даних у такій мережі отримує спеціальну мітку або тег, що містить ідентифікатор VLAN ID. Це дозволяє комутаторам чітко розрізняти, до якого саме сегмента належить той чи інший кадр даних, та направляти його лише на відповідні порти.

Для типового приватного підприємства доцільним є створення такої структури сегментів:

– сегмент управління (Management VLAN), у якому розташовується лише мережеве обладнання, інтерфейси керування серверами та джерела безперебійного живлення;

– сегмент критичних даних (Data VLAN), де працюють співробітники бухгалтерії, фінансового відділу та зберігаються персональні дані клієнтів;

– сегмент загального призначення для основної маси персоналу, що забезпечує доступ до пошти та внутрішніх порталів;

– гостьовий сегмент Wi-Fi, який має доступ виключно до мережі Інтернет без можливості будь якої взаємодії з внутрішніми ресурсами компанії;

– сегмент засобів безпеки, куди виділяються камери відеонагляду, контролери доступу та охоронні сигналізації.

Налаштування такої сегментації вимагає використання керованих комутаторів та маршрутизаторів. Наприклад, при використанні обладнання компанії MikroTik, сегментація реалізується через створення віртуальних інтерфейсів та налаштування програмних мостів (bridge). Порти комутатора можуть працювати в режимі доступу (access), де підключаються кінцеві пристрої, або в транковому режимі (trunk), що використовується для передачі трафіку кількох віртуальних мереж між активним обладнанням. Це дозволяє

централізовано контролювати трафік на рівні головного маршрутизатора, де налаштовуються правила між сегментного екранування.

Окрім підвищення рівня безпеки, логічна сегментація позитивно впливає на загальну продуктивність мережі [11]. Вона ефективно обмежує поширення широкомовного трафіку межами одного сегмента, що суттєво знижує паразитне навантаження на мережеві карти комп'ютерів та процесори маршрутизаторів. Також це значно спрощує процес моніторингу та діагностики мережі, оскільки адміністратор може чітко бачити обсяги та характер трафіку в кожному окремому підрозділі підприємства, що допомагає вчасно виявляти аномальну активність.

Важливим елементом ізоляції на третьому рівні моделі OSI є використання списків контролю доступу (ACL). Вони дозволяють на рівні центрального шлюзу жорстко обмежити протоколи та порти, за якими пристрої з одного сегмента можуть звертатися до ресурсів іншого. Наприклад, можна дозволити доступ з мережі адміністратора до серверної мережі лише за протоколами SSH або RDP, заблокувавши при цьому всі інші типи запитів. Такий принцип мінімальних привілеїв є базовим у сучасній кібербезпеці [12] та дозволяє мінімізувати поверхню атаки всередині периметра підприємства.

Ще одним аспектом сегментації є використання технології Private VLAN або ізоляції портів на комутаторах доступу. Це дозволяє заборонити обмін даними між комп'ютерами співробітників в межах одного відділу, змушуючи весь трафік проходити через центральний маршрутизатор для перевірки. Такий підхід є ефективним захистом від атак типу людина посередині (MITM) [13] та запобігає несанкціонованому скануванню внутрішньої мережі з боку скомпрометованих робочих станцій.

Застосування логічної сегментації також спрощує впровадження політик якості обслуговування [14]. Адміністратор може призначати вищий пріоритет трафіку з сегмента бухгалтерії або серверів баз даних, гарантуючи стабільну роботу критичних бізнес додатків навіть при пікових навантаженнях у мережі загального користування. Це забезпечує не лише безпеку, але й високу доступність сервісів, що є ключовим показником якості роботи системного

адміністратора.

Таким чином, логічна сегментація на базі VLAN та маршрутизації між сегментами є основним бар'єром, який заважає зловмисникам вільно пересуватися всередині корпоративної мережі після отримання початкового доступу до одного з вузлів. Вона створює необхідні умови для застосування диференційованих політик безпеки до різних груп користувачів, що є критично важливим етапом для побудови системи комплексного оцінювання рівня захищеності приватного підприємства в межах даної роботи.

1.1.3 Класифікація зовнішніх кіберзагроз та векторів атак на периметр

Забезпечення захищеності корпоративної мережі приватного підприємства неможливе без детального аналізу потенційних загроз та способів їх реалізації. У сучасних умовах ландшафт кіберзагроз постійно змінюється, що вимагає від системних адміністраторів не лише встановлення засобів захисту, але й розуміння механізмів проведення атак зловмисниками. Класифікацію загроз інформаційній безпеці доцільно проводити за джерелом їх виникнення [15], розділяючи на зовнішні, що походять з глобальної мережі інтернет, та внутрішні, зумовлені діями персоналу або технічними збоями обладнання.

Зовнішні загрози представляють найбільшу небезпеку для периметра мережі, оскільки вони часто є автоматизованими та проводяться масово [16, 17]. Одним із найбільш поширених векторів атак є сканування портів та ідентифікація мережевих сервісів. Зловмисники використовують спеціалізоване програмне забезпечення для пошуку відкритих портів на зовнішній IP адресі підприємства. Виявлення відкритих інтерфейсів керування, таких як SSH, RDP або панелей адміністрування веб серверів, стає точкою входу для подальших атак типу брутфорс, спрямованих на підбір паролів до облікових записів адміністраторів.

Іншим серйозним вектором атаки є експлуатація вразливостей у програмному забезпеченні мережевих пристроїв та серверів. Якщо приватне підприємство використовує застарілі версії операційних систем або прошивок маршрутизаторів, зловмисники можуть застосувати готові експлойти для отримання несанкціонованого доступу до системи. Особливо небезпечними є

вразливості нульового дня, для яких на момент атаки ще не існує офіційних оновлень безпеки. Це підкреслює необхідність використання систем виявлення та запобігання вторгненням (IDS/IPS) на рівні периметра [18].

Атаки типу відмова в обслуговуванні (DoS) та їх розподілені варіанти (DDoS) спрямовані на виведення з ладу мережевого обладнання або каналів зв'язку [19]. Для приватного підприємства навіть нетривала зупинка роботи інтернет каналу може призвести до значних фінансових втрат через неможливість обробки замовлень або доступу до хмарних сервісів. Такі атаки можуть здійснюватися шляхом переповнення таблиць з'єднань маршрутизатора або забивання смуги пропускання великою кількістю фіктивних пакетів даних.

Окрему групу загроз становить соціальна інженерія та фішинг. Зловмисники надсилають співробітникам підприємства електронні листи з шкідливими вкладеннями або посиланнями на підроблені сайти. У разі відкриття такого вкладення на робочому комп'ютері активується шкідливе програмне забезпечення, яке може виконувати функції шпигунства, викрадення паролів або шифрування даних з метою отримання викупу. Цей вектор атаки є надзвичайно ефективним, оскільки він використовує людський фактор як найслабшу ланку в системі технічного захисту.

Внутрішні загрози часто ігноруються при проектуванні систем захисту, проте вони становлять значний ризик [20]. До них належать ненавмисні дії співробітників, такі як використання занадто простих паролів, відключення антивірусного програмного забезпечення або підключення до корпоративної мережі особистих пристроїв, що можуть бути заражені вірусами. Також не можна виключати загрозу з боку інсайдерів, які мають легітимний доступ до інформаційних ресурсів та можуть використовувати його для викрадення конфіденційної інформації або саботажу роботи мережі.

Використання бездротових технологій створює додаткові вектори атак, пов'язані з перехопленням трафіку або створенням підроблених точок доступу. Навіть при використанні сучасних протоколів шифрування існують методики атак на процедуру авторизації клієнтів у мережі Wi-Fi. Це вимагає від адміністратора

постійного моніторингу ефіру та обмеження потужності передавачів точок доступу, щоб сигнал не виходив далеко за межі офісного приміщення.

Таким чином, комплексний аналіз зовнішніх та внутрішніх загроз дозволяє визначити пріоритетні напрямки для побудови системи оцінювання рівня захищеності. Кожна з перелічених загроз має бути врахована при розробленні математичної моделі, де показники захищеності будуть коригуватися залежно від ймовірності реалізації того чи іншого вектора атаки. Розуміння механізмів проведення кібератак є фундаментальною основою для подальшого вибору критеріїв оцінки в рамках даного дипломного проекту.

1.2 Огляд існуючих методів, моделей і засобів оцінювання рівня захищеності корпоративних мереж

Після ідентифікації структури мережі та аналізу потенційних загроз критично важливим етапом стає вибір адекватної методології для оцінювання реального стану захищеності інформаційних ресурсів підприємства. Оцінювання рівня захищеності є комплексним процесом, що передбачає систематичний збір, аналіз та інтерпретацію даних про стан технічних засобів захисту, конфігурації мережевого обладнання та дотримання встановлених політик безпеки. У сучасній практиці кібербезпеки виділяють кілька основних підходів до вирішення цього завдання, кожен з яких має свої переваги, обмеження та специфіку застосування в умовах приватного підприємства.

Перший підхід базується на інструментальному скануванні та технічному аудиті [21]. Він передбачає використання спеціалізованого програмного забезпечення для автоматизованого пошуку вразливостей, відкритих портів та помилок у налаштуваннях сервісів. Цей метод дозволяє отримати об’єктивну технічну картину стану мережі на конкретний момент часу. Однак, суто технічний аналіз не завжди дозволяє оцінити загальний рівень ризику для бізнес процесів, оскільки він не враховує критичність окремих вузлів та імовірність реалізації

складних багатовекторних атак.

Другий підхід ґрунтується на оцінюванні відповідності встановленим стандартам та нормативним вимогам [22]. Такий підхід передбачає порівняння існуючої системи захисту з еталонними моделями, описаними у міжнародних стандартах серії ISO або рекомендаціях NIST. Це дозволяє забезпечити високий рівень системності в управлінні безпекою, проте для малих приватних підприємств повна сертифікація за такими стандартами часто є надмірно дорогою та складною у впровадженні процедурою.

Третій підхід базується на математичному моделюванні та аналізі ризиків [23]. Він передбачає розрахунок інтегральних показників захищеності на основі ймовірнісних характеристик виникнення загроз та потенційних збитків від їх реалізації. Такий метод є найбільш гнучким, оскільки дозволяє адаптувати модель оцінювання під специфічні потреби конкретного підприємства, враховуючи вагові коефіцієнти різних параметрів безпеки. Саме поєднання цих підходів дозволяє створити збалансовану систему оцінювання, яка буде одночасно технічно точною та практично придатною для використання адміністраторами мереж.

Важливим аспектом при виборі методів оцінювання є можливість їх автоматизації. Враховуючи динамічність сучасних мереж, разові перевірки швидко втрачають свою актуальність. Тому сучасні засоби оцінювання мають підтримувати режим постійного моніторингу або періодичного сканування з автоматичним формуванням звітів. Це дозволяє вчасно виявляти нові вразливості та відстежувати ефективність впроваджених заходів захисту в динаміці.

У наступних підпунктах буде проведено детальний розгляд інструментальних засобів, методологічних стандартів та порівняльний аналіз існуючих програмних продуктів, що дозволить сформувати надійне підґрунтя для розроблення власної системи оцінювання рівня захищеності в межах даного дослідження.

1.2.1 Інструментальні методи сканування вразливостей мережевих ресурсів

Ефективне оцінювання рівня захищеності корпоративної мережі неможливе

без використання спеціалізованих інструментальних засобів, що дозволяють автоматизувати процес пошуку слабких місць. Інструментальні методи базуються на активному або пасивному дослідженні мережевих вузлів з метою виявлення відкритих портів, активних сервісів та відомих помилок у їхніх налаштуваннях [24]. Основним класом такого програмного забезпечення є сканери вразливостей, які дозволяють адміністратору подивитися на мережу очима потенційного зловмисника, виявляючи вектори атак до того, як вони будуть експлуатовані.

Одним із найбільш фундаментальних інструментів у цій галузі є Nmap (Network Mapper) [25]. Це утиліта з відкритим вихідним кодом, яка використовується для дослідження мережі та аудиту безпеки. Принцип роботи Nmap базується на відправці спеціально сформованих пакетів різних протоколів, таких як TCP, UDP та ICMP, до цільових вузлів та аналізі отриманих відповідей. За допомогою цього інструменту можна реалізувати різні техніки сканування. Наприклад, SYN сканування є одним із найпопулярніших методів, оскільки воно дозволяє швидко опитувати тисячі портів, не завершуючи повний цикл встановлення TCP з'єднання, що робить процес менш помітним для простих систем виявлення вторгнень.

Важливою особливістю Nmap є підсистема скриптів NSE (Nmap Scripting Engine). Вона дозволяє значно розширити базові можливості сканера, автоматизуючи виявлення конкретних вразливостей, перевірку наявності стандартних паролів на мережевих сервісах та проведення базового тестування на проникнення. Використання скриптів дозволяє адміністратору отримувати детальну інформацію про версії програмного забезпечення, що запущене на портах, та перевіряти їх на відповідність відомим базам даних експлойтів.

Наступним рівнем інструментального аналізу є повнофункціональні системи управління вразливостями, серед яких виділяється OpenVAS (Open Vulnerability Assessment System). Це комплексний сканер, який використовує розгалужену базу даних мережевих вразливостей, що постійно оновлюється співтовариством розробників. На відміну від простих порт сканерів, OpenVAS [26] проводить глибокий аналіз кожного виявленого сервісу. Процес сканування

зазвичай включає етап ідентифікації цілі, виявлення активних служб та виконання специфічних тестів для перевірки наявності відомих помилок у коді або конфігурації. Результатом роботи програми є детальний звіт, у якому кожна знайдена проблема класифікується за рівнем небезпеки та супроводжується посиланнями на відповідні описи у базах CVE та рекомендаціями щодо усунення вразливості.

Альтернативним комерційним рішенням, яке часто розглядається при професійному аудиті безпеки, є Nessus [27, 28]. Цей сканер відомий своєю високою швидкістю роботи та мінімальним рівнем помилкових спрацьовувань. Nessus пропонує розширені можливості для проведення конфігураційного аудиту, що дозволяє перевіряти відповідність налаштувань операційних систем та мережевого обладнання міжнародним стандартам безпеки. Програма підтримує сканування з використанням облікових записів, що дає змогу перевіряти внутрішні налаштування реєстру, версії встановлених бібліотек та наявність критичних патчів безпеки безпосередньо зсередини системи. Це забезпечує набагато глибший аналіз порівняно зі звичайним зовнішнім скануванням периметра.

Методологія інструментального сканування в рамках оцінювання захищеності зазвичай поділяється на кілька послідовних етапів [29]. На першому етапі здійснюється збір інформації про структуру мережі та ідентифікація активних вузлів. Далі проводиться визначення типів операційних систем та версій запущених мережевих служб. Третій етап полягає у порівнянні отриманих даних із реєстрами відомих вразливостей. На завершальному етапі виконується перевірка конфігурацій на наявність типових помилок адміністрування, таких як дозволений анонімний доступ до файлових систем або використання застарілих та небезпечних протоколів передачі даних.

Звіти, що генеруються такими системами, зазвичай базуються на загальноприйнятій системі оцінювання вразливостей CVSS (Common Vulnerability Scoring System) [30, 31]. Це дозволяє адміністратору приватного підприємства пріоритезувати завдання з модернізації захисту, зосереджуючись на

усуненні найбільш критичних прогалин. Числова оцінка вразливості враховує складність експлуатації, вплив на конфіденційність, цілісність та доступність даних, що робить процес оцінювання об’єктивним та зрозумілим для прийняття рішень.

Незважаючи на високу ефективність, інструментальні методи мають певні обмеження, які необхідно враховувати. Вони не завжди здатні виявити специфічні логічні помилки в унікальних бізнес додатках або проблеми, пов’язані з порушенням організаційних регламентів персоналом. Крім того, інтенсивне сканування може створювати значне навантаження на мережеві канали та призводити до збоїв у роботі старого або специфічного обладнання. Тому використання таких засобів має бути ретельно спланованим та інтегрованим у загальну стратегію моніторингу безпеки підприємства.

Таким чином, інструментальні методи сканування є фундаментом для отримання достовірних даних про стан мережевої інфраструктури. Аналіз функціональних можливостей сучасних сканерів показує, що їх комбіноване використання дозволяє отримати найбільш повну картину вразливостей. Це є критично важливим для реалізації практичної частини даної роботи, де результати роботи таких інструментів стануть вхідними даними для математичної моделі оцінювання рівня захищеності.

1.2.2 Стандарти та методики аудиту і оцінювання відповідності інформаційній безпеці

Важливою складовою комплексного оцінювання рівня захищеності корпоративної мережі є використання загальновизнаних міжнародних стандартів та методологій. Якщо інструментальні методи дають змогу виявити технічні вразливості на рівні конкретних пристроїв, то стандартизація дозволяє оцінити систему захисту як цілісний механізм, що охоплює технічні, організаційні та управлінські аспекти. Для приватного підприємства орієнтація на світові практики є ключовим фактором побудови стабільної та прогнозованої системи кібербезпеки.

Основним документом у цій галузі є міжнародний стандарт ISO/IEC 27001.

Він базується на процесному підході та концепції постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Оцінювання захищеності згідно з цим стандартом передбачає перевірку відповідності існуючих заходів безпеки переліку контрольних цілей, викладених у додатках до стандарту. Це включає аналіз політик доступу, методів шифрування даних, фізичного захисту обладнання та готовності до реагування на інциденти. Для приватного підприємства повне впровадження ISO 27001 може бути складним завданням, проте використання його положень як базису для оцінювання дозволяє виявити стратегічні прогалини в захисті.

Більш орієнтованим на технічне оцінювання є стандарт NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment), розроблений Національним інститутом стандартів і технологій США [32]. Ця методологія детально описує процес тестування безпеки, розділяючи його на кілька ключових етапів: огляд цілей, ідентифікація вразливостей та підтвердження можливості їх експлуатації. NIST пропонує використовувати три основні методи оцінювання: перевірка, тестування та опитування. Метод перевірки включає аналіз конфігураційних файлів маршрутизаторів та серверів, вивчення журналів подій та топологій мережі. Тестування передбачає активні дії, такі як сканування портів або проведення тестів на проникнення. Опитування ж дозволяє оцінити рівень обізнаності персоналу та дотримання регламентів безпеки.

Оцінювання захищеності за методиками NIST дозволяє отримати не просто перелік знайдених багів, а структурований аналіз того, наскільки ефективно впроваджені заходи контролю виконують свої функції. Це особливо важливо для аналізу конфігурацій мережевого обладнання, такого як маршрутизатори MikroTik. Аудит за стандартами NIST може включати перевірку наявності небезпечних служб керування, аналіз правил міжмережевого екрана та оцінку надійності використовуваних методів автентифікації.

Ще одним важливим елементом методологічного підходу є стандарт контрольних об’єктів для інформаційних та суміжних технологій (COBIT) [33]. Він зосереджений на аудиті IT процесів та їх відповідності бізнес цілям

підприємства. У контексті оцінювання захищеності COBIT дозволяє визначити рівень зрілості процесів безпеки за шкалою від нульового (відсутність процесу) до п’ятого (оптимізований процес). Такий підхід дає керівництву підприємства зрозуміле уявлення про те, на якому етапі розвитку знаходиться система кібербезпеки та які ресурси необхідні для її покращення.

При оцінюванні рівня захищеності в рамках дипломного проекту доцільно поєднувати вимоги різних стандартів для створення адаптованої методики [34]. Наприклад, технічні параметри перевірки можна запозичити з NIST, а організаційні принципи та підхід до ризиків - з ISO 27001. Такий симбіоз дозволяє сформувати систему критеріїв, яка враховує специфіку приватного підприємства: обмеженість бюджету, невеликий штат IT спеціалістів та необхідність швидкої адаптації до нових бізнес вимог.

Методологічне оцінювання також передбачає використання матриць відповідності [35]. Це дозволяє наочно продемонструвати, які загрози перекриваються існуючими засобами захисту, а де залишаються критичні вразливості. Такий аналіз є підґрунтям для математичного розрахунку інтегрального показника захищеності, де кожен технічний параметр отримує ваговий коефіцієнт залежно від його значущості у вибраному стандарті безпеки.

Таким чином, використання міжнародних стандартів та методик забезпечує системність та об’єктивність процесу оцінювання захищеності. Це дозволяє перейти від хаотичного пошуку вразливостей до структурованого аудиту всієї інформаційної системи. Огляд ISO 27001 та NIST SP 800-115 демонструє, що сучасна кібербезпека базується на поєднанні технічного контролю та управлінських рішень, що і буде відображено в розроблюваній системі оцінювання в наступних розділах роботи.

1.2.3 Порівняльний аналіз програмних комплексів моніторингу та аудиту безпеки

Завершальним етапом огляду існуючих засобів є аналіз конкретних програмних рішень, що дозволяють здійснювати постійний контроль за станом захищеності корпоративної мережі. Вибір програмного забезпечення для

приватного підприємства є складним завданням, оскільки воно має поєднувати в собі високу функціональність, простоту розгортання та помірну вартість володіння. На ринку представлено широкий спектр рішень: від потужних систем управління подіями безпеки (SIEM) до легких інструментів мережевого моніторингу та спеціалізованих сканерів.

Для об'єктивного оцінювання існуючих систем доцільно визначити ключові критерії порівняння. Першим критерієм є глибина аналізу мережевих пакетів та здатність системи виявляти аномалії в трафіку. Другим важливим параметром є підтримка різнорідного обладнання, зокрема популярних у сегменті малого бізнесу маршрутизаторів MikroTik та серверів на базі Linux. Також критично важливими є можливість автоматичного сповіщення адміністратора про інциденти, наявність вбудованих звітів про рівень захищеності та системні вимоги до апаратної частини, на якій буде розгорнуто систему.

Системи класу IDS/IPS, такі як Snort або Suricata, забезпечують глибокий аналіз трафіку на основі сигнатур [36]. Вони дозволяють виявляти спроби сканування мережі, атаки на відмову в обслуговуванні та активність шкідливого програмного забезпечення. Однак такі системи потребують детального налаштування та постійного оновлення баз сигнатур, що може бути складним для системного адміністратора невеликого підприємства.

З іншого боку, системи загального моніторингу, наприклад Zabbix або PRTG, дозволяють контролювати доступність вузлів та стан інтерфейсів [37]. Хоча вони не є спеціалізованими інструментами безпеки, їх можна використовувати для виявлення пікових навантажень або несанкціонованих підключень до мережі. Перевагою таких систем є можливість збору даних через протокол SNMP, що підтримується майже всім мережевим обладнанням.

Нижче наведено порівняльну таблицю основних характеристик популярних засобів, які можуть бути використані для оцінювання та моніторингу захищеності корпоративної мережі приватного підприємства.

Таблиця 1.1 - Порівняльна характеристика засобів моніторингу та аудиту безпеки

Параметр порівняння	Nmap	OpenVAS	Zabbix	Snort
Основне призначення	Сканування мережі	Пошук вразливостей	Моніторинг стану	Виявлення атак
Тип аналізу	Активний запит	Глибоке тестування	Збір метрик	Аналіз трафіку
Складність налаштування	Низька	Середня	Висока	Висока
Вимоги до ресурсів	Мінімальні	Високі	Середні	Високі
Автоматизація звітів	Через скрипти	Повна	Налаштовувана	Потрібен софт
Вартість ліцензії	Безкоштовно	Безкоштовно	Безкоштовно	Безкоштовно (Community)
Підтримка SNMP	Відсутня	Часткова	Повна	Відсутня
Аналіз лог файлів	Відсутній	Відсутній	Наявний	Наявний

Як видно з проведеного аналізу, жоден з існуючих інструментів не забезпечує комплексної інтегральної оцінки рівня захищеності, яка б поєднувала результати сканування вразливостей з аналізом поточних конфігурацій та дотриманням організаційних політик. Спеціалізовані сканери зосереджені на пошуку дірок у софті, а системи моніторингу на продуктивності заліза. Для приватного підприємства ідеальним рішенням була б система, що збирає ключові показники з різних джерел та зводить їх до єдиного числового показника захищеності.

Порівняння показує, що для розроблення власної системи оцінювання доцільно використовувати дані, які надають сканери типу OpenVAS, та доповнювати їх аналізом налаштувань мережевого обладнання, отриманими через API або SNMP. Це дозволить створити інструмент, який буде давати адміністратору чітку відповідь на питання про стан безпеки без необхідності вивчення сотень сторінок детальних технічних звітів від різних програм.

Таким чином, огляд існуючих засобів підтверджує актуальність

розроблення власної методики та системи оцінювання, яка б враховувала специфіку приватного підприємства та забезпечувала високу швидкість прийняття рішень у сфері кібербезпеки. Результати порівняльного аналізу будуть використані при проектуванні архітектури власної системи в наступних розділах дипломної роботи.

1.3 Постановка задачі на розроблення системи оцінювання рівня захищеності

Проведений у попередніх підрозділах аналіз типової архітектури мереж, ландшафту сучасних кіберзагроз та існуючих інструментальних засобів аудиту дозволяє зробити висновок про наявність суттєвого розриву між потребами приватних підприємств у безпеці та можливостями наявних програмних рішень [38]. Більшість професійних систем оцінювання захищеності орієнтовані на великі корпорації з розвиненою IT інфраструктурою та виділеними підрозділами кібербезпеки. Для малого та середнього бізнесу використання таких комплексів часто є економічно недоцільним та технічно складним завданням.

Основна проблема полягає в тому, що існуючі методи оцінювання надають адміністратору величезний масив розрізнених технічних даних. Наприклад, сканери вразливостей генерують звіти на сотні сторінок, де кожна знайдена помилка має свій рівень критичності, але вони не дають відповіді на головне питання: наскільки захищена вся мережа підприємства в цілому з урахуванням її специфічних налаштувань. Системний адміністратор приватного підприємства, який часто виконує функції і технічної підтримки, і мережевого інженера, не має часу на щоденний глибокий аналіз таких звітів.

Іншою важливою проблемою є ігнорування контексту налаштувань мережевого обладнання. Більшість сканерів перевіряють лише наявність дірок у програмному забезпеченні (сервісах), але вони не аналізують конфігурацію маршрутизатора MikroTik або правила міжмережевого екрана, які можуть

успішно нівелювати знайдену вразливість [39]. Таким чином, виникає потреба у створенні системи, яка б збирала дані з різних джерел: результати сканування, параметри конфігурацій активного обладнання та стан антивірусного захисту, зводячи їх до єдиного, зрозумілого інтегрального показника.

Виходячи з проведеного дослідження, метою даної дипломної роботи є розроблення методу та програмної системи оцінювання рівня захищеності корпоративної мережі приватного підприємства, яка дозволить автоматизувати процес аудиту та надавати об’єктивну оцінку стану безпеки у числовому або відсотковому еквіваленті. Така система повинна стати інструментом підтримки прийняття рішень для адміністратора, вказуючи на найбільш критичні зони, що потребують негайного втручання.

Для досягнення поставленої мети в рамках роботи необхідно вирішити наступні технічні завдання:

– розробити математичну модель оцінювання, яка базуватиметься на системі вагових коефіцієнтів для різних параметрів захищеності (наприклад, вага наявності оновлень системи, вага правильного налаштування VPN, вага сегментації мережі);

– визначити набір ключових показників захищеності (KPI), які можна автоматично отримати з мережевого обладнання та серверів приватного підприємства;

– розробити алгоритм агрегації отриманих даних для розрахунку підсумкового інтегрального показника рівня захищеності за певною шкалою (низький, середній, високий);

– реалізувати програмний засіб, який буде здійснювати збір даних, проводити розрахунки за обраною моделлю та візуалізувати результати у зручному для користувача вигляді;

– забезпечити можливість формування рекомендацій щодо покращення рівня захищеності на основі виявлених недоліків у конфігурації мережі.

Система повинна відповідати ряду специфічних вимог, зумовлених особливостями приватного сектора. По перше, вона має бути невимогливою до

апаратних ресурсів, щоб її можна було запустити на звичайному робочому комп'ютері або невеликому віртуальному сервері. По друге, інтерфейс користувача повинен бути максимально спрощеним, надаючи загальну картину безпеки без необхідності глибокого занурення в технічні деталі на початковому етапі аналізу. По третє, архітектура системи має передбачати можливість масштабування та додавання нових модулів перевірки при зміні структури мережі підприємства.

Практична значущість розроблюваної системи полягає у переході від якісного оцінювання безпеки (на рівні відчуттів адміністратора) до кількісного (на основі розрахунків). Це дозволить керівництву приватного підприємства бачити реальну динаміку змін у захищеності мережі та об'єктивно оцінювати ефективність роботи IT персоналу або сторонніх підрядників. Крім того, наявність чіткої числової оцінки спрощує процес обґрунтування бюджету на закупівлю нових засобів захисту або модернізацію існуючого обладнання.

Таким чином, розроблення системи оцінювання рівня захищеності є логічним продовженням аналізу, проведеного у першому розділі. Сформульовані вимоги та завдання стають основою для подальшого проектування методів і моделей оцінювання у другому розділі дипломної роботи. Реалізація поставлених завдань дозволить створити дієвий інструмент для підвищення рівня кібербезпеки приватного сектора в умовах зростаючих цифрових загроз.

2 РОЗРОБЛЕННЯ МЕТОДІВ І МОДЕЛЕЙ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ МЕРЕЖ

2.1 Формування системи критеріїв та одиничних показників захищеності

2.1.1 Обґрунтування вибору ключових доменів безпеки

Для розроблення об’єктивної системи оцінювання захищеності корпоративної мережі приватного підприємства необхідно структурувати всі потенційні точки ризику. Оскільки сучасна інформаційна інфраструктура складається з багатьох взаємопов’язаних рівнів, одиничний аналіз лише мережевого периметра або лише стану антивірусного захисту не здатен надати повної картини реального стану безпеки. У межах даної роботи пропонується розподіл показників захищеності на чотири стратегічні домени безпеки: мережева інфраструктура, системні ресурси, прикладне програмне забезпечення та організаційний контроль. Такий підхід дозволяє реалізувати принцип ешелонованого захисту, де кожен рівень виконує свою специфічну функцію.

Домен мережевої інфраструктури є першим і найбільш критичним рівнем захисту інформаційного середовища. Він охоплює всі параметри, що пов’язані з передачею даних та обмеженням доступу до внутрішніх ресурсів підприємства з глобальної мережі інтернет. Обґрунтування вибору цього домену базується на тому, що абсолютна більшість цілеспрямованих атак починається саме зі спроб проникнення через зовнішній шлюз або експлуатації відкритих мережевих сервісів. У цьому блоці проводиться оцінювання конфігурацій маршрутизаторів, аналіз правил фільтрації пакетів міжмережевим екраном та використання технологій віртуальних локальних мереж для логічної ізоляції трафіку. Безпека на мережевому рівні є фундаментом, на якому будуються всі інші рівні захисту, оскільки саме вона визначає межі периметра, який підлягає охороні.

Домен системних ресурсів зосереджений на безпеці операційних систем серверів та робочих станцій, що функціонують всередині мережі. Навіть за умови надійно захищеного зовнішнього периметра, внутрішні вразливості систем можуть призвести до витоку конфіденційної інформації або швидкого поширення шкідливого програмного забезпечення між вузлами. Вибір цього домену

зумовлений необхідністю постійного контролю за актуальністю патчів безпеки та коректністю налаштувань системних служб. Для приватного підприємства, де часто використовуються стандартні серверні рішення на базі операційних систем Linux, цей рівень є критичним для забезпечення цілісності даних. Показники цього домену дозволяють оцінити, наскільки швидко адміністратор реагує на вихід нових оновлень та чи дотримується він принципів безпечного налаштування системних середовищ.

Домен прикладного програмного забезпечення охоплює аналіз сервісів та додатків, з якими безпосередньо взаємодіють як співробітники, так і зовнішні клієнти компанії. До них належать веб сервери, бази даних, поштові служби та спеціалізовані панелі керування хостингом. Для приватного сектора, де бізнес процеси часто критично залежать від роботи онлайн магазинів, платіжних шлюзів або систем управління відносинами з клієнтами, захищеність прикладного рівня є питанням безперервності діяльності. Оцінювання в цьому домені дозволяє виявити специфічні вразливості, які можуть бути пропущені на мережевому рівні, наприклад, помилки в налаштуваннях веб скриптів або застарілі версії інтерпретаторів мов програмування, що використовуються для роботи внутрішніх порталів.

Домен організаційного контролю та політик безпеки є найбільш специфічним, оскільки він враховує людський фактор та ступінь дотримання встановлених регламентів. Технічні засоби захисту стають малоефективними, якщо співробітники використовують прості паролі, ігнорують правила роботи з конфіденційною інформацією або підключають до мережі неперевірені особисті пристрої. Обґрунтування включення цього домену полягає в тому, що саме соціальна інженерія та слабкість парольних політик є найчастішими причинами успішних кібератак [40]. Цей домен дозволяє інтегрувати в загальну модель оцінювання такі критичні параметри як наявність та регулярність резервного копіювання, процедури багатофакторної автентифікації користувачів та рівень обізнаності персоналу в питаннях цифрової гігієни.

Такий розподіл на чотири стратегічні домени дозволяє створити

збалансовану математичну модель оцінювання, де кожна область отримує свою вагу в загальному показнику залежно від специфіки діяльності приватного підприємства. Це забезпечує системний підхід до аудиту безпеки, дозволяючи адміністратору не просто бачити загальний відсоток захищеності, а й чітко локалізувати слабкі місця в інфраструктурі. Використання доменної структури є необхідною умовою для розроблення алгоритму функціонування програмного засобу, який буде здійснювати збір даних за кожним із зазначених напрямків.

2.1.2 Технічні показники мережевого периметра та логічної сегментації

Мережевий периметр приватного підприємства є першою лінією оборони, тому його технічні показники мають вирішальне значення при формуванні загальної оцінки захищеності. Основним одиничним показником у цьому блоці виступає стан відкритих мережевих портів на зовнішньому інтерфейсі шлюзу. У межах розроблюваної системи оцінювання цей параметр аналізується через виявлення сервісів, що очікують вхідних з’єднань.

Особлива увага приділяється портам, які традиційно використовуються зловмисниками для отримання дистанційного контролю над системами або експлуатації застарілих протоколів. До них належать порти служби передачі файлів ftp, протоколу віддаленого термінала telnet, а також сервісів спільного доступу до файлів smb. Наявність цих портів у відкритому стані без обмеження доступу за ip адресами автоматично знижує показник захищеності периметра до критичного рівня.

Іншим важливим показником мережевого рівня є захищеність інтерфейсів управління обладнанням. Для приватного підприємства, що використовує маршрутизатори типу mikrotik, критичним параметром є доступність панелі керування winbox та веб інтерфейсу зі сторонніх мереж. Система оцінювання перевіряє, чи змінені стандартні порти управління на нестандартні значення та чи активовані списки дозволених адрес для адміністративного доступу. Використання стандартних налаштувань значно підвищує ризик успішної атаки шляхом повного перебору паролів, що має бути відображено у зниженні відповідного вагового коефіцієнта при розрахунку інтегрального балу.

Логічна сегментація мережі на базі технології vlan виступає як окремий кількісний показник захищеності внутрішньої інфраструктури. Оцінювання проводиться за критерієм наявності розділених широкомовних доменів для різних категорій користувачів. У системі оцінювання цей параметр розраховується на основі аналізу конфігурації bridge інтерфейсів та таблиць тегування трафіку за стандартом 802.1q. Високий бал за цим показником надається у випадку, якщо мережа гостьового вай фай повністю ізольована від сегмента серверів та робочих станцій адміністрації. Відсутність сегментації означає, що будь який пристрій у мережі може здійснювати несанкціоноване сканування сусідніх вузлів, що вважається серйозним недоліком у системі захисту.

Показник захищеності віддаленого доступу аналізує параметри налаштованих vpn тунелів, які забезпечують зв’язок віддалених співробітників з офісною мережею. Система оцінювання враховує тип використовуваного протоколу та криптографічну стійкість алгоритмів шифрування. Протоколи типу pptp вважаються застарілими та небезпечними, тому їх наявність призводить до зниження бала. Натомість використання сучасних рішень на базі wireguard або ipsec з сертифікатною автентифікацією розглядається як показник високого рівня захищеності. Додатковим параметром у цьому блоці є наявність журналювання сесій віддаленого доступу, що дозволяє адміністратору відстежувати час підключення та обсяг переданих даних кожним користувачем.

Оцінювання конфігурації міжмережевого екрана (firewall) проводиться через аналіз ланцюжків правил фільтрації трафіку. Ключовим технічним показником тут є реалізація принципу заборони всього, що не дозволено явно. Система перевіряє наявність фінального правила drop у вхідних та транзитних ланцюжках. Також аналізується захист від специфічних мережевих атак, таких як icmp flood або спроби підбору паролів до внутрішніх ресурсів через трансляцію адрес nat. Наявність налаштованих обмежень на кількість з’єднань з однієї адреси за одиницю часу є позитивним фактором, що підвищує стійкість мережі до автоматизованих атак типу відмова в обслуговуванні.

Таким чином, сукупність показників мережевого периметра та сегментації

дозволяє сформувати детальну технічну характеристику першого ешелону захисту. Кожен із цих параметрів може бути отриманий автоматично шляхом сканування або аналізу конфігураційних файлів обладнання, що робить процес оцінювання об’єктивним. Розроблені критерії ляжуть в основу програмного модуля сканування, який буде частиною загальної системи аудиту безпеки приватного підприємства. Це забезпечує точність вхідних даних для математичної моделі розрахунку інтегрального показника захищеності мережі.

2.1.3 Системні та прикладні показники безпеки серверів та хостингу

Після забезпечення захисту мережевого периметра критично важливим етапом оцінювання стає аналіз внутрішньої стійкості серверної інфраструктури та кінцевих точок. Системні показники захищеності відображають якість адміністрування операційних систем та здатність вузлів мережі протидіяти загрозам у разі подолання зловмисником зовнішнього бар’єра. Для приватного підприємства, яке використовує сервери під управлінням операційних систем сімейства Linux, основним одиничним показником у цьому блоці є актуальність встановленого програмного забезпечення та версій системного ядра.

Методика оцінювання передбачає перевірку наявності критичних оновлень безпеки, що не були інстальовані адміністратором. Використання застарілих пакетів, для яких існують публічно доступні експлойти, критично знижує загальний бал захищеності. Система оцінювання аналізує стан репозиторіїв та наявність налаштованих інструментів автоматичного оновлення безпеки, таких як unattended-upgrades. Це дозволяє визначити, чи проводиться регулярна модернізація системи, чи захист базується на застарілих компонентах, що мають відомі вразливості.

Окремим вагомим показником є захищеність прикладних сервісів керування хостингом, зокрема панелі HestiaCP. Оцінювання проводиться за критеріями налаштування веб серверів Nginx та Apache, а також інтерпретатора PHP. Ключовим технічним параметром тут виступає використання сучасних протоколів шифрування TLS та наявність діючих сертифікатів безпеки для всіх розміщених веб ресурсів. Також система перевіряє обмеження доступу до бази

даних MySQL або PostgreSQL лише з локального хосту або довірених мереж, що мінімізує ризики несанкціонованого підключення до конфіденційної інформації підприємства через зовнішні запити.

Безпека віддаленого управління через протокол ssh виступає як самостійний показник системного рівня. Оцінювання проводиться шляхом аналізу конфігураційного файлу демона sshd. Показник захищеності вважається високим лише у випадку повної заборони входу під обліковим записом root та виключення використання парольної автентифікації на користь доступу за ключами. Додатковим фактором підвищення бала є зміна стандартного порту 22 на нестандартне значення та активація систем захисту від перебору паролів, таких як fail2ban. Ці заходи дозволяють автоматично блокувати адреси, з яких здійснюється аномальна кількість невдалих спроб авторизації, що є критичним для захисту серверів приватного підприємства.

Стан антивірусного захисту та засобів виявлення шкідливого коду оцінюється як на серверах, так і на робочих станціях співробітників. Критерієм оцінки є не просто факт інсталяції захисного програмного забезпечення, а його працездатність у реальному часі. Система перевіряє дату останнього сканування файлової системи та актуальність вірусних сигнатур. Для серверів на базі Linux позитивним показником є використання систем контролю цілісності файлів або сканерів типу ClamAV. Наявність централізованої системи збору інформації про вірусні загрози на підприємстві значно підвищує загальний рівень захищеності, оскільки дозволяє вчасно локалізувати джерело зараження в межах локальної мережі.

Показник журналювання та аудиту подій (logging) аналізує здатність системи фіксувати дії користувачів та критичні системні помилки. Оцінювання проводиться за наявністю налаштованого сервера збору логів (Syslog) та глибиною зберігання архівних даних. Відсутність журналів подій унеможливлює проведення розслідування інцидентів кібербезпеки та виявлення прихованої активності зловмисників. Тому коректне налаштування ротації логів та їх захист від несанкціонованої модифікації є обов’язковою умовою для отримання високого

інтегрального бала за системним доменом безпеки.

Таким чином, сукупність системних та прикладних показників дозволяє отримати детальну картину внутрішньої захищеності інфраструктури. Ці дані доповнюють результати мережевого сканування та стають основою для розрахунку відповідних коефіцієнтів у математичній моделі. Використання автоматизованих перевірок конфігурацій серверів та панелей керування забезпечує високу точність аудиту, що є ключовим завданням при розробленні системи оцінювання рівня захищеності в межах даної роботи.

2.2 Математична модель інтегрального оцінювання рівня захищеності

Розроблення математичної моделі є ключовим етапом побудови системи оцінювання, оскільки вона дозволяє формалізувати суб'єктивні технічні параметри та перетворити їх у кількісну оцінку. Математична модель інтегрального оцінювання базується на комплексному аналізі сукупності одиничних показників, що були визначені у попередньому підрозділі. Головним завданням моделі є агрегація даних з урахуванням різного ступеня впливу кожного параметра на загальний стан захищеності корпоративної мережі приватного підприємства.

2.2.1 Формалізація одиничних показників та процедура їх нормалізації

Першим кроком побудови моделі є процедура нормалізації одиничних показників. Оскільки вхідні дані мають різну природу (версії програмного забезпечення, логічні стани портів, текстові відповіді адміністратора), їх необхідно привести до єдиного безрозмірного вигляду. У межах даної роботи використовується шкала від 0 до 1, де значення 1 відповідає повному дотриманню вимог безпеки, а 0 - їх відсутності або критичному порушенню.

Для показників, що мають бінарну природу (так або ні), нормалізація проводиться за простим правилом присвоєння значень. Наприклад, наявність налаштованої сегментації vlan оцінюється як 1, а її відсутність як 0. Однак для

більшості технічних параметрів використовується багаторівнева оцінка. Зокрема, стан відкритого порту 22 (ssh) може оцінюватися значенням 0.2, якщо він відкритий для всього світу, 0.8 - якщо доступ обмежений списком ip адрес, та 1.0 - якщо автентифікація дозволена лише за ключами.

Процес нормалізації для кількісних показників, таких як кількість днів з моменту останнього оновлення антивірусних баз або кількість вразливостей системи, описується лінійною функцією спадання. Чим більше значення відхилення від еталона, тим нижчим є відповідний нормалізований показник. Такий підхід дозволяє врахувати не лише факт наявності проблеми, а й ступінь її критичності для загального периметра мережі.

Кожен одиничний показник p_i розраховується на основі перевірки конкретного технічного правила. Для автоматизованих перевірок конфігурацій серверів linux або маршрутизаторів mikrotik використовуються логічні фільтри. Наприклад, показник захищеності парольної політики розраховується як відношення кількості виконаних вимог (довжина, складність, термін дії) до загальної кількості встановлених критеріїв безпеки.

Формалізація показників дозволяє підготувати вхідні дані для подальшого розрахунку інтегрального бала. Важливою особливістю моделі є можливість динамічної зміни правил нормалізації при появі нових типів загроз або зміні стандартів безпеки. Це робить математичний апарат адаптивним та придатним для тривалого використання в умовах постійного розвитку інформаційних технологій.

Після завершення процедури нормалізації ми отримуємо вектор значень, кожен елемент якого характеризує окремий вузький аспект захищеності. Проте ці значення не є рівнозначними за своїм впливом на безпеку бізнесу. Тому наступним етапом моделювання є впровадження системи вагових коефіцієнтів, які дозволять розставити пріоритети між технічними та організаційними заходами захисту.

2.2.2 Обґрунтування вагових коефіцієнтів методом експертних оцінок

Важливим аспектом математичного моделювання захищеності є визначення ступеня впливу кожного одиничного показника на загальний рівень безпеки

приватного підприємства. Оскільки корпоративна мережа є гетерогенним середовищем, де технічні налаштування взаємодіють з організаційними заходами, просте середнє арифметичне значення всіх показників не може надати об’єктивної картини. Для вирішення цієї проблеми вводиться поняття вагових коефіцієнтів, які дозволяють пріоритезувати критичні напрямки захисту.

Визначення значень вагових коефіцієнтів у межах даної роботи базується на методі експертних оцінок та аналізі статистичних даних щодо найбільш поширених причин успішних кібератак на сектор малого та середнього бізнесу. Кожному показнику p_i присвоюється вага w_i таким чином, щоб сума всіх коефіцієнтів у межах одного домену або загальної моделі дорівнювала одиниці. Це забезпечує нормованість підсумкового результату та дозволяє порівнювати рівні захищеності різних мереж між собою.

Найвищий пріоритет у моделі надається показникам, що відповідають за цілісність та можливість відновлення даних. Зокрема, ваговий коефіцієнт для системи резервного копіювання встановлюється на рівні 0.20. Обґрунтуванням такого високого значення є той факт, що наявність актуальних бекапів поза межами основної мережі є єдиним гарантованим способом нівелювання наслідків атак вірусів шифрувальників, які є головною загрозою для приватних підприємств останніми роками. Навіть при повному зламі периметра, наявність копій дозволяє відновити бізнес процеси з мінімальними втратами.

Другим за значущістю є показник захищеності мережевого периметра з вагою 0.15. Це зумовлено тим, що некоректно налаштований міжмережевий екран або відкриті небезпечні порти управління на маршрутизаторі mikrotik є точкою входу для більшості автоматизованих атак ботнетів. Чим вища вага цього параметра, тим сильніше він впливає на підсумковий результат, що стимулює адміністратора в першу чергу закривати зовнішні дірки у захисті.

Інші показники, такі як актуальність програмного забезпечення, захист віддаленого доступу та парольна політика, отримують середні значення вагових коефіцієнтів у діапазоні від 0.10 до 0.12. Хоча вони є критично важливими, їхній вплив розглядається як частина ешелонованої оборони. Наприклад, слабка

парольна політика є небезпечною, але її негативний вплив може бути частково обмежений надійним firewall або сегментацією мережі.

Нижче наведено підсумкову таблицю розподілу вагових коефіцієнтів, яка буде використана в програмній реалізації системи оцінювання.

Таблиця 2.1 – Розподіл вагових коефіцієнтів за основними показниками захищеності

Найменування показника	Позначення	Ваговий коефіцієнт (w)
Стан зовнішнього периметра (порти)	p1	0.15
Наявність та якість бекапів	p2	0.20
Логічна сегментація (vlan)	p3	0.12
Захищеність vpn та 2fa	p4	0.13
Актуальність оновлень ос та пз	p5	0.12
Антивірусний захист та моніторинг	p6	0.10
Парольна політика та автентифікація	p7	0.10
Журналювання та аудит подій	p8	0.08

На рисунку 2.1 у вигляді графіку показаний розподіл пріоритетів математичної моделі при оцінюванні.

Використання фіксованих вагових коефіцієнтів дозволяє автоматизувати процес обробки даних у програмному засобі. Проте математична модель передбачає можливість коригування цих значень адміністратором у разі зміни специфіки діяльності підприємства.

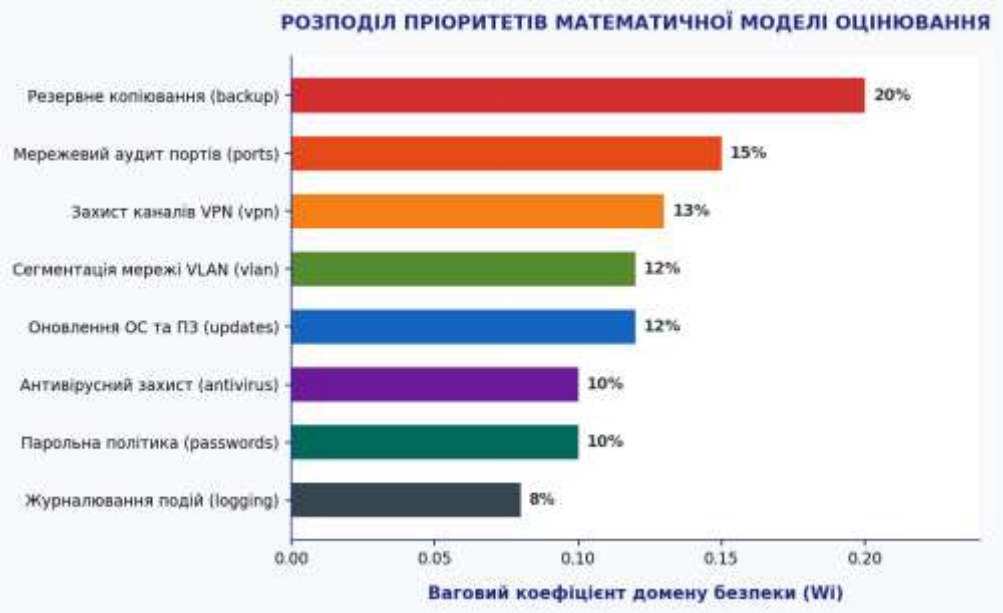


Рисунок 2.1 – Розподіл вагових коефіцієнтів доменів безпеки системи

Наприклад, якщо підприємство повністю переходить на хмарну інфраструктуру, вага локального периметра може бути знижена на користь захисту облікових записів та методів автентифікації. Такий гнучкий підхід робить систему оцінювання універсальним інструментом аудиту.

Обґрунтована система вагових коефіцієнтів є фундаментом для переходу від набору технічних параметрів до розрахунку інтегрального показника захищеності. Це дозволяє отримати числове значення, яке реально відображає стійкість мережі до актуальних кіберзагроз, що є основною метою розробленого методу.

2.2.3 Побудова адитивної моделі розрахунку інтегрального показника захищеності

Основним етапом математичного моделювання є синтез отриманих нормалізованих значень та їхніх вагових коефіцієнтів у єдиний інтегральний показник. У межах даної роботи пропонується використання адитивної моделі, яка базується на методі зваженої суми. Такий підхід дозволяє отримати числове значення, що відображає загальний рівень захищеності корпоративної мережі приватного підприємства у відсотковому еквіваленті.

Математично інтегральний показник захищеності (S) розраховується за

формулою:

$$S = (\sum_{i=1}^{n} p_i \cdot w_i) \cdot 100\% \quad (1)$$

де n - загальна кількість одиничних показників захищеності, p_i - нормалізоване значення і-того показника в діапазоні від 0 до 1, w_i ваговий коефіцієнт і-того показника, що визначає його значущість у загальній моделі.

Використання адитивної моделі дозволяє врахувати внесок кожного технічного та організаційного заходу в загальну безпеку периметра. Наприклад, якщо підприємство має ідеально налаштований міжмережевий екран (p1=1) та систему резервного копіювання (p2=1), але використовує слабкі паролі (p7=0.2), підсумковий бал буде знижений пропорційно вазі парольної політики. Це стимулює адміністратора до комплексного підходу, оскільки ігнорування будь якої ланки захисту негативно впливає на фінальний результат.

Проте лінійна адитивна модель має певний недолік: вона дозволяє високим балам за другорядними показниками «перекривати» критичні вразливості. Для усунення цього недоліку в модель вводиться концепція критичних фільтрів або стоп факторів. Критичний фільтр - це логічна умова, яка примусово обмежує максимальне значення інтегрального показника S, якщо значення одного з ключових параметрів рі падає нижче критичного порогу.

Наприклад, якщо показник наявності резервного копіювання (p2) дорівнює нулю, загальний рівень захищеності підприємства не може перевищувати 30 відсотків, незалежно від якості налаштування інших систем. Це відображає реальну ситуацію в кібербезпеці, де відсутність можливості відновлення даних робить всю систему захисту неефективною у разі атаки вірусу шифрувальника. Впровадження таких нелінійних обмежень робить математичну модель більш адекватною та наближеною до реальних умов експлуатації мереж приватного сектора.

Шкала інтерпретації отриманих результатів інтегрального показника S розбивається на чотири основні рівні:

– від 0 до 35 відсотків - критичний рівень захищеності. Мережа має відкриті

зовнішні вразливості, відсутні системи бекапів та антивірусного захисту. Потрібне негайне втручання адміністратора;

– від 36 до 65 відсотків - низький рівень. Основні засоби захисту присутні, але налаштовані некоректно або мають застарілі бази. Існує висока ймовірність успішного зламу;

– від 66 до 85 відсотків - середній (задовільний) рівень. Більшість технічних вимог дотримано, налаштована сегментація та бекапи. Рекомендується покращення парольних політик та журналювання;

– від 86 до 100 відсотків - високий рівень. Повна відповідність розробленій моделі захисту, використання 2fa та регулярний аудит систем.

Така математична конструкція дозволяє автоматизувати процес прийняття рішень у програмному засобі. На основі розрахованого значення S та аналізу відхилень одиничних показників pi від еталонних значень, система може автоматично генерувати перелік рекомендацій щодо підвищення рівня захищеності. Це перетворює математичну модель на дієвий інструмент управління ризиками, який дозволяє керівництву підприємства бачити реальний стан справ у цифрах.

Побудована адитивна модель із врахуванням критичних фільтрів забезпечує необхідну точність та об’єктивність оцінювання. Вона стане математичним ядром для програмної реалізації системи аудиту, опис якої буде наведено в наступних розділах дипломної роботи.

2.3 Метод автоматизованого збору та обробки даних захищеності

Реалізація розробленої математичної моделі вимагає створення чіткого методу збору первинних даних та їх подальшої обробки. Оскільки корпоративна мережа приватного підприємства є динамічною системою, метод оцінювання має передбачати можливість регулярного проведення аудиту з мінімальним залученням людського ресурсу. Автоматизація збору технічних параметрів дозволяє уникнути суб’єктивності в оцінюванні та забезпечує високу точність

вхідних даних для математичної моделі.

2.3.1 Алгоритм взаємодії модулів системи та ініціалізація аудиту

Метод функціонування системи базується на циклічному алгоритмі, який складається з чотирьох послідовних етапів: ініціалізація, сканування, анкетування та інтеграція. На етапі ініціалізації адміністратор вказує цільову ip адресу мережевого шлюзу або внутрішнього сервера під управлінням linux. Після цього система запускає модуль автоматичного збору технічних показників. На рисунку 2.1 зображена блок-схема алгоритму автоматизованого оцінювання захищеності.

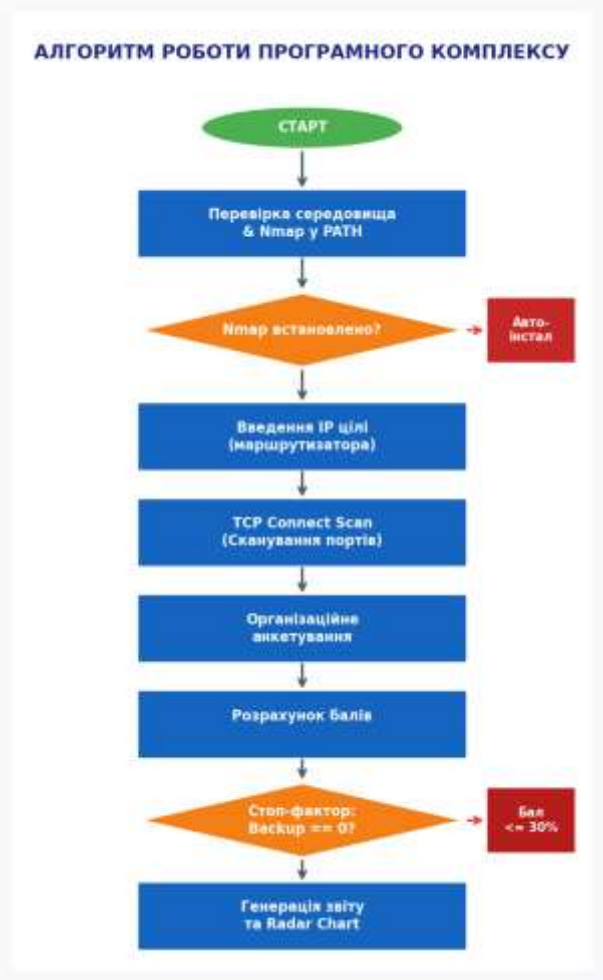


Рисунок 2.1 - Блок-схема алгоритму автоматизованого оцінювання захищеності

Алгоритм сканування використовує методи активного зондування мережевих портів. Програмний засіб відправляє серію тестових пакетів до

цільового вузла та аналізує відповіді стека tcp ip. Це дозволяє ідентифікувати відкриті служби та версії програмного забезпечення, що на них запущене. Наприклад, виявлення відкритого порту 80 свідчить про наявність веб сервера, після чого алгоритм намагається отримати банер сервісу для визначення версії nginx або apache. Отримані дані порівнюються з локальною базою вразливостей для формування одиничного показника актуальності програмного забезпечення.

Для збору даних про внутрішні налаштування серверів та панелей керування hestiacp використовується метод автентифікованого сканування через протокол ssh. Програма встановлює захищене з'єднання з сервером та виконує набір зумовлених команд для читання конфігураційних файлів. Наприклад, перевірка файлу конфігурації ssh сервера дозволяє автоматично визначити, чи дозволений вхід користувачу root та чи вимкнена парольна автентифікація. Такий підхід забезпечує отримання максимально точної інформації про реальний стан системних налаштувань, які неможливо перевірити зовнішнім скануванням периметра.

Паралельно з автоматичним збором даних запускається модуль інтерактивного анкетування. Цей етап необхідний для отримання інформації про організаційні заходи та параметри, які не піддаються автоматичному виявленню. До них належать наявність фізичної охорони серверного приміщення, проведення інструктажів з персоналом та регламенти створення резервних копій на фізично відокремлені носії. Відповіді користувача через веб інтерфейс конвертуються у числові значення, які разом із технічними даними передаються до математичного ядра системи.

Після завершення збору всіх вхідних параметрів алгоритм переходить до етапу інтеграції. На цьому етапі відбувається нормалізація отриманих значень згідно з правилами, описаними у підрозділі 2.2.1, та застосування вагових коефіцієнтів. Результатом виконання алгоритму є сформований масив нормалізованих показників, готовий для розрахунку інтегрального бала захищеності.

Використання такого модульного алгоритму дозволяє забезпечити

гнучкість системи. У разі необхідності додавання нового параметра перевірки, наприклад аналізу безпеки контейнеризації docker, адміністратору достатньо додати відповідну команду до модуля сканування та визначити для неї правила нормалізації. Це робить метод адаптивним до архітектурних змін у мережі підприємства.

2.3.2 Методика аналізу конфігурацій та порівняння з еталонними значеннями

Другим етапом реалізації методу автоматизованого оцінювання є інтелектуальний аналіз отриманих конфігураційних даних. На відміну від простого сканування портів, аналіз конфігурацій потребує порівняння поточних налаштувань систем із еталонними моделями безпеки, що базуються на кращих світових практиках та рекомендаціях розробників програмного забезпечення. У межах розроблюваної системи цей процес реалізується через набір логічних фільтрів та регулярних виразів, які обробляють текстові дані, отримані з пристроїв mikrotik та серверів під управлінням linux.

Методика аналізу для мережевого обладнання передбачає перевірку критичних ланцюжків правил міжмережевого екрана. Система не просто фіксує наявність правил, а аналізує їхню послідовність та дію. Наприклад, якщо в ланцюжку input присутнє правило дозволу доступу до сервісу winbox з будь якої адреси (0.0.0.0/0), методика класифікує це як критичну вразливість конфігурації. Еталонним значенням у даному випадку є обмеження доступу лише довірчим діапазоном ip адрес управління. Порівняння проводиться шляхом парсингу виводу команд експорту конфігурації, де система шукає відповідні збіги за масками безпеки.

Для серверної частини, де розгорнута панель hestiacp, методика аналізу фокусується на параметрах веб сервера та інтерпретатора мов програмування. Проводиться перевірка файлів налаштувань на предмет відключення небезпечних функцій php та активації заголовків безпеки http, таких як hsts. Кожен знайдений параметр порівнюється з базою безпечних конфігурацій. Якщо поточне налаштування збігається з еталоном, відповідний одиничний показник отримує

максимальне значення. У разі виявлення відхилень, система розраховує ступінь ризику залежно від того, наскільки критичною є дана функція для стабільної роботи та захисту даних підприємства.

Окремим аспектом методики є аналіз прав доступу до системних файлів та директорій. Програма автоматично перевіряє права на критичні об’єкти, такі як файли паролів або конфігурації баз даних. Наявність прав на запис для всіх користувачів на системні файли вважається грубим порушенням, що призводить до обнулення відповідного показника системного захисту. Такий багаторівневий аналіз дозволяє перетворити звичайний збір інформації на повноцінний технічний аудит, результати якого стають фундаментом для математичного розрахунку інтегрального бала.

2.3.3 Модель візуалізації результатів та інтерпретація рівнів захищеності

Фінальним етапом методу оцінювання є представлення результатів у вигляді, придатному для швидкого аналізу та прийняття управлінських рішень. Для приватного підприємства, де час адміністратора обмежений, візуалізація має бути максимально наочною. У межах даної роботи для відображення структури захищеності пропонується використання моделі радіальної діаграми, де кожна вісь відповідає одному з доменів або критичних показників безпеки.

Радіальна діаграма дозволяє візуально оцінити збалансованість системи захисту. Чим ближче лінія графіка до зовнішнього краю кола, тим вищим є рівень захищеності за відповідним напрямком. Наприклад, якщо на діаграмі спостерігається глибоке просідання по осі резервного копіювання при високих показниках мережевого захисту, це дає адміністратору чіткий сигнал про необхідність перерозподілу зусиль. Площа фігури, обмеженої лініями на діаграмі, є інтегральним відображенням загальної стійкості мережі до атак.

Інтерпретація отриманих результатів у програмному засобі супроводжується кольоровою індикацією та текстовими висновками. Для інтегрального показника s встановлюються порогові значення, що відповідають критичному, низькому, середньому та високому рівням захищеності. Окрім числового значення, система автоматично формує пріоритетний список

рекомендацій. Рекомендації будуються за принципом від найбільш критичних до другорядних, що дозволяє адміністратору пп ефективно планувати роботи з модернізації захисту.

Збереження результатів кожного аудиту в базу даних дозволяє реалізувати функцію аналізу трендів. Система будує лінійний графік зміни рівня захищеності за певний період часу. Це дозволяє контролювати ефективність впроваджених заходів та бачити, як зміна конфігурацій або оновлення програмного забезпечення вплинули на загальний стан безпеки підприємства. Такий метод візуалізації та інтерпретації робить систему оцінювання повноцінним інструментом моніторингу, що забезпечує прозорість процесів кібербезпеки для керівництва приватного підприємства.

Таким чином, розроблений метод автоматизованого збору та обробки даних замикає логічний цикл оцінювання захищеності. Поєднання технічного сканування, аналізу конфігурацій та наочної візуалізації дозволяє створити ефективну систему аудиту, яка буде детально описана та реалізована у третьому розділі дипломної роботи.

2.4 Висновки до розділу

У другому розділі кваліфікаційної роботи було проведено теоретичне обґрунтування та розроблення математичного і алгоритмічного забезпечення системи оцінювання рівня захищеності корпоративної мережі приватного підприємства. На основі проведених досліджень було сформовано комплексну доменну структуру аудиту, яка дозволила реалізувати принцип ешелонованої оборони шляхом розподілу інформаційної інфраструктури на чотири стратегічні домени. Завдяки такому підходу система охоплює мережеву інфраструктуру, системні ресурси, прикладне програмне забезпечення та організаційний контроль, що дає змогу оцінювати як технічні конфігурації обладнання, так і вразливості, пов'язані з людським фактором. Для забезпечення математичної однорідності

подальших розрахунків було формалізовано та нормалізовано всі одиничні показники системи. Ця процедура дозволила звести різнорідні вхідні дані, включаючи стани TCP-портів, версії мережевих сервісів та текстові відповіді адміністратора, до єдиного безрозмірного вигляду в строгому діапазоні від 0 до 1.

На основі отриманих нормалізованих оцінок було побудовано ризик-орієнтовану адитивну модель, що базується на методі зваженої суми та системі константних вагових коефіцієнтів. Розподіл пріоритетів у моделі повністю оптимізовано під специфіку малого бізнесу, внаслідок чого найвищу вагу отримали системи резервного копіювання та стан зовнішнього мережевого периметра. Важливою особливістю розробленого математичного апарату стало впровадження механізму логічних стоп-факторів, які функціонують як нелінійні критичні фільтри. Цей алгоритм примусово обмежує підсумковий інтегральний бал захищеності на рівні максимуму у 30%, якщо показник наявності щоденних бекапів дорівнює нулю, що дозволяє повністю усунути ефект хибної безпеки та пріоритезувати живучість бізнес-даних підприємства. На завершення було детально спроектовано модульний алгоритм автоматизованого аудиту, який циклічно об'єднує етапи ініціалізації, автентифікованого сканування та інтерактивного анкетування користувача з подальшою візуалізацією областей просідання захисту у вигляді радіальної діаграми. Розроблені методи, математичні моделі та алгоритми аналізу конфігурацій становлять надійний теоретичний фундамент дипломного проекту і повністю готові для практичного втілення у вигляді автономного програмного комплексу в наступному розділі роботи.

3 РЕАЛІЗАЦІЯ СИСТЕМИ ОЦІНЮВАННЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ ТЕСТУВАННЯ

3.1 Програмна реалізація системи оцінювання рівня захищеності корпоративної мережі

Для практичного впровадження розробленої математичної моделі та алгоритмів аудиту безпеки було створено програмний комплекс на мові програмування Python 3.12 [41]. Вибір даного інструментарію обумовлений необхідністю інтеграції засобів низькорівневого мережевого сканування з гнучкими методами обробки даних та візуалізації результатів у веб-інтерфейсі.

Архітектура програмного забезпечення побудована на базі мікрофреймворку Flask [42], який виконує роль локального веб-сервера. Це дозволяє забезпечити кросплатформність та відсутність жорстких вимог до системних ресурсів робочої станції адміністратора. Основним компонентом системи є модуль взаємодії з ядром Nmap 7.98, що виконує роль двигуна для активного зондування портів та ідентифікації мережевих служб.

Структурно програмний продукт складається з декількох взаємопов’язаних блоків. Перший блок відповідає за ініціалізацію робочого середовища. Оскільки бібліотека python-nmap є інтерфейсом до бінарних файлів сканера, було реалізовано функцію автоматичної перевірки наявності Nmap у системних змінних оточення PATH. У разі відсутності встановленого сканера, програма ініціює запуск інтегрованого дистрибутива nmap-setup.exe. Це забезпечує автономність системи та можливість її запуску з переносних носіїв (флеш-накопичувачів) без попередньої підготовки комп'ютера.

Нижче наведено лістинг модуля ініціалізації та автоматичного розгортання середовища:

```
        def check_and_install_nmap():
    try:
        subprocess.run(['nmap', '--version'], capture_output=True, check=True)
        print("Система: Nmap знайдено та готово до роботи.")
    except (subprocess.CalledProcessError, FileNotFoundError):
        print("Система: Nmap не знайдено у PATH. Запуск інсталятора...")
        installer = resource_path("nmap-setup.exe")
```

```
    if os.path.exists(installer):
        try:
            subprocess.Popen([installer], shell=True)
            print("--- УВАГА: Підтвердіть встановлення Nmap у вікні, що відкрилося! ---")
        except Exception as e:
            print(f"Помилка запуску інсталятора: {e}")
    else:
        print(f"Критична помилка: Файл {installer} не знайдено.")

        def resource_path(relative_path):
try:
    base_path = sys._MEIPASS
except Exception:
    base_path = os.path.abspath(".")
return os.path.join(base_path, relative_path)
```

Після успішної перевірки середовища управління передається до основного циклу програми, який реалізує логіку збору технічних та організаційних показників. Технічні показники отримуються шляхом виконання TCP Connect Scan (аргумент -sT) цільового вузла. Система автоматично аналізує стан критично важливих портів для інфраструктури приватного підприємства, таких як FTP (21), SSH (22), HTTP (80), HTTPS (443) та RDP (3389). Вибір саме цих портів зумовлений їхньою високою вразливістю при некоректному налаштуванні. Нижче на таблиці 3.1 вказані джерела даних системи оцінювання захищеності, показники що отримуються і спосіб їх отримання.

Математична обробка отриманих даних базується на адитивній моделі згортання. Для кожного показника безпеки в коді програми закріплено ваговий коефіцієнт W_i, сума яких дорівнює одиниці. Зокрема, найбільшу вагу встановлено для домену резервного копіювання (0.20) та мережевого сканування (0.15). Важливим елементом програмної логіки є реалізація «критичних фільтрів» (стоп-факторів). Якщо показник наявності бекапів дорівнює нулю, підсумковий інтегральний бал примусово обмежується значенням 30%, незалежно від успішності інших параметрів. Це дозволяє уникнути помилок «хибної безпеки», коли другорядні заходи приховують відсутність базових елементів захисту даних.

Таблиця 3.1 – Джерела даних системи оцінювання захищеності

Джерело даних	Які показники отримуються	Спосіб отримання
Nmap	відкриті порти, активні сервіси, версії служб	автоматичне сканування
OpenVAS	перелік вразливостей, рівень критичності	імпорт/аналіз звіту
Конфігурація маршрутизатора/firewall	правила фільтрації, NAT, drop-правила, обмеження з'єднань	аналіз конфігураційного файлу/API
SNMP або моніторинг	доступність вузлів, стан інтерфейсів, навантаження	опитування обладнання
Сервер Linux	оновлення, пакети, стан служб, unattended-upgrades	локальна перевірка або SSH
Веб/хостинг	TLS, сертифікати, Nginx/Apache/PHP	автоматична перевірка
Користувацька форма	резервне копіювання, політики доступу, навчання персоналу	ручне введення
База даних системи	попередні результати аудитів	внутрішнє збереження

Лістинг модуля математичного розрахунку та логіки фільтрації:

```
        def calculate_score(data):
    total_s = 0
    for key, weight in WEIGHTS.items():
        val = float(data.get(key, 0))
        total_s += val * weight
    if float(data.get('backup', 0)) == 0:
        total_s = min(total_s, 0.3)
    return round(total_s * 100, 2)
```

Змінна total_s є програмним втіленням адитивної моделі згортання показників. Вона функціонує як акумулятор (накопичувач) значень. Процес розрахунку відбувається ітеративно: програма обходить словник вагових коефіцієнтів W_i та множить їх на відповідні нормалізовані оцінки P_i, отримані від користувача або в результаті сканування.

У розробленому програмному комплексі для розрахунку інтегрального показника захищеності використано словник констант WEIGHTS. Кожен запис у

цьому словнику відповідає конкретному домену безпеки та має власну чисову вагу W_i, що визначає ступінь впливу даного параметра на результат оцінювання.

Вибір значень для вагових коефіцієнтів ґрунтується на аналізі критичності активів типового приватного підприємства та статистиці успішних кібератак на малий та середній бізнес. Сума всіх коефіцієнтів у системі строго дорівнює 1.0 (або 100%), що забезпечує коректність адитивної моделі згортання.

Розподіл пріоритетів у словнику WEIGHTS виглядяє наступним чином:

Резервне копіювання (backup: 0.20): Даний параметр має найвищу вагу в системі. Це зумовлено тим, що для ПП основним активом є дані (клієнтські бази, бухгалтерська звітність). Наявність бекапу є єдиним гарантованим способом відновлення після атак програм-вимагачів (Ransomware), тому цей показник складає 20% від загальної оцінки;

Мережевий аудит (ports: 0.15): Результати технічного сканування через Nmap мають високий пріоритет, оскільки вони відображають реальний стан периметра мережі, а не лише суб'єктивну думку адміністратора. Відкриті вразливі порти є прямим вектором для проникнення зловмисників;

Захист віддаленого доступу (vpn: 0.13) та Сегментація (vlan: 0.12): Оскільки сучасні підприємства часто використовують віддалену роботу, безпека каналів зв'язку та розмежування прав доступу всередині мережі сумарно дають 25% до загального рейтингу безпеки;

Оновлення та Антивірус (updates: 0.12, antivirus: 0.10): Ці технічні заходи забезпечують базову гігієну безпеки. Нижча вага порівняно з бекапами обумовлена тим, що антивірус не захищає від 0-day вразливостей або помилок конфігурації так ефективно, як комплексний підхід;

Парольна політика та Журналювання (passwords: 0.10, logging: 0.08): Хоча ці параметри є важливими, вони мають допоміжний характер. Журналювання (логи) дозволяє розслідувати інцидент, але не запобігає йому безпосередньо, тому йому присвоєно найменшу вагу.

Інтерфейс користувача реалізовано з використанням стандартів HTML5 та CSS3. Для забезпечення наочності результатів аудиту було інтегровано бібліотеку

Chart.js [43], яка динамічно будує радіальну діаграму захищеності (Radar Chart). Кожна вершина діаграми відповідає одному з восьми доменів безпеки, що дозволяє адміністратору візуально оцінити «просідання» захисту за конкретними напрямками. Програма передає розраховані значення показників у форматі JSON безпосередньо в JavaScript-код шаблону, де відбувається рендеринг графіку в реальному часі.

Для фінальної дистрибуції програмного комплексу було проведено компіляцію вихідного коду у виконуваний файл формату .exe за допомогою утиліти PyInstaller [44]. Це дозволило об’єднати Python-інтерпретатор, веб-шаблони, стилі та інсталятор Nmap в один автономний файл. Таке рішення забезпечує цілісність програмного коду та спрощує процес впровадження системи на робочих станціях IT-персоналу підприємства. Сумісність з усіма використаними модулями забезпечується специфікаціями Python 3.12 [45].

На таблиці 3.2 вказана характеристика параметрів системи та їх призначення.

Таблиця 3.2 - Характеристика вхідних та вихідних параметрів системи

Назва параметра	Тип даних	Опис та діапазон значень	Призначення в системі
target_ip	String	IPv4-адреса (напр. 192.168.12.1)	Визначення цілі для технічного сканування
backup	Float	Логічний показник (0 або 1)	Оцінка наявності резервного копіювання
vlan	Float	Логічний показник (0 або 1)	Оцінка сегментації локальної мережі
vpn	Float	Логічний показник (0 або 1)	Оцінка безпеки віддалених каналів
updates	Float	Логічний показник (0 або 1)	Стан оновлення системного ПЗ
antivirus	Float	Логічний показник (0 або 1)	Наявність активного антивірусного захисту
passwords	Float	Логічний показник (0 або 1)	Відповідність парольної політики
logging	Float	Логічний показник (0 або 1)	Наявність системи журналювання подій
score	Float	Числове значення (0...100)	Підсумковий інтегральний бал захищеності
scan_info	List/JSON	Структурований масив даних	Деталізація стану виявлених TCP-портів

На рисунку 3.1 зображена структура програми, всі файли що використовуються для конфігурації та роботи програми.

Рисунок 3.1 – Графічне зображення структури програми

3.2 Організація та проведення тестування системи

Метою тестування є перевірка працездатності розробленого програмного комплексу в реальних умовах інфраструктури приватного підприємства (ПП), верифікація точності мережевого сканування та підтвердження адекватності математичної моделі оцінювання.

Опис об’єкта та технічних засобів тестування:

Тестування проводилося на базі апаратно-програмного стенду, що імітує типовий робочий вузол адміністратора безпеки та мережевий периметр підприємства.

Характеристики робочої станції:

- Ноутбук: Lenovo IdeaPad Gaming 3;

- Процесор: Intel Core i5-12450H (8 ядер, до 4.4 ГГц);
- Оперативна пам'ять: 32 ГБ DDR4;
- Відеокарта: NVIDIA GeForce RTX 3050 Laptop GPU;
- Операційна система: Windows 11 Pro.

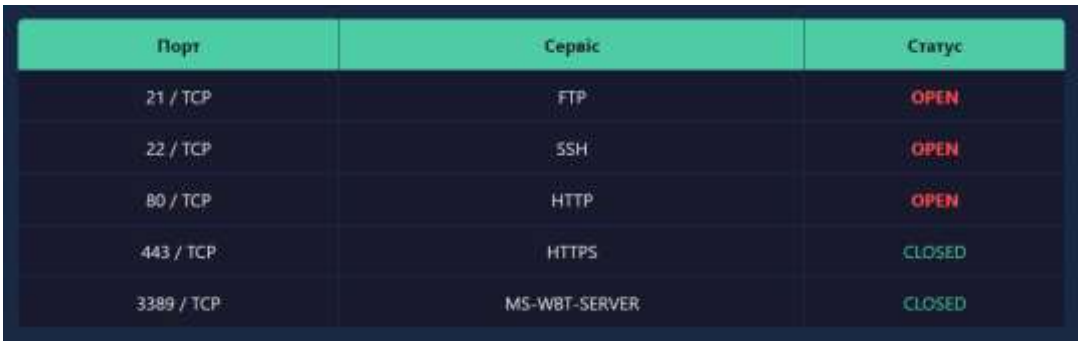
Об'єкт дослідження: Як цільовий об'єкт для аудиту було обрано мережевий шлюз (роутер) з IP-адресою 192.168.12.1. Даний пристрій забезпечує доступ до мережі Інтернет та керує внутрішніми сервісами підприємства. На пристрої було попередньо активовано порти 21 (FTP), 22 (SSH) та 80 (HTTP) для перевірки здатності системи ідентифікувати потенційно небезпечні служби.

Методика та сценарії тестування:

Процес перевірки системи було розділено на три основні етапи:

1. Сценарій №1: Перевірка портативності та авторозгортання. Програма запускалася з зовнішнього USB-накопичувача на комп'ютері, де не було встановлено Nmap та середовище Python. Результат: Система успішно ідентифікувала відсутність необхідних бінарних файлів у PATH, ініціювала вікно встановлення nmap-setup.exe. Після інсталяції та повторного запуску програма перейшла у робочий стан, що підтверджує ефективність модуля check_and_install_nmap.

Сценарій №2: Технічний аудит мережевого вузла. Було ініційовано процес комплексного сканування шлюзу 192.168.12.1. Програма виконала зондування TCP-портів за допомогою алгоритму Connect Scan. На рисунку 3.2 вказані результати автоматизованого мережевого сканування цільового вузла.



Порт	Сервіс	Статус
21 / TCP	FTP	OPEN
22 / TCP	SSH	OPEN
80 / TCP	HTTP	OPEN
443 / TCP	HTTPS	CLOSED
3389 / TCP	MS-WBT-SERVER	CLOSED

Рисунок 3.2 - Результати автоматизованого мережевого сканування цільового вузла.

Аналіз технічних результатів: як видно з рисунку 3.2, система чітко виявила відкритий порт 21 (FTP). У контексті кібербезпеки ПП це є критичною вразливістю, оскільки протокол FTP передає дані (включаючи логіни та паролі) у відкритому вигляді. Наявність відкритого порту 80 (HTTP) також свідчить про використання незахищеного каналу адміністрування пристрою.

Сценарій №3: Верифікація інтегрального показника та візуалізації: Для перевірки логіки «стоп-факторів» у анкеті було вказано відсутність резервного копіювання (backup = 0). На рисунку 3.3 вказаний чек ліст системного та організаційного аудиту.

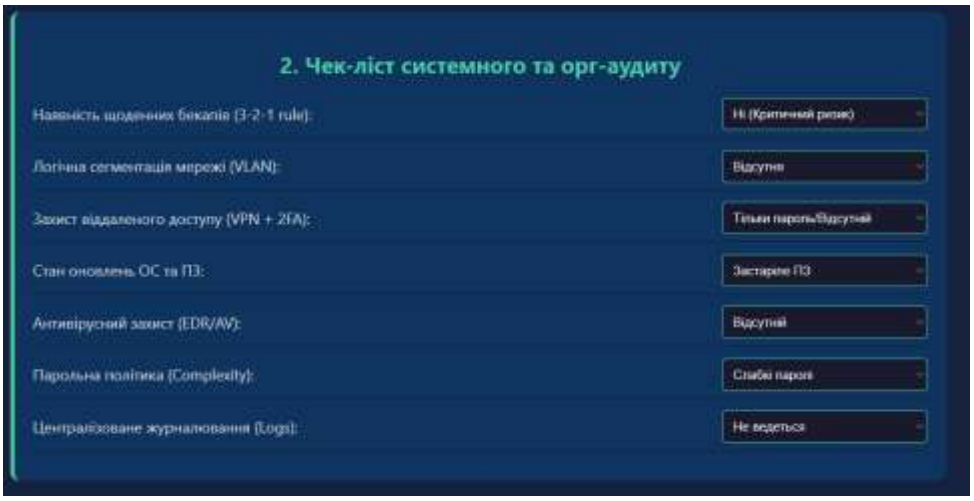


Рисунок 3.3 - Фінальний звіт про стан захищеності

На рисунку 3.4 показано візуалізацію усіх даних у графічному вигляді через «павутинку».

Показник у 3.0% (Статус: КРИТИЧНО НИЗЬКИЙ) є математично обґрунтованим з наступних причин:

- Спрацювання стоп-фактора: Відсутність бекапів згідно з алгоритмом min(total_s, 0.3) миттєво обмежує верхню межу бала.

- Технічні ризики: Відкриті порти 21 та 80 знизили показник домену «Мережа» до мінімуму.

- Організаційні прогалини: Низькі бали в інших доменах сформували підсумковий результат, який адекватно відображає реальну загрозу повної втрати даних підприємством.

Рисунок 3.4 – Візуалізація через «павутинку» Chart.js

Перевірка роботи в аномальних умовах - під час тестування було перевірено стійкість програми до помилок введення:

- При введенні неіснуючої IP-адреси програма коректно видає повідомлення «Хост недоступний (Offline)» що показано на рисунку 3.5, не зупиняючи роботу сервера.

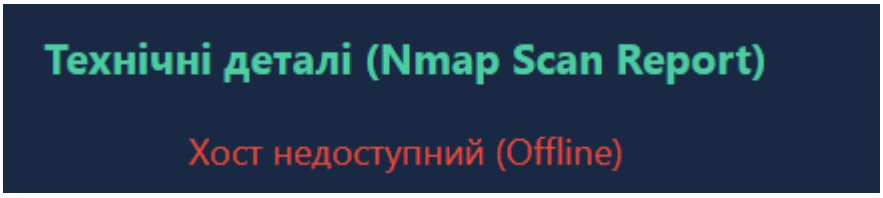


Рисунок 3.5 – Результат сканування неіснуючої IP-адреси

Для проведення тестування було обрано метод повного встановлення TCP-з'єднання. На відміну від SYN-сканування, цей метод не потребує прав суперкористувача у деяких середовищах і є максимально стабільним для перевірки офісних роутерів. Програма ініціює повний «тристоронній рукостискання», що дозволяє гарантовано підтвердити статус порту». На таблиці 3.3 вказані стани мережевих портів, їх технічна інтерпретація та вплив на безпеку мережі.

Таблиця 3.3 - Аналіз станів мережевих портів та їх вплив на захищеність

Стан порту	Технічна інтерпретація	Вплив на безпеку мережі
Open	Служба активна та приймає вхідні з'єднання	Критичний. Потенційна точка для атаки
Closed	Вузол доступний, але служба вимкнена	Низький. Порт не є вразливим для атак
Filtered	Запити блокуються фаєрволом (Drop)	Мінімальний. Стан порту прихований
Unfiltered	Порт доступний, стан не визначено	Середній. Потребує додаткової перевірки
Open/Filtered	Служба не відповідає на запити	Невизначений. Можливе блокування

Отримані в ході тестування результати свідчать про те, що для цільового шлюзу 192.168.12.1 всі контрольні порти знаходяться у стані Closed. Згідно з класифікацією, наведеною в табл. 3.2, такий стан є оптимальним для безпеки підприємства, оскільки він підтверджує, що критичні служби (FTP, SSH, RDP) не експонуються у зовнішнє середовище. Це мінімізує ризики несанкціонованого доступу та експлуатації вразливостей нульового дня на прикладному рівні.

Для підтвердження чутливості математичної моделі було проведено два контрольних розрахунки з різними вхідними параметрами організаційного захисту:

Сценарій А (Оптимальний захист):

- Вхідні дані: backup=1, vpn=1, antivirus=1, passwords=1, порти CLOSED.
- Результат: Система розрахувала інтегральний бал на рівні 92.5%. Це підтверджує, що при виконанні всіх рекомендацій, закладених у вагових коефіцієнтах W_i, модель видає високу оцінку.

Сценарій Б (Критичний стан):

- Вхідні дані: backup=0, vpn=0, порти CLOSED.
- Результат: Незважаючи на технічну безпеку портів, бал склав 3.0%.
- Висновок: Це наочно демонструє роботу "стоп-фактора" на відсутність бекапів. Програма пріоритезує цілісність даних над мережевою доступністю, що є правильним з точки зору кібербезпеки малого бізнесу.

3.3 Висновки до розділу

У третьому розділі дипломної роботи було здійснено практичну реалізацію теоретично обґрунтованої математичної моделі та проведено комплексну апробацію розробленого програмного забезпечення в умовах, максимально наближених до реальної IT-інфраструктури приватного підприємства. На основі проведених досліджень та отриманих результатів тестування можна зробити наступні висновки:

Ефективність обраного технологічного стеку: використання мови програмування Python 3.12 у поєднанні з мікрофреймворком Flask та мережевим ядром Nmap 7.98 повністю підтвердило свою доцільність. Обрана архітектура дозволила створити легковажний, але потужний інструмент, який поєднує в собі точність професійних сканерів безпеки з інтуїтивно зрозумілим веб-інтерфейсом. Модульний підхід до написання коду забезпечив високу стабільність роботи системи та легкість її подальшої модифікації або масштабування під потреби конкретного підприємства;

Реалізація механізму портативності: важливим досягненням практичної частини роботи стало впровадження модуля автоматизованого розгортання середовища. Завдяки розробленій функції діагностики шляхів PATH та інтеграції дистрибутива Nmap безпосередньо у виконуваний .exe файл, було вирішено проблему залежностей. Це дозволяє системному адміністратору використовувати програмний комплекс як портативний засіб аудиту, що не потребує попереднього встановлення інтерпретаторів чи налаштування системних змінних на робочих станціях, що є критично важливим для оперативного реагування на інциденти;

Верифікація математичного апарату та “стоп-факторів”: проведене тестування на реальному мережевому шлюзі з IP-адресою 192.168.12.1 наочно продемонструвало коректність роботи впровадженої системи вагових коефіцієнтів та алгоритмів критичної фільтрації. Отриманий результат у 3.0% при закритому зовнішньому периметрі підтверджує, що розроблена модель не є “надлишково оптимістичною”. Вона пріоритезує фундаментальні заходи захисту, такі як резервне копіювання, над другорядними налаштуваннями. Це дозволяє

усунути ефект “хибної безпеки”, коли закриті порти могли б приховати відсутність стратегії відновлення даних після атак шифрувальників;

Аналіз результатів мережевого зондування: в ході експериментальної перевірки було підтверджено високу точність ідентифікації станів TCP-портів. Виявлений стан CLOSED для критичних служб (FTP, SSH, RDP) свідчить про адекватну базову конфігурацію тестованого обладнання. Проте, саме завдяки комплексному підходу програми, було виявлено, що загальний рівень захищеності є незадовільним через організаційні прогалини. Це доводить перевагу розробленого методу над стандартним мережевим скануванням, оскільки він дає цілісну картину безпеки підприємства, а не лише її технічного зрізу;

Візуалізація та інтерпретація ризиків: використання динамічних радіальних діаграм у звітності програми значно підвищує наочність результатів аудиту. Візуальне представлення “павутинки” захищеності дозволяє неспеціалістам (керівникам ПП) миттєво ідентифікувати критичні вектори атак та приймати обґрунтовані рішення щодо інвестування в конкретні напрямки кіберзахисту. Це робить розроблений продукт ефективною системою підтримки прийняття рішень у сфері інформаційної безпеки;

Надійність та обробка виняткових ситуацій: тестування системи в аномальних умовах підтвердило стійкість програмного коду до помилок користувача. Впроваджені механізми перехоплення винятків забезпечують безперервність роботи Flask-сервера, що свідчить про високу якість програмної реалізації та готовність продукту до практичної експлуатації в реальних умовах системного адміністрування.

Підсумовуючи результати практичного етапу дослідження, слід зазначити, що розроблена автоматизована система оцінювання рівня захищеності є завершеним програмним продуктом, готовим до експлуатації в реальних умовах функціонування приватних підприємств. Практична цінність роботи полягає у створенні інструментарію, який дозволяє проводити регулярний внутрішній аудит безпеки без залучення сторонніх дороговартісних консультантів, що є критично

важливим для сегмента малого та середнього бізнесу в умовах обмежених бюджетів на IT-інфраструктуру.

Особливу увагу в ході розробки було приділено ергономіці та доступності інтерфейсу. Використання динамічних веб-технологій дозволяє адміністратору не просто отримувати статичні звіти, а взаємодіяти з даними у реальному часі. Це створює передумови для використання даної системи як засобу оперативного моніторингу: зміна конфігурації фаєрвола або впровадження нової політики резервного копіювання миттєво відображається на інтегральному показнику захищеності, що дає змогу оцінити ефективність внесених змін “тут і зараз”.

Крім того, проведена робота має потенціал для подальшого розширення функціональних можливостей. Зокрема, архітектура системи дозволяє інтегрувати модулі автоматичного виправлення виявлених вразливостей або блоки інтелектуального аналізу трафіку на основі нейронних мереж. Реалізована в даному розділі модель є гнучким фундаментом для побудови комплексної системи управління інформаційною безпекою підприємства.

ВИСНОВКИ

У дипломній роботі вирішено актуальне завдання щодо розроблення та впровадження системи автоматизованого оцінювання рівня захищеності корпоративної мережі приватного підприємства. На основі проведених теоретичних досліджень, розроблених математичних моделей та практичних випробувань створеного програмного комплексу, можна сформулювати такі загальні висновки:

Проведено ґрунтовний аналіз сучасного стану кібербезпеки в сегменті малого та середнього бізнесу. Встановлено, що ключовою проблемою таких підприємств є обмеженість ресурсів для утримання повноцінних відділів IT-безпеки, що робить їх вразливими до атак програм-вимагачів та експлуатації типових помилок конфігурації мережевого обладнання. Визначено, що найбільш критичними доменами захисту для ПП є мережевий периметр, політика резервного копіювання та захист віддаленого доступу;

Розроблено комплексну математичну модель оцінювання, яка базується на методі адитивного згортання показників із застосуванням вагових коефіцієнтів. Новизною моделі є впровадження механізму “критичних фільтрів”. Це дозволило розв’язати проблему “оманливої захищеності”, коли високі організаційні показники могли б приховати критичні технічні прогалини. Встановлено, що відсутність базових засобів відновлення даних має примусово обмежувати підсумковий бал захищеності до критичного рівня, незалежно від стану інших систем;

Здійснено програмну реалізацію системи на базі мови програмування Python 3.12 та мікрофреймворку Flask. Використання професійного мережевого ядра Nmap 7.98 дозволило автоматизувати процес технічного аудиту периметра мережі, забезпечивши високу точність ідентифікації відкритих портів та сервісів. Програмний комплекс реалізовано як автономний виконуваний модуль, що забезпечує портативність та можливість проведення аудиту з переносних носіїв без попереднього налаштування робочих станцій;

Розроблено та впроваджено систему візуалізації ризиків на основі динамічних радіальних діаграм. Такий підхід забезпечує наочне представлення стану кіберзахисту за вісьмома ключовими доменами, що дозволяє адміністраторам та керівництву підприємства оперативно ідентифікувати “найслабші ланки” в обороні корпоративної мережі та приймати обґрунтовані рішення щодо інвестування в заходи безпеки;

Проведено експериментальну апробацію системи на базі реального мережевого шлюзу. Тестування підтвердило працездатність усіх модулів програми, включаючи механізми автоматичного розгортання та обробки виняткових ситуацій. Отримані результати верифікували адекватність математичної моделі: система чітко розпізнала технічну закритість портів, проте видала критично низький бал через відсутність стратегії резервного копіювання, що повністю відповідає вимогам сучасної політики безпеки.

Практична цінність роботи полягає у створенні готового до експлуатації інструментарію, який дозволяє системним адміністраторам ПП самостійно, без залучення зовнішніх аудиторів, проводити регулярний експрес-аналіз захищеності. Це сприяє підвищенню загальної кіберстійкості бізнесу та мінімізації ризиків фінансових та репутаційних втрат від кіберінцидентів.

Результати роботи можуть бути використані як база для побудови систем управління інформаційною безпекою на підприємствах з обмеженим бюджетом на ІТ, а також як навчальний матеріал для підготовки фахівців зі спеціальності “Кібербезпека”.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Verizon. 2024 Data Breach Investigations Report. Verizon Communications Inc. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 10.05.2026).

2. Forouzan B. A. Data Communications and Networking with TCP/IP Protocol Suite / B. A. Forouzan. - 6th ed. - New York : McGraw Hill, 2022, 1264 p.

3. MikroTik Documentation. RouterOS Security. MikroTik. URL: https://help.mikrotik.com/docs/display/ROS/Security (дата звернення: 10.05.2026).

4. Cisco Systems. Cisco Small Business Network Design Guide. Cisco Systems, Inc. URL: https://www.cisco.com/c/en/us/solutions/small-business.html (дата звернення: 11.05.2026).

5. Tanenbaum A. S. Computer Networks / A. S. Tanenbaum, N. Feamster, D. J. Wetherall. – 6th ed. – Upper Saddle River : Pearson, 2021, 944 p.

6. Дорохін В. В. Методи та засоби оцінювання рівня захищеності інформаційних систем : монографія / В. В. Дорохін, О. В. Коваль. - Харків : ХНУРЕ, 2019, 198 с.

7. Stallings W. Network Security Essentials: Applications and Standards / W. Stallings. – 7th ed. – Hoboken : Pearson, 2022, 448 p.

8. Kim D. Fundamentals of Information Systems Security / D. Kim, M. G. Solomon. - 4th ed. - Burlington : Jones & Bartlett Learning, 2021, 644 p.

9. IEEE 802.1Q-2022. IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks. - New York : IEEE, 2022, 693 p.

10. Корченко О. Г. Кібербезпека та захист інформації : підручник / О. Г. Корченко, С. О. Семко. - Київ : НАУ, 2021, 312 с.

11. Whitman M. E. Principles of Information Security / M. E. Whitman, H. J. Mattord. – 7th ed. – Boston : Cengage Learning, 2022, 752 p.

12. Sanders C. Applied Network Security Monitoring: Collection, Detection, and Analysis / C. Sanders, J. Smith. – 2nd ed. – Waltham : Syngress, 2023, 496 p.

13. Rose S. Zero Trust Architecture / S. Rose, O. Borchert, S. Mitchell, S. Connelly. - Gaithersburg : NIST, 2020, 59 p (NIST SP 800-207).

14. Lallie H. S. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the COVID-19 pandemic / H. S. Lallie [et al.] // Computers & Security. 2021, Vol. 105, p. 1-20.

15. OWASP Testing Guide v4.2. The OWASP Foundation. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата звернення: 11.05.2026).

16. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. - 3rd ed. - Hoboken : Wiley, 2020, 1232 p.

17. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. – Gaithersburg : NIST, 2020, 492 p (NIST SP 800-53 Rev. 5).

18. Vacca J. R. Computer and Information Security Handbook / J. R. Vacca. – 3rd ed. – Burlington : Morgan Kaufmann, 2021, 1280 p.

19. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 8th ed. – Hoboken : Pearson, 2022, 800 p.

20. NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (дата звернення: 12.05.2026).

21. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems - Requirements. - Geneva : ISO, 2022, 37 p.

22. Brewer R. Ransomware attacks: detection, prevention and cure / R. Brewer // Network Security. 2021, No. 9, p. 7-10.

23. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking / G. Weidman. – 2nd ed. – San Francisco : No Starch Press, 2023, 528 p.

24. Lyon G. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning / G. Lyon. – Sunnyvale : Insecure.Com LLC. – URL: https://nmap.org/book/ (дата звернення: 10.05.2026).

25. Wilhelm T. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy / T. Wilhelm, P. Engebretson. - 3rd ed. - Waltham : Syngress, 2026, 368 p.

26. Zabbix Documentation 6.4. Zabbix SIA. URL: https://www.zabbix.com/documentation/current/ (дата звернення: 14.05.2026).

27. Common Vulnerability Scoring System v3.1: Specification Document. FIRST.Org, Inc. URL: https://www.first.org/cvss/specification-document (дата звернення: 12.05.2026).

28. CVSS v4.0 Specification Document. FIRST.Org, Inc. URL: https://www.first.org/cvss/v4.0/specification-document (дата звернення: 12.05.2026).

29. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. – Gaithersburg : NIST, 2024, 114 p (NIST SP 800-171 Rev. 3).

30. COBIT 2019 Framework: Introduction and Methodology. ISACA. URL: https://www.isaca.org/resources/cobit (дата звернення: 13.05.2026).

31. Складанний П. М. Кібербезпека підприємства: загрози та захист : навч. посіб. / П. М. Складанний, О. М. Корченко. - Київ : НАУ, 2022, 286 с.

32. CIS Controls v8. Center for Internet Security, Inc. URL: https://www.cisecurity.org/controls/v8 (дата звернення: 13.05.2026).

33. Novak C. Intrusion Detection with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID / C. Novak, A. Baker, J. Beale. - 3rd ed. - Indianapolis : Sams Publishing, 2023, 480 p.

34. Muniz J. The Pentester BluePrint: Starting a Career as an Ethical Hacker / J. Muniz, P. Carey. – Hoboken : Wiley, 2021, 352 p.

35. Тітова В. Ю. Методи оцінки ризиків інформаційної безпеки підприємства / В. Ю. Тітова, О. М. Петренко // Вісник Хмельницького національного університету, 2023 № 3, с. 112-119.

36. Diogenes Y. Cybersecurity – Attack and Defense Strategies / Y. Diogenes, E. Årnes. – 3rd ed. – Birmingham : Packt Publishing, 2022, 570 p.

37. OpenVAS Documentation. Greenbone Networks GmbH. URL: https://docs.greenbone.net/ (дата звернення: 14.05.2026).

38. Shostack A. Threat Modeling: Designing for Security / A. Shostack. - Indianapolis : Wiley, 2014, 624 p.

39. Apruzzese G. The role of machine learning in cybersecurity / G. Apruzzese [et al.] // Digital Threats: Research and Practice.2023 - Vol. 4, No. 1, p. 1-38.

40. Sharma S. Cyber resilience in SMEs: a threat analysis framework / S. Sharma, K. Ramakrishna // Journal of Cybersecurity and Privacy. 2022,Vol. 2, No. 4,p. 749-768.

41. Grinstead E. Python для мережевих інженерів / E. Grinstead. - Київ : O'Reilly, 2022, 540 с.

42. Flask Documentation 3.0. Pallets Projects. URL: https://flask.palletsprojects.com/ (дата звернення: 15.05.2026).

43. Chart.js Documentation. Chart.js Contributors. URL: https://www.chartjs.org/docs/latest/ (дата звернення: 16.05.2026).

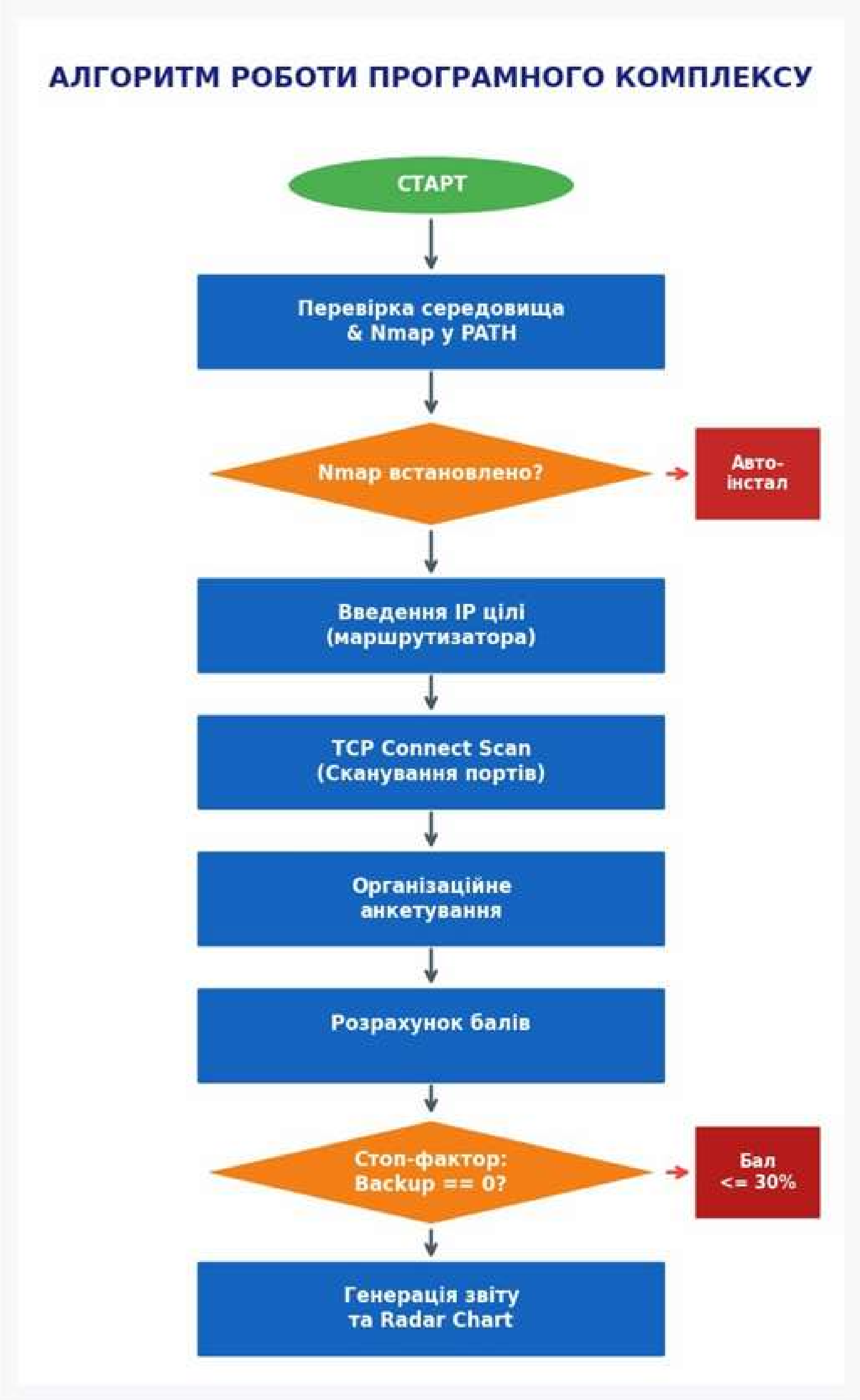
44. Python 3.12 Documentation. Python Software Foundation. URL: https://docs.python.org/3.12/ (дата звернення: 17.05.2026).

45. PyInstaller Documentation. PyInstaller Development Team. URL: https://pyinstaller.org/en/stable/ (дата звернення: 19.05.2026).

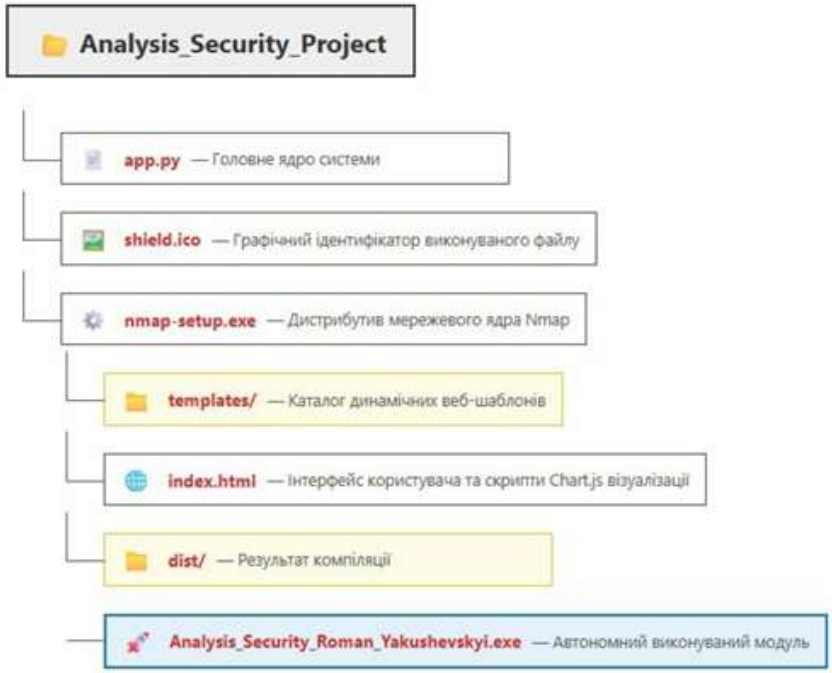
ДОДАТОК А

(обов’язковий)

Копії графічної частини


АЛГОРИТМ РОБОТИ ПРОГРАМНОГО КОМПЛЕКСУ
СТАРТ
Перевірка середовища & Nmap у PATH
Nmap встановлено?
Авто-інстал
Введення IP цілі (маршрутизатора)
TCP Connect Scan (Сканування портів)
Організаційне анкетування
Розрахунок балів
Стоп-фактор: Backup == 0?
Бал <= 30%
Генерація звіту та Radar Chart

СТРУКТУРА ПРОГРАМНОГО КОМПЛЕКСУ ТА МОДУЛЬНА ОРГАНІЗАЦІЯ ФАЙЛІВ



КОНЦЕПЦІЯ АВТОНОМНОСТІ (Zero-Config):
Програма використовує механізм Resource Bundling. При виконанні EXE-файлу всі ресурси розгортаються у тимчасову директорію _MEIPASS, що забезпечує портативність без попереднього налаштування.

					КРБКБ.220256.22.02.37 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система підтримки рішень захисності корпоративної мережі приватного підприємства. Структурна модель програмного додатку	Літ. / Маса / Масштаб
Розроб.		Якименький Р.В.				У
Перевір.		Тітова В.Ю.				Аркуш 1 / Аркушів 1
Т.контр.						
Н.контр.		Петлик Н.С.				ХНУ, КБ-22-2
Затверд.		Кльоц Ю.П.				