Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут комп'ютерних наук та штучного інтелекту

Спеціальність 125 «Кібербезпека та захист інформації»

Освітня програма «Безпека інформаційних і комунікаційних систем»

В.о. зав. кафедрою КІСМТ

Марина ЄСІНА

"Допущено до захисту"

"___" _____2024р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: "Аналіз і розробка методики вибору засобів побудови системи мережевої безпеки"

оцінка "_____"

Голова ЕК

Лемешко О.В.

Керівник: д.т.н. Олійников Р.В _____

Рецензент: PhD з комп. наук Родінко М.Ю

_____

Виконавець: студент групи КБ-61

Стешенко І.Є._____

Харків 2024

РЕФЕРАТ

Дипломна робота магістерського рівня вищої освіти на тему «Аналіз і розробка методики вибору засобів побудови системи мережевої безпеки» містить 80 сторінок, 3 таблиці, 13 рисунків, 1 додаток та посилання на 26 джерел.

Основною метою роботи є аналіз і розробка методики вибору засобів побудови системи мережевої безпеки, зокрема міжмережевих екранів. Актуальність проблеми обумовлена необхідністю ефективного захисту інформаційних систем організацій від кіберзагроз.

У дослідженні був застосований метод аналізу ієрархій (AHP), що дозволяє вирішувати багатокритеріальні завдання прийняття рішень. Цей метод надає змогу структурувати задачу вибору засобів безпеки, визначати важливість критеріїв і проводити порівняння альтернатив. Програмна частина роботи була реалізована мовою Python, що дозволяє автоматизувати процес вибору. Програма зчитує вагові коефіцієнти критеріїв із текстового файлу і дозволяє користувачеві вводити оцінки для кожної альтернативи.

У результаті роботи була розроблена методика вибору міжмережевих екранів, яка базується на методі аналізу ієрархій. Запропонована методика дозволяє об'єктивно порівнювати альтернативи за низкою критеріїв, таких як продуктивність, безпека, масштабованість, вартість та інші. Програмне забезпечення, створене в рамках роботи, дає змогу автоматизувати процес прийняття рішень і забезпечує точність розрахунків. Новизна роботи полягає в адаптації AHP до специфічного завдання вибору міжмережевих екранів, що робить підхід ефективним у сфері мережевої безпеки.

Запропоновану методику та програмне забезпечення можна рекомендувати для використання в організаціях, які потребують надійної та ефективної системи мережевої безпеки. Методика допоможе приймати зважені рішення, враховуючи

важливі критерії, що стосуються продуктивності, безпеки та вартості засобів. Крім того, програма дозволяє легко адаптуватися до змін у пріоритетах організації, що робить її універсальною.

Практична значущість роботи полягає в розробці інструменту для прийняття рішень у сфері мережевої безпеки, який можна адаптувати під різні умови. Запропонована методика та програмне забезпечення дають змогу підвищити рівень безпеки організації через ретельний і систематичний вибір міжмережевих екранів. Використання методу аналізу ієрархій дозволяє знизити суб'єктивні впливи на прийняття рішень та забезпечити обґрунтований підхід до вибору засобів захисту. Отримані у роботі результати підтверджують, що застосування багатокритеріальних методів вибору, таких як метод аналізу ієрархій, є ефективним у сучасних умовах.

Подальші дослідження можуть бути спрямовані на розширення кількості критеріїв, що використовуються при виборі засобів мережевої безпеки. Зокрема, можна врахувати такі аспекти, як екологічність, енергоефективність або ступінь інтеграції з іншими системами безпеки. Крім того, можливо вдосконалення програмного забезпечення, зокрема додавання функціоналу для порівняння більшої кількості альтернатив та розширення можливостей щодо аналізу чутливості результатів. Ще один напрямок розвитку може полягати у застосуванні методу аналізу ієрархій для вибору інших засобів безпеки, що дозволить створити комплексний підхід до побудови мережевої інфраструктури з урахуванням усіх аспектів безпеки.

Ключові слова: МЕРЕЖЕВА БЕЗПЕКА, КІБЕРЗАГРОЗИ, МІЖМЕРЕЖЕВИЙ ЕКРАН, МЕТОД АНАЛІЗУ ІЄРАРХІЙ, МЕТОДИКА ВИБОРУ.

ABSTRACT

The master's thesis "Analysis and Development of a Methodology for Selecting Tools for Network Security Systems" consists of 80 pages, 3 tables, 13 figures, 1 appendix, and references of 26 sources.

The primary objective of this work is to analyze and develop a methodology for selecting tools to build network security systems, with a particular focus on firewalls. The relevance of this topic stems from the need for effective protection of organizational information systems against cyberthreats.

The research employs the Analytic Hierarchy Process (AHP) method, which is effective for addressing multi-criteria decision-making tasks. This method enables structuring the task of security tool selection, defining the importance of criteria, and comparing alternatives. The software component of the work was implemented in Python, allowing the selection process to be automated. The program reads criterion weight coefficients from a text file and allows the user to input ratings for each alternative.

As a result of this work, a firewall selection methodology based on AHP was developed. The proposed methodology enables objective comparison of alternatives across several criteria, such as performance, security, scalability, cost, and more. The software developed within this project automates decision-making and ensures calculation accuracy. The novelty of this work lies in the adaptation of AHP to the specific task of firewall selection, making this approach effective in the field of network security.

The proposed methodology and software are recommended for use in organizations that require a reliable and efficient network security system. The methodology aids in making balanced decisions, considering important criteria related to the performance, security, and cost of the tools. Additionally, the program allows for easy adaptation to changing organizational priorities, enhancing its versatility.

The practical significance of this work lies in the development of a decision-making tool for network security that can be adapted to different conditions. The proposed methodology and software enable organizations to improve their security level through a thorough and systematic firewall selection process. The use of AHP helps reduce subjective influences on decision-making and ensures a justified approach to choosing security tools. The results obtained confirm that the application of multi-criteria selection methods, such as AHP, is effective under modern conditions.

Further research may focus on expanding the number of criteria used for selecting network security tools. In particular, aspects such as environmental impact, energy efficiency, or the degree of integration with other security systems could be considered. Additionally, the software could be enhanced by adding functionality for comparing a larger number of alternatives and expanding sensitivity analysis capabilities. Another direction for development may involve applying AHP to the selection of other security tools, allowing for a comprehensive approach to building network infrastructure that considers all security aspects.

Keywords: NETWORK SECURITY, CYBERTHREATS, FIREWALL, ANALYTIC HIERARCHY PROCESS, SELECTION METHODOLOGY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

IoT	-	Інтернет речей
ME	-	Міжмережевий екран
AHP	-	Analytic Hierarchy Process
ASA	-	Adaptive Security Appliance
CI	-	Coherence Index
CR	-	Consistency Ratio
DoS	-	Denial-of-Service
DNS	-	Domain Name System
FTP	-	File Transfer Protocol
HTTP	-	Hyper Text Transfer Protocol
IAM	-	Identity and Access Management
IDS	-	Intrusion Detection System
IP	-	Internet Protocol
IPS	-	Intrusion Prevention System
NAT	-	Network Address Translation
NGFW	-	Next-Generation Firewall
OSI	-	Open Systems Interconnection
PF	-	Packet Filter
QoS	-	Quality of Service
SMTP	-	Simple Mail Transfer Protocol
TCP	-	Transmission Control Protocol
TLS	-	Transport Layer Security
UFW	-	Uncomplicated Firewall
VLAN	-	Virtual Local Area Network
VPN	-	Virtual Private Network

ВСТУП

З розвитком інформаційних технологій і збільшенням обсягів даних, які передаються через мережі, питання захисту інформаційних ресурсів стає все більш актуальним. Інформаційна безпека сучасних підприємств і організацій залежить від ефективності засобів захисту мережевих інфраструктур, що дозволяє запобігати несанкціонованому доступу, атакам і витоку конфіденційних даних. Одним із ключових аспектів забезпечення безпеки є побудова ефективної системи мережевої безпеки, що включає в себе комплекс методик і засобів захисту [1].

Метою даної дипломної роботи є аналіз існуючих методів та інструментів побудови системи мережевої безпеки, а також розробка методики вибору оптимальних засобів захисту для конкретного середовища. У роботі буде розглянуто різноманітні підходи до побудови мережевої безпеки, зокрема методики побудови багаторівневих систем захисту, використання криптографічних протоколів, аутентифікації та контролю доступу, а також засоби виявлення вторгнень (IDS/IPS), захисту від DDoS-атак, VPN та інші інструменти.

Існує безліч підходів до забезпечення мережевої безпеки, кожен з яких має свої сильні сторони та обмеження. Основні методи можна умовно поділити на декілька груп.

Методи аутентифікації та контролю доступу, аутентифікація користувачів та контроль доступу до ресурсів є однією з перших ліній захисту в мережевих системах. Використання сучасних методів аутентифікації, таких як двофакторна аутентифікація (2FA) або біометричні засоби, дозволяє значно підвищити рівень захисту.

Криптографічні методи, захист даних під час їх передавання забезпечується завдяки використанню криптографічних алгоритмів. Протоколи на основі

симетричного і асиметричного шифрування, такі як TLS, IPsec, забезпечують безпеку каналів зв'язку та захист від перехоплення або модифікації інформації.

Методи сегментації мережі, розділення мережі на сегменти дозволяє ізолювати важливі ресурси та обмежити шляхи для потенційних атак. Використання VLAN та інших технологій віртуалізації сприяє підвищенню безпеки та полегшує адміністрування мереж.

Системи виявлення та запобігання вторгненням (IDS/IPS). Системи IDS та IPS дозволяють аналізувати трафік та виявляти потенційно небезпечну активність у реальному часі. IDS здійснює пасивний моніторинг, тоді як IPS може активно блокувати атаки, втручаючись у трафік.

Захист від DDoS-атак, що полягають у перевантаженні системи великою кількістю запитів, є одними з найпоширеніших і небезпечних загроз для сучасних мереж. Засоби захисту від таких атак включають фільтрацію трафіку, балансування навантаження та використання спеціалізованих програмно-апаратних рішень.

Віртуальні приватні мережі (VPN), які дозволяють створювати захищені канали зв'язку через незахищені мережі, наприклад, Інтернет. Це забезпечує конфіденційність та цілісність даних, що передаються, і є важливим інструментом для забезпечення безпеки в розподілених системах.

Особливе місце серед засобів мережевої безпеки займають міжмережеві екрани (firewall). Вони є першою лінією захисту і виконують роль фільтра між внутрішньою мережею та зовнішнім світом, дозволяючи або блокуючи трафік на основі заданих правил [2]. Міжмережеві екрани можуть бути програмними, апаратними або комбінованими рішеннями, що працюють на різних рівнях мережевої моделі OSI (переважно на мережевому та транспортному рівнях).

Сучасні міжмережеві екрани еволюціонували від простого фільтрування пакетів до комплексних рішень, що включають в собі функції аналізу додатків,

виявлення загроз, моніторингу трафіку в реальному часі, а також інтеграцію з іншими системами безпеки, такими як IDS/IPS. Такі рішення відомі як NGFW (Next-Generation Firewall) і мають низку переваг порівняно з традиційними рішеннями.

Міжмережеві екрани є важливим елементом будь-якої системи мережевої безпеки завдяки своїй гнучкості, масштабованості та ефективності. Вони дозволяють контролювати доступ до мережі, забезпечують сегментацію трафіку та можуть використовуватись як частина комплексної стратегії захисту. У даній роботі особливу увагу буде приділено міжмережевим екранам, їхньому аналізу та вибору оптимальних рішень для побудови ефективної системи мережевої безпеки [2].

В даній роботі буде проведено аналіз прийняття рішень в умовах невизначеності, для мінімізації ризиків і допомоги у прийнятті оптимальних рішень, використовуються різні методи аналізу рішень, які будуть продемонстровані і докладно оглянуто в ході роботи.

Методика вибору засобів побудови системи мережевої безпеки, яку буде розроблено в цій роботі, передбачає не лише врахування особливостей кожного з елементів захисту, але й фокусуватиметься на інтеграції міжмережевого екрану як ключового компонента для захисту мережі від зовнішніх і внутрішніх загроз.

Розробка ефективної методики вибору засобів побудови системи мережевої безпеки є актуальним завданням, яке вимагає комплексного підходу. Міжмережевий екран є одним з ключових компонентів такої системи і його вибір повинен здійснюватися з урахуванням специфічних потреб організації.

1 АНАЛІЗ ВИМОГ ДО ЗАСОБІВ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1 Сучасні виклики мережевої безпеки

Сучасний світ інформаційних технологій характеризується стрімким зростанням обсягів інформації, що передається, збільшенням кількості пристроїв, підключених до мережі, та активним розвитком цифрових інфраструктур. Це створює нові виклики у сфері мережевої безпеки. З одного боку, підприємства, державні установи та окремі користувачі все більше залежать від безперебійної роботи мережевих систем. З іншого боку, кібератаки стають все більш витонченими, а загрози все більш різноманітними і небезпечними [3].

Зростання кіберзлочинності, такої як фішингові атаки, соціальна інженерія, атаки типу «відмова в обслуговуванні» (DDoS) та кібершпигунство, призвело до постійного підвищення вимог до мережевої безпеки. Багато організацій стикаються з необхідністю захищати не лише свої внутрішні мережі, але й мобільні пристрої, хмарні сервіси та віддалених працівників.

Основними цілями мережевої безпеки є конфіденційність, цілісність і доступність даних. Для задоволення сучасних потреб необхідно застосовувати комплексний підхід, який включає використання різних технологій, таких як шифрування, аутентифікація, контроль доступу, міжмережеві екрани, системи виявлення і запобігання вторгнень і антивірусне програмне забезпечення [4].

Сьогодні мережеві системи є основою підприємств, державних установ та індивідуальних користувачів. Однак, зі збільшенням їхнього розміру та складності зростають і виклики щодо забезпечення їхньої безпеки.

Кількість кібератак продовжує зростати, а самі атаки стають все більш складними та витонченими. Наприклад, фішингові атаки спрямовані на отримання

конфіденційних даних користувачів за допомогою соціальної інженерії, а атаки на відмову в обслуговуванні (DDoS) виводять з ладу цілі мережеві інфраструктури [5].

Розвиток шкідливого програмного забезпечення, яке еволюціонувало від простих вірусів до більш складних загроз, таких як програми-вимагачі, що блокують доступ до даних користувача і вимагають викуп за їх відновлення.

Зміни в робочому середовищі, такі як збільшення віддаленої роботи і використання мобільних пристроїв, створили необхідність захисту мереж, які містять безліч точок доступу і працюють в різних середовищах.

Зростання використання хмарних сервісів. Хмарні сервіси пропонують значні можливості для зберігання та обробки даних, але також створюють нові загрози безпеці, оскільки дані зберігаються на зовнішніх серверах і можуть бути вразливими до атак [4].

Щоб проаналізувати поточні виклики у сфері мережевої безпеки, візьмемо приклад компанії Colonial Pipeline, яка зазнала масштабної кібератаки у травні 2021 року. Цей інцидент ілюструє поточні ризики для критичної інфраструктури та те, як атака на таку компанію може мати серйозні економічні та соціальні наслідки [5].

Colonial Pipeline є однією з найбільших у США систем транспортування палива, що забезпечує приблизно 45% усіх поставок бензину, дизельного палива та авіаційного пального на східному узбережжі країни.

У травні 2021 року компанія стала жертвою атаки за допомогою програм-вимагачів (ransomware), яка призвела до масштабного відключення роботи трубопроводів.

Основні реалізовані загрози [5]:

- Атака програм-вимагачів (ransomware). Хакерська група DarkSide, яка організувала цю атаку, використала шкідливе програмне забезпечення для шифрування даних Colonial Pipeline. Це спричинило припинення

транспортування палива, оскільки компанія не могла відновити контроль над своїми системами безпеки.

- Компрометація через фішингові атаки. Ймовірною причиною зламу стала фішингова атака або використання вразливих облікових даних, що дало хакерам доступ до внутрішніх систем. Цей приклад вказує на значну загрозу, яку становить соціальна інженерія для великих підприємств.
- Відсутність сегментації критичних систем. Атака зачепила не лише адміністративну частину мережі, але й вплинула на операційні технології (ОТ), які контролюють сам процес транспортування палива. Це показує, що внутрішні системи не були достатньо сегментовані, що дозволило зловмисникам поширювати атаку на критичну інфраструктуру компанії.

Наслідки цієї атаки стали згубними для суспільства, а саме компанія змушена була призупинити свою діяльність майже на тиждень, що призвело до дефіциту палива, підвищення цін і панічних закупів на сході США. Це продемонструвало, наскільки вразливою може бути економіка країни до кібератак на критичну інфраструктуру.

Фінансові втрати та виплата викупу. Colonial Pipeline сплатила хакерам викуп у розмірі 4,4 мільйона доларів у криптовалюті, щоб відновити доступ до своїх даних. Це також вказує на проблеми з управлінням ризиками та стратегіями реагування на інциденти.

Широкий суспільний резонанс. Інцидент привернув увагу як громадськості, так і уряду США, що підсилило необхідність запровадження жорсткіших заходів кібербезпеки на державному рівні для захисту критичної інфраструктури. На рисунку 1.1 зображено масштаб інциденту з Colonial Pipeline.

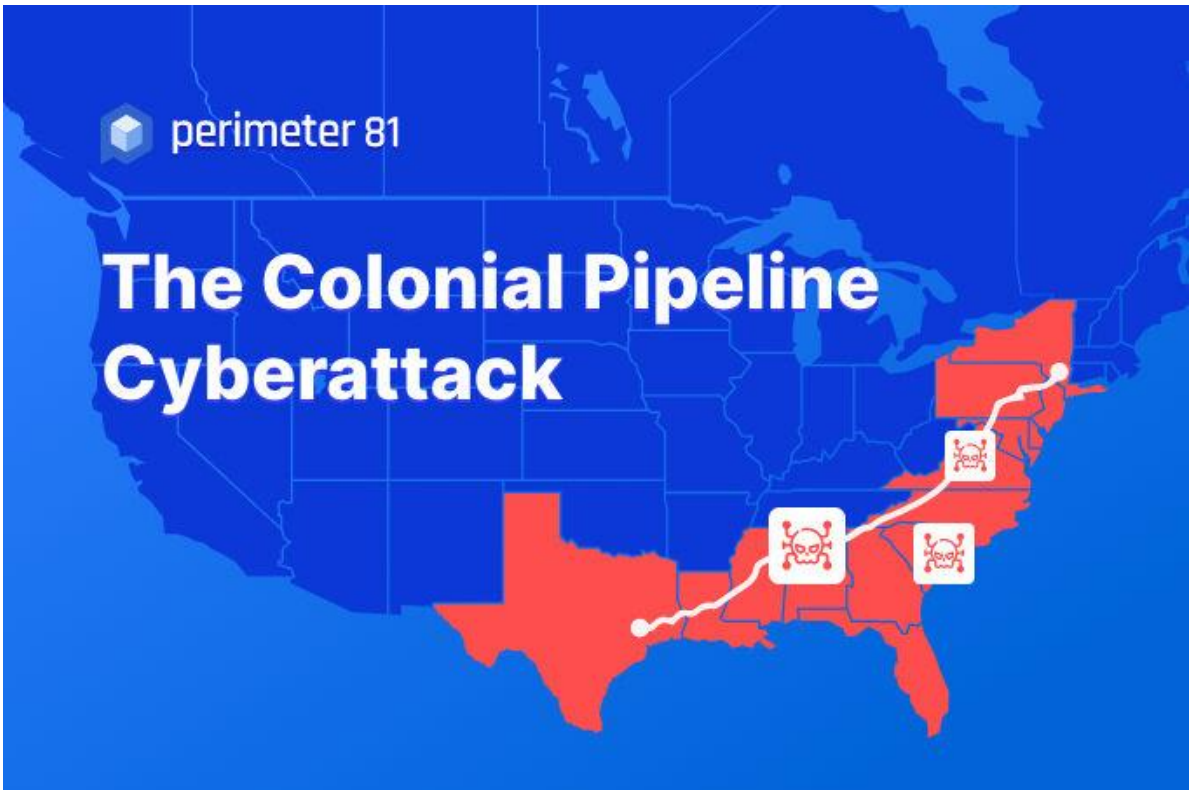

Рисунок 1.1 — Кібератака на систему транспортування палива США 2021 року.

Colonial Pipeline стала жертвою одного з найсучасніших типів кібератак — програм-вимагачів, які часто використовуються проти великих підприємств.

Цей інцидент вказує на важливість захисту не лише інформаційних технологій, а й операційних систем, які контролюють критичні процеси в компаніях.

Україна є яскравим прикладом країни, яка протягом останніх років зіткнулася з численними кібератаками, багато з яких мали політичний підтекст і масштабні наслідки.

Основні виклики [4]:

- Кібертероризм і геополітичні конфлікти. Україна стала мішенню численних кібератак з боку інших держав, особливо в контексті конфлікту з Росією. Одним із найвідоміших прикладів стала атака шкідливим програмним забезпеченням NotPetya у 2017 році, яка паралізувала безліч державних

установ та великих компаній, включаючи банки, транспортні системи та енергетичні компанії.

- Компрометація критичної інфраструктури. Атаки на енергетичні системи України (наприклад, атака на електромережі у 2015 та 2016 , 2022-2024 роках) вказують на наявність значних ризиків для критичних секторів. Ці інциденти показали, наскільки вразливими є енергетичні мережі та інші ключові системи, які можуть бути метою для кібератак.
- Слабкий кіберзахист державних органів. Багато державних установ України довгий час не мали належного рівня кіберзахисту, що дозволяло зловмисникам отримувати доступ до чутливої інформації. Недостатня фінансова підтримка розвитку кібербезпеки на державному рівні ускладнювала вирішення цієї проблеми.
- Недостатня кіберосвіта та кадровий голод. Проблема кіберзахисту ускладнюється браком кваліфікованих фахівців і недостатнім рівнем кіберосвіти. Це стосується як державних органів, так і приватних компаній, що стикаються з труднощами у пошуку професіоналів для захисту своїх мереж.

Наслідки:

- Підрив економіки. Атаки на критичну інфраструктуру, такі як атаки на енергомережі, призводять до фінансових втрат та впливають на життєздатність економіки.
- Загроза національній безпеці. Здатність інших держав проводити кібероперації, які можуть завдати шкоди національній інфраструктурі, становить серйозну загрозу для суверенітету та безпеки країни.
- Реформа кібербезпеки. Після атак Україна почала активно реформувати сферу кібербезпеки, створюючи спеціальні підрозділи для боротьби з кіберзагрозами та підвищуючи рівень кіберграмотності серед державних службовців. Зокрема,

була створена Державна служба спеціального зв'язку та захисту інформації України, яка займається питаннями кіберзахисту.

Одним із найвідоміших випадків кібератаки на критичну інфраструктуру України стала атака на енергетичні компанії, зокрема на "Прикарпаттяобленерго", у грудні 2015 року [6].

Зловмисники, використовуючи троянську програму BlackEnergy, проникли в комп'ютерні мережі кількох енергопостачальних компаній, в тому числі "Прикарпаттяобленерго".

В результаті атаки було вимкнено близько 30 підстанцій, що призвело до відключення електроенергії для близько 230 тисяч споживачів.

Основні наслідки кібератаки [6]:

- Масові відключення електроенергії, тисячі людей залишилися без світла на кілька годин.
- Економічні збитки, атака призвела до значних фінансових втрат для енергетичних компаній та споживачів.
- Порушення роботи критичної інфраструктури, відключення електроенергії могло призвести до серйозних наслідків для інших галузей економіки.
- Підвищення загрози для національної безпеки, атака продемонструвала вразливість критичної інфраструктури України до кібератак.

1.2. Основні загрози мережевій безпеці

Мережева безпека стикається з численними загрозами, які можуть спричинити як значні фінансові втрати, так і компрометацію конфіденційних даних. Сучасні кібератаки стають дедалі складнішими, використовуючи нові техніки для обману систем захисту. У цьому розділі детально розглянемо ключові загрози мережевій безпеці, які залишаються найбільш поширеними та небезпечними для будь-якої організації [7].

1) Атаки на конфіденційність.

Конфіденційність даних — це одна з основних послуг інформаційної безпеки, що передбачає захист від несанкціонованого доступу до приватної або корпоративної інформації [8].

Перехоплення трафіку (маніпуляції посередника, "Man-in-the-Middle" атаки). Цей тип атаки полягає у втручанні зловмисника в комунікаційний канал між двома сторонами, що дозволяє йому отримати доступ до даних, які передаються через мережу, без відома сторін.

Зловмисник може переглядати, підробляти або викрадати конфіденційні дані, зокрема паролі, номери кредитних карток, приватні листування тощо.

Фішинг — це один з найпоширеніших видів соціальної інженерії, при якому зловмисники використовують підроблені веб-сайти, електронні листи або повідомлення для того, щоб обманом змусити користувачів надати конфіденційну інформацію [8].

Шкідливе програмне забезпечення для збору даних. Деякі види шкідливого ПЗ призначені для викрадення даних користувачів, таких як keylogger (програми для запису натискань клавіш) або spyware (програмне забезпечення для шпигунства), яке слідкує за активністю користувачів на їхніх пристроях і передає інформацію зловмисникам.

Успішна атака на конфіденційність може мати серйозні наслідки. Витік даних може спричинити фінансові втрати, зниження репутації, юридичні наслідки, а також втрату довіри з боку клієнтів і партнерів.

2) DDoS-атаки.

Атаки типу "відмова в обслуговуванні" (Denial of Service, DoS) і, зокрема, їхня розширена форма — DDoS-атаки (Distributed Denial of Service) — є одними з найнебезпечніших загроз для мережевих інфраструктур. Суть таких атак полягає в

тому, що зловмисники навмисно перевантажують сервер або інший мережевий ресурс величезною кількістю запитів, внаслідок чого легальні користувачі втрачають можливість отримати доступ до послуг [9].

У DDoS-атаках використовується розподілена мережа з великої кількості заражених пристроїв (ботнет), які одночасно надсилають запити на сервер жертви. Результатом такої атаки може бути:

Недоступність ресурсів. Внаслідок перевантаження серверів користувачі не можуть підключитися до веб-сайту або мережевого ресурсу. Це може мати катастрофічні наслідки для організацій, що надають критично важливі послуги або ведуть бізнес онлайн.

Фінансові збитки. Бізнеси, залежні від постійного доступу до своїх сервісів (наприклад, інтернет-магазини або фінансові установи), зазнають серйозних фінансових втрат через недоступність своїх послуг для клієнтів. Час простою через DDoS-атаку може обчислюватися тисячами або навіть мільйонами доларів.

Порушення роботи внутрішніх систем. DDoS-атаки можуть не лише вивести з ладу веб-сайти, але й паралізувати роботу внутрішніх мережевих систем підприємств, що ускладнює роботу співробітників і негативно впливає на продуктивність.

Захист від DDoS-атак вимагає використання спеціалізованих інструментів для фільтрації трафіку та балансування навантаження, що дозволяє ізолювати шкідливі запити і зберігати доступність послуг для легальних користувачів.

3) Шкідливе програмне забезпечення.

Шкідливе програмне забезпечення є однією з найпоширеніших загроз для мережевої безпеки. Існує кілька типів шкідливих програм, кожен з яких має свої особливості та цілі. Найпоширеніші види шкідливого ПЗ включають:

Віруси здатні поширюватися через мережу або файлові системи, заражаючи інші комп'ютери та програми. Хробаки, на відміну від вірусів, можуть поширюватися без втручання користувача, автоматично переміщаючись від одного пристрою до іншого [10].

Програми-вимагачі (ransomware). Це шкідливе ПЗ блокує доступ до комп'ютерної системи або даних користувача і вимагає викуп за їх відновлення. Ransomware-атаки останнім часом стали одними з найпоширеніших загроз для організацій, адже після зараження вони швидко блокують критично важливі ресурси та можуть паралізувати діяльність підприємства.

Трояни. Це шкідливе ПЗ, яке маскується під легальне програмне забезпечення. Після завантаження та встановлення троян відкриває зловмисникам прихований доступ до комп'ютера користувача, дозволяючи викрадати дані або виконувати інші дії від імені користувача.

Spyware. Шпигунські програми призначені для непомітного збору інформації про користувачів та їхню активність. Вони можуть відстежувати веб-перегляди, збирати паролі, кредитні картки та інші чутливі дані.

Шкідливе ПЗ часто поширюється через електронну пошту, заражені веб-сайти або підроблені програми. Наслідки зараження можуть бути руйнівними для організацій, оскільки зловмисники можуть викрадати критичну інформацію, завдавати шкоди інфраструктурі або вимагати викуп.

4)Атаки на мережеву інфраструктуру.

Мережева інфраструктура — це основа будь-якої мережі, яка включає в себе маршрутизатори, комутатори, сервери та інші пристрої, що забезпечують обмін даними. Атаки на ці компоненти можуть призвести до масштабних порушень роботи мережі і, відповідно, до порушень у роботі організацій [11]. Основні види атак на мережеву інфраструктуру включають:

Атаки на маршрутизатори і комутатори. Зловмисники можуть спробувати захопити контроль над маршрутизаторами і комутаторами для перенаправлення трафіку через свої системи або для відмови у обслуговуванні певних сегментів мережі.

Використання вразливостей протоколів. Протоколи, такі як TCP/IP або DNS, можуть містити вразливості, які дозволяють зловмисникам перехоплювати або змінювати трафік, що проходить через мережу.

Сервери є критичними елементами мережі, що зберігають і обробляють великі обсяги даних. Атаки на сервери можуть включати спроби отримати несанкціонований доступ до баз даних, підробку даних, або встановлення шкідливого ПЗ, яке дає змогу зловмисникам контролювати сервер віддалено.

Такі атаки можуть призвести до втрати даних, порушення роботи послуг або крадіжки конфіденційної інформації.

5) Соціальна інженерія.

Соціальна інженерія є однією з найбільш підступних і складних для запобігання загроз, оскільки вона спрямована не стільки на вразливості в системах, скільки на людський фактор. Зловмисники використовують методи обману для того, щоб змусити користувачів розкрити свої облікові дані або іншу конфіденційну інформацію. До найбільш поширених видів соціальної інженерії належать [12]:

- Фішингові атаки, які полягають у використанні підроблених електронних листів або веб-сайтів, які намагаються ввести користувача в оману і змусити його ввести свої особисті дані або паролі.
- Spear-phishing. Це більш цілеспрямована форма фішингу, при якій атаки націлені на конкретних осіб або організації.
- Різновиди фішингу, які використовують голосові дзвінки (вішинг) або текстові повідомлення (смішинг) для спроб обману користувачів.

Атаки соціальної інженерії важко виявити, оскільки вони використовують психологічні методи обману. Основним захистом від таких атак є навчання користувачів і підвищення обізнаності про можливі загрози, а також використання додаткових методів аутентифікації.

1.3 Основні методи та інструменти забезпечення мережевої безпеки

У відповідь на численні загрози, які постійно еволюціонують, індустрія мережевої безпеки пропонує широкий спектр рішень для захисту інфраструктури. Кожне з них орієнтоване на різні аспекти захисту, від запобігання вторгненням і фільтрації шкідливого трафіку до моніторингу мережевої активності та управління доступом. Важливо розуміти, що мережеву безпеку не можна забезпечити лише одним інструментом або методом, тому комплексний підхід є основою ефективного захисту [13]. У цьому розділі розглянемо сучасні рішення, які використовуються для забезпечення надійної мережевої безпеки.

1.3.1 Міжмережеві екрани

Міжмережеві екрани залишаються одним із найстаріших, але водночас найбільш ефективних засобів захисту мережевих систем. Основна функція міжмережевого екрану полягає у фільтрації вхідного та вихідного трафіку на основі встановлених правил. Міжмережевий екран може блокувати або дозволяти трафік залежно від його походження, призначення або типу, що дозволяє захищати внутрішню мережу від зовнішніх загроз [14].

Існує кілька видів міжмережевих екранів:

- Традиційні мережеві екрани.

Це найпростіші міжмережеві екрани, які здійснюють фільтрацію трафіку на основі IP-адрес, портів і протоколів. Вони є основою будь-якої системи безпеки, але мають обмежені можливості, оскільки не здатні аналізувати вміст самих пакетів даних, що робить їх менш ефективними проти складних загроз.

- Міжмережеві екрани наступного покоління (NGFW, Next-Generation Firewall).

Це більш досконалі рішення, які поєднують у собі функціонал традиційних міжмережевих екранів і додаткові можливості, такі як глибокий аналіз пакетів (DPI), інтеграція з системами виявлення вторгнень (IDS/IPS), а також здатність ідентифікувати та блокувати шкідливий трафік на рівні додатків. NGFW здатні виявляти більш складні загрози, такі як атаки на прикладному рівні або шкідливі програми, які маскуються під легальний трафік.

- Хмарні міжмережеві екрани.

З розвитком хмарних технологій, багато компаній переходять до використання хмарних рішень для міжмережевих екранів. Такі системи забезпечують фільтрацію та моніторинг трафіку між хмарними сервісами та внутрішньою мережею організації.

Хмарні міжмережеві екрани часто інтегруються з іншими хмарними рішеннями для безпеки, що дозволяє централізовано управляти захистом в багатохмарних середовищах.

Міжмережеві екрани грають ключову роль в захисті мережевих систем, оскільки дозволяють запобігати несанкціонованому доступу до внутрішніх ресурсів. Проте, вони повинні бути належним чином налаштовані та оновлені для забезпечення максимальної ефективності, адже хибна конфігурація може стати вразливістю для зловмисників.

1.3.2 Системи виявлення та запобігання вторгнень (IDS/IPS)

Системи виявлення вторгнень (IDS) і запобігання вторгнень (IPS) призначені для виявлення підозрілої активності в мережі та відповідного реагування на потенційні загрози. IDS є пасивною системою, яка лише виявляє та сповіщає про аномалії, тоді як IPS може активно блокувати або ізолювати підозрілий трафік [15].

IDS (Intrusion Detection System) аналізує мережевий трафік і порівнює його з відомими шаблонами атак або аномальною поведінкою. Якщо виявляється аномалія, система генерує сповіщення для адміністраторів безпеки, щоб ті могли оперативно відреагувати на потенційну загрозу. IDS не втручається у сам трафік, що робить його підходящим для моніторингу, але недостатньо ефективним для активного захисту.

IPS (Intrusion Prevention System) працює в режимі реального часу і може не лише виявляти, але й блокувати підозрілу активність. IPS інтегрується з іншими рішеннями для безпеки і може миттєво реагувати на атаки, що робить його одним з найбільш ефективних засобів захисту від загроз, таких як DDoS-атаки або шкідливе ПЗ.

IDS/IPS-системи є критичними компонентами сучасної мережевої безпеки, оскільки вони дозволяють оперативно виявляти та запобігати вторгненням. Водночас для їхньої ефективності необхідне постійне оновлення бази сигнатур і шаблонів загроз, а також ретельний моніторинг мережевої активності.

1.3.3 VPN (Віртуальні приватні мережі)

VPN забезпечує шифрування трафіку між користувачами та організаційними ресурсами, що дозволяє захистити дані від перехоплення під час їхньої передачі через інтернет або інші загальнодоступні мережі [16].

Особливо актуально використання VPN стало під час збільшення кількості віддалених співробітників, які потребують безпечного доступу до корпоративних систем.

Використання VPN дозволяє [16]:

- Шифрувати трафік. VPN забезпечує захист конфіденційності даних, переданих між користувачем і сервером, використовуючи протоколи шифрування, такі як IPsec або TLS.

- Захищати від атак "людина посередині" (Man-in-the-Middle). Оскільки весь трафік зашифрований, зловмисники, навіть маючи доступ до каналу передачі даних, не можуть прочитати або змінити інформацію, що передається через VPN.
- Забезпечувати доступ до внутрішніх ресурсів. VPN дозволяє співробітникам організацій безпечно підключатися до внутрішніх мереж і отримувати доступ до критичних ресурсів, навіть якщо вони працюють за межами офісу.

Хоча VPN є ефективним засобом захисту даних, важливо належним чином його налаштувати та використовувати надійні протоколи шифрування для захисту від потенційних атак.

1.3.4 Антивірусне програмне забезпечення

Антивірусне програмне забезпечення є одним з основних інструментів для захисту кінцевих точок (комп'ютерів, серверів) від шкідливого ПЗ.

Основна мета антивірусів полягає в тому, щоб виявляти, блокувати та видаляти шкідливе програмне забезпечення, таке як віруси, трояни, хробаки та програми-вимагачі [17].

Сучасні антивірусні програми використовують такі підходи до захисту:

- Сигнатурний аналіз, при якому антивірусні програми порівнюють файли та процеси на комп'ютері з базою даних відомих шкідливих програм.
- Аналіз поведінки. Антивірусні програми, що використовують цей підхід, спостерігають за тим, як поводяться програми та файли на комп'ютері.
- Деякі антивірусні системи використовують хмарні сервіси для аналізу нових загроз у режимі реального часу.

Антивірусне програмне забезпечення забезпечує базовий захист від відомих загроз, але його ефективність залежить від регулярного оновлення бази даних шкідливих програм і його здатності аналізувати нові загрози в режимі реального

часу. В сучасних умовах використання антивірусів має доповнюватися іншими рішеннями для забезпечення більш комплексного захисту.

1.3.5 Управління ідентифікацією та доступом (IAM)

Системи управління ідентифікацією та доступом (Identity and Access Management, IAM) дозволяють контролювати, які користувачі мають доступ до певних ресурсів у мережі. Використовуючи IAM, організації можуть забезпечити, щоб тільки уповноважені користувачі мали доступ до конфіденційної інформації або критичних систем [18].

IAM-системи можуть використовувати різні методи аутентифікації, включаючи багатофакторну аутентифікацію (MFA), де, крім пароля, користувач повинен ввести додатковий код або підтвердити свою особу за допомогою біометрії.

Після успішної аутентифікації система IAM визначає, до яких ресурсів користувач має доступ. Це дозволяє чітко контролювати права доступу кожного співробітника або групи користувачів у межах організації.

1.4 Актуальні тенденції у розвитку технологій мережевої безпеки

З розвитком технологій та збільшенням масштабів кіберзагроз, мережеві рішення мають постійно вдосконалюватися. Сучасні тенденції у сфері мережевої безпеки зосереджені на інноваціях, які дозволяють не тільки захищати системи від загроз, але й ефективно реагувати на інциденти, передбачати потенційні атаки, інтегрувати захист у хмарні платформи та використовувати штучний інтелект для покращення безпеки [19].

Аналіз найактуальніших напрямків у розвитку технологій мережевої безпеки:

1) Штучний інтелект та машинне навчання

Штучний інтелект та машинне навчання стають ключовими інструментами у боротьбі з кіберзагрозами.

Ці технології дозволяють значно підвищити ефективність захисту завдяки автоматизації процесів виявлення загроз і реагування на них.

Системи штучного інтелекту здатні обробляти величезні обсяги мережевих даних у реальному часі, шукаючи аномалії, які можуть свідчити про вторгнення. Машинне навчання дозволяє системам вивчати нормальну поведінку мережі та автоматично ідентифікувати відхилення, навіть якщо вони ще не були задокументовані як відомі атаки [20].

Штучний інтелект дозволяє створювати системи, які можуть автоматично блокувати підозрілий трафік або ізолювати заражені вузли, зменшуючи час реакції та мінімізуючи шкоду від атаки.

Розвиток технологій штучного інтелекту та машинного навчання дає змогу зменшити навантаження на IT-відділи, автоматизувати багато рутинних процесів і забезпечити швидшу реакцію на нові та складніші загрози.

2) Модель Zero Trust

Також розглянемо технологію моделі нульової довіри (Zero Trust) — це концепція, яка радикально змінює підхід до мережевої безпеки. Вона базується на принципі, що нікому не можна довіряти, навіть якщо користувач знаходиться всередині корпоративної мережі. Замість того, щоб захищати лише периметр мережі, модель Zero Trust передбачає постійну верифікацію кожного запиту до ресурсів [21].

Модель Zero Trust вимагає перевірки кожного запиту незалежно від того, чи це запит від зовнішнього користувача, чи від внутрішнього співробітника. Користувачі повинні постійно підтверджувати свою особу, що знижує ризики, пов'язані з компрометацією облікових даних.

Система Zero Trust дозволяє оцінювати контекст запиту, включаючи геолокацію, тип пристрою, час доступу тощо, для визначення того, чи є запит

безпечним. Це знижує ризик несанкціонованого доступу навіть у разі викрадених паролів.

3) Хмарні технології

З огляду на стрімке зростання використання хмарних технологій, організації все частіше переходять до інтеграції систем безпеки у хмарні середовища. Це дозволяє компаніям ефективніше управляти ресурсами, масштабувати захист і забезпечувати безпеку в будь-який час та з будь-якої локації [22].

Хмарні міжмережеві екрани та безпека як послуга (Security as a Service, SaaS). Багато постачальників хмарних сервісів пропонують інтегровані рішення для безпеки, які включають міжмережеві екрани, системи виявлення загроз та антивірусні програми. Це дозволяє компаніям зменшити навантаження на внутрішні команди безпеки та скоротити витрати на підтримку власної інфраструктури безпеки.

Важливим аспектом хмарної безпеки є захист даних за допомогою шифрування. Нові методи, такі як гомоморфне шифрування, дозволяють виконувати обчислення з зашифрованими даними без необхідності їхнього розшифрування, що мінімізує ризики витоків даних.

4) Інтернет речей (IoT)

Потрібно зазначити, що з розвитком Інтернету речей (IoT) кількість підключених до мережі пристроїв зросла до мільярдів, що створило нові виклики для безпеки. IoT-пристрої зазвичай мають обмежені ресурси і слабкі вбудовані засоби захисту, що робить їх вразливими для кібератак [23].

Одним з найбільш ефективних методів захисту IoT-пристроїв є сегментація мережі. Цей підхід дозволяє ізолювати IoT-пристрої від критичних корпоративних ресурсів, що мінімізує ризики у разі компрометації цих пристроїв.

Використання безпечних методів аутентифікації та шифрування між IoT-пристроями та центральними серверами є ключовим для захисту мережі.

1.5 Постановка задач досліджень

Тенденції у розвитку технологій мережевої безпеки демонструють спрямованість на підвищення автоматизації, використання інтелектуальних систем і впровадження нових моделей, таких як Zero Trust та хмарні рішення. Штучний інтелект, машинне навчання, хмарні платформи, захист IoT та автоматизація процесів дозволяють організаціям ефективніше боротися з сучасними загрозами та забезпечити безперервний захист навіть в умовах стрімкого розвитку кіберзагроз.

Для подальшого огляду та розробки методики вибору засобів побудови системи мережевої безпеки вирішено зосередитися на міжмережевому екрані як основному компоненті захисту. Міжмережеві екрани відіграють ключову роль у забезпеченні безпеки мереж, виконуючи функції контролю та фільтрації мережевого трафіку. Їх завдання полягає в тому, щоб блокувати несанкціоновані спроби доступу до внутрішніх ресурсів компанії та захищати систему від загроз, що виникають як із зовнішніх, так і з внутрішніх джерел.

Вибір міжмережевого екрану обґрунтований його важливістю для забезпечення першої лінії захисту, контролю доступу до внутрішньої мережі та можливістю гнучкого налаштування залежно від потреб організації. Саме тому цей інструмент стане центральним елементом для розробки методики вибору засобів мережевої безпеки. Він також забезпечує широку інтеграцію з іншими рішеннями безпеки, що дозволить створити багаторівневу систему захисту з врахуванням сучасних вимог і загроз.

Основними задачами є детальний огляд технології міжмережевого екрану, обширний аналіз методів прийняття рішень в умовах невизначеності, розробка власної методики вибору засобів міжмережевої безпеки, також автоматизація створеної методики програмно з подальшим тестуванням створеного рішення.

2 ТЕХНОЛОГІЇ ПОБУДОВИ МІЖМЕРЕЖЕВИХ ЕКРАНІВ

2.1 Основні типи міжмережевих екранів та їх функції

Міжмережеві екрани є основними інструментами захисту комп'ютерних мереж від несанкціонованого доступу. Їхня роль полягає у фільтрації трафіку, моніторингу та блокуванні потенційних загроз на основі певних правил. Існує кілька основних типів міжмережевих екранів, кожен з яких має свої особливості [24].

2.1.1 Пакетні фільтри

Цей тип МЕ аналізує окремі пакети даних, які надходять у мережу, і приймає рішення про їх пропуск або блокування на основі інформації, що міститься в заголовках пакетів (IP-адреси, порти, протокол) [25]. Основні функції:

- Базуються на правилах, що визначають, дозвіл передавати пакети.
- Працюють швидко, оскільки аналізують лише заголовки пакетів.
- Не забезпечують повного захисту,не можуть аналізувати вміст самих пакетів.
- Не можуть захищати від атак на рівні прикладного протоколу.

На рисунку 2.1 зображено принцип роботи даного типу міжмережевого екрану.

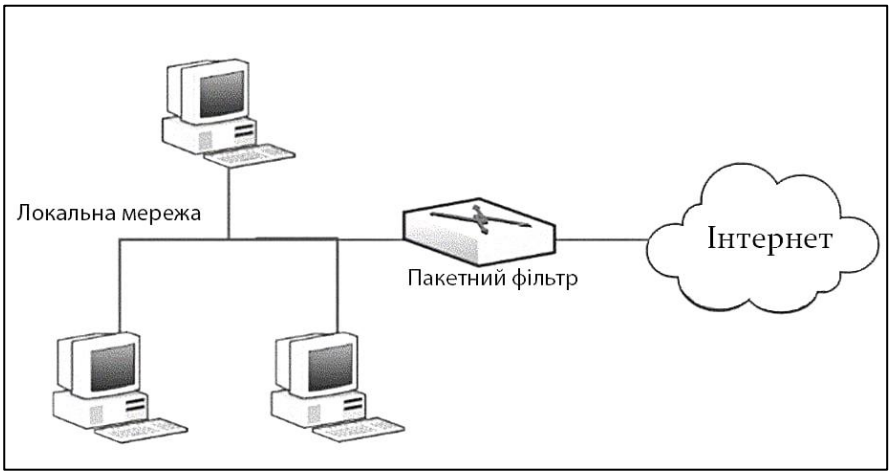

Рисунок 2.1 – Принцип роботи пакетного фільтру

Перевагами є висока продуктивність завдяки мінімальному аналізу та легка реалізація та налаштування.

Недоліками є обмежений рівень безпеки, оскільки не враховує контекст сесії чи додаткову інформацію про стан з'єднання.

2.1.2 Шлюзи прикладного рівня

Цей тип працює на рівні додатків (рівень 7 моделі OSI). Він виступає посередником між клієнтом і сервером, пропускаючи або блокуючи трафік залежно від його змісту. На відміну від пакетних фільтрів, шлюзи аналізують вміст пакетів і взаємодію на рівні конкретних додатків, таких як HTTP, FTP, SMTP [26].

Функції:

- Перевіряють трафік на основі змісту (payload), що дозволяє виявляти атаки, засновані на помилках додатків.
- Можуть виконувати більш складний аналіз, наприклад, розшифровувати шифровані з'єднання для аналізу.

На рисунку 2.2 зображено схему роботи Проксі-серверу.

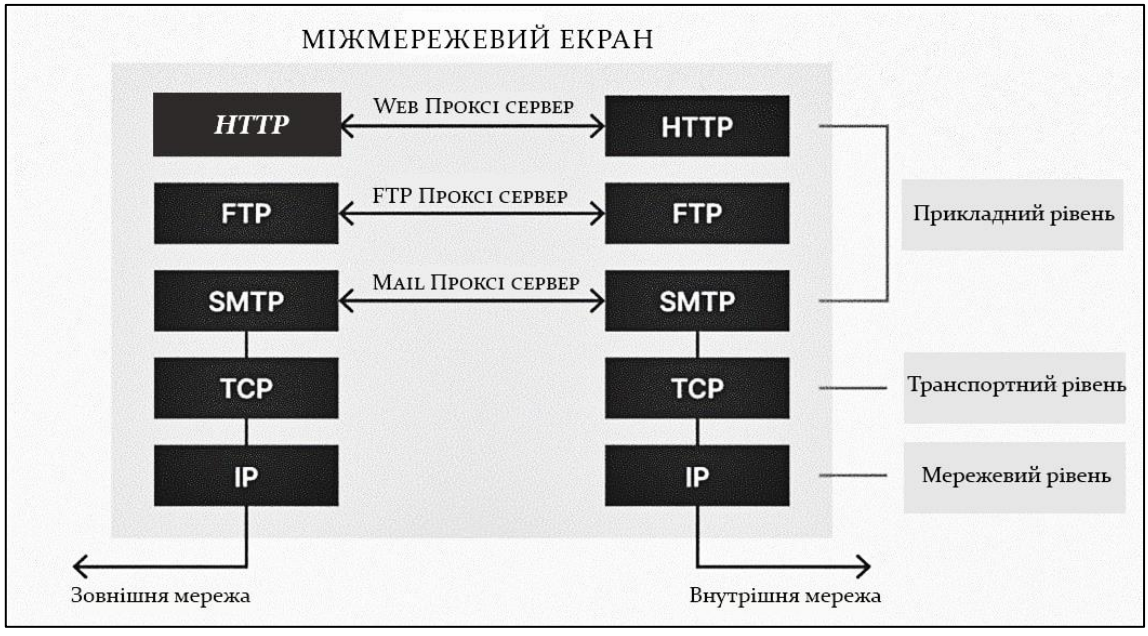

Рисунок 2.2 - Проксі-сервер

Перевагами буде підвищений рівень безпеки завдяки глибшому аналізу трафіку, а також можливість блокування небезпечного вмісту або несанкціонованих операцій на рівні додатків.

Недоліками є зниження продуктивності через потребу в детальному аналізі трафіку, такий тип вимагає більше ресурсів для роботи.

2.1.3 Шлюзи з фільтрацією на рівні сесій

Цей тип міжмережевих екранів контролює стан сесій. Вони працюють на мережевому та транспортному рівнях (рівень 3 та 4 OSI), відстежуючи повну сесію з'єднання, а не лише окремі пакети [27]. Функції:

- Відстежують стан кожного з'єднання (ініціація, активність, завершення).
- Зберігають інформацію про стан сесій і використовують її для прийняття рішень щодо трафіку.
- Дозволяють трафік, що є частиною відомих сесій, блокуючи все, що виглядає підозріло.

Принцип роботи міжмережевого екрану іспекції стану пакета зображено на рисунку 2.3.

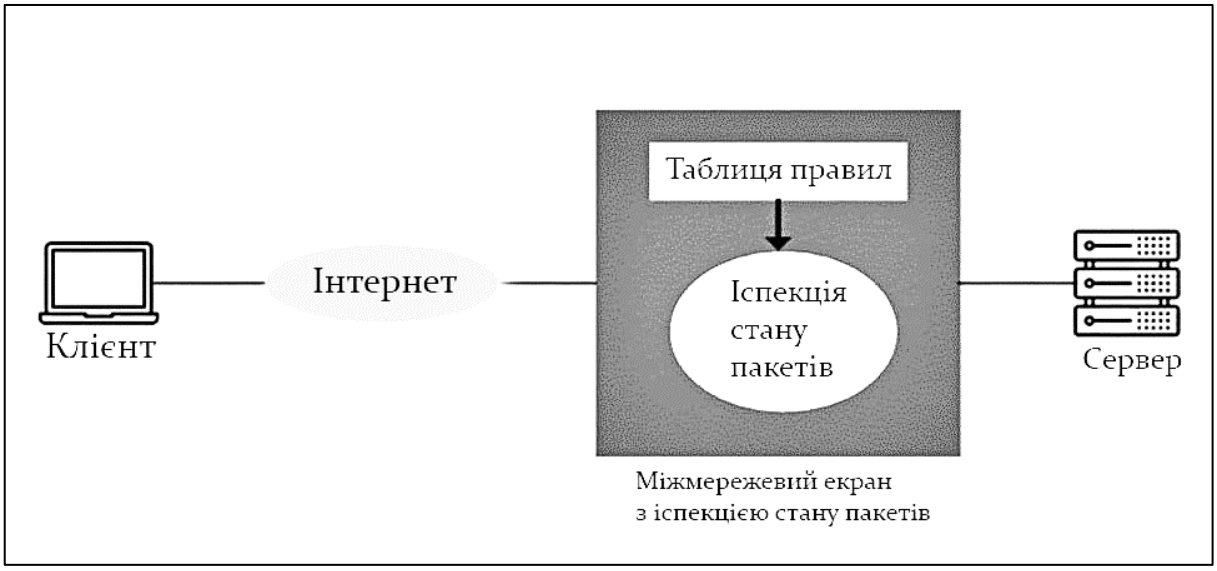

Рисунок 2.3 - МЕ інспекції стану пакета

Перевагами буде більш ефективна фільтрація завдяки знанню контексту сесії. Підтримка динамічних протоколів, які використовують випадкові порти.

Недоліком є ускладнення налаштування через необхідність вказувати складні правила.

2.1.4 Міжмережеві екрани нового покоління

Це сучасний тип міжмережевих екранів, що комбінує традиційні методи фільтрації трафіку з інтелектуальними механізмами виявлення загроз.

Основні це аналіз поведінки, інтеграція з системами виявлення вторгнень (IDS), а також глибока перевірка пакетів (DPI) [28].

Функції:

- Виявлення загроз на основі поведінкових моделей.
- Інтеграція з іншими системами кібербезпеки, такими як системи запобігання вторгнень (IPS).
- Можуть включати антивірусний захист, блокування шпигунського ПЗ та фільтрацію веб-контенту.

Перевагами є комплексний захист з використанням декількох методів одночасно, підтримка сучасних кіберзагроз та атак.

Недоліками є висока вартість впровадження та обслуговування, вимоги до апаратних ресурсів для підтримки високої пропускної здатності.

Кожен тип міжмережевого екрану має свої сильні та слабкі сторони, і вибір відповідного рішення залежить від конкретних потреб організації [29].

Пакетні фільтри підходять для простих мереж з мінімальними вимогами до безпеки, в той час як шлюзи прикладного рівня або NGFW забезпечують високий рівень захисту для складних мереж.

2.2 Огляд засобів реалізації міжмережевих екранів

Міжмережеві екрани можуть бути реалізовані різними способами, залежно від типу інфраструктури, потреб безпеки та використовуваних технологій. Деякі з найпопулярніших реалізацій міжмережевих екранів включають програмні рішення, апаратні пристрої та гібридні підходи [30]. Ось основні приклади:

2.2.1 Iptables

Популярний інструмент iptables у системах Linux для налаштування правил міжмережевого екрану. Він працює на основі пакетних фільтрів і забезпечує контроль за вхідним, вихідним та переспрямованим трафіком на мережевому (рівень 3) і транспортному рівнях (рівень 4) моделі OSI [31].

Особливості:

- Використовує таблиці, ланцюжки та правила для фільтрації та маніпулювання трафіком.
- Підтримує різні дії для пакетів: приймати, відхиляти, скидати.
- Можливе налаштування NAT (перетворення мережевих адрес) для маршрутизації.
- Використовується у більшості дистрибутивів Linux для забезпечення базового рівня безпеки.

Даний засіб є гнучким у налаштуванні, безкоштовним і відкритим програмним забезпеченням та має широкі можливості для скриптів автоматизації.

2.2.2 Packet Filter

Утиліта pf — це інший потужний інструмент для фільтрації пакетів, який спочатку був розроблений для OpenBSD, але також використовується в FreeBSD і macOS. Він працює на рівнях 3 та 4 OSI і виконує роль міжмережевого екрану за принципом пакетної фільтрації [32].

Особливості:

- Підтримка NAT, контроль за станом з'єднань і фільтрація трафіку.
- Широкий набір функцій для шифрування та фрагментації.
- Забезпечує управління смугою пропускання (QoS) для контролю використання ресурсів мережі.

Засіб простий у налаштуванні і має потужний синтаксис правил, підтримує функцію журналювання та моніторингу, але поширений переважно в Unix-подібних системах.

2.2.3 Firewalld

Firewalld — це сучасний демон міжмережевого екрану для Linux, який забезпечує динамічне управління правилами, підтримує зони безпеки та дозволяє змінювати конфігурацію міжмережевого екрану без перезавантаження системи [33].

Особливості:

- Зони безпеки дозволяють застосовувати різні правила для різних мережевих інтерфейсів або підмереж.
- Підтримка IPv4, IPv6, NAT і маршрутизації.
- Інтуїтивний інтерфейс для керування за допомогою командного рядка або графічної оболонки.

Даний засіб легкий у керуванні з підтримкою динамічних змін та підходить для роботи з великими мережами. Однам має недолік в обмеженій гнучкості у порівнянні з iptables.

2.2.4 Uncomplicated Firewall

UFW — це спрощений інтерфейс для управління iptables, орієнтований на користувачів, які хочуть простіше налаштувати міжмережевий екран у Linux-системах [34].

Особливості:

- Простий синтаксис для створення правил дозволу або заборони трафіку.
- Легке налаштування політик для вхідного та вихідного трафіку.
- Підтримка IPv4, IPv6 і NAT.

Простіший у використанні, ніж iptables, має швидке налаштування базової безпеки. Із недоліків менша гнучкість для складних налаштувань.

2.2.5 Cisco Adaptive Security Appliance

Cisco ASA — це апаратне рішення від Cisco, яке поєднує функції міжмережевого екрану, VPN-шлюзу, системи виявлення вторгнень (IDS), а також інших можливостей мережевої безпеки. Це апаратний міжмережевий екран, який виконує функції пакетної фільтрації, контролю стану з'єднань, і глибокого аналізу пакетів (DPI) [35].

Особливості:

- Підтримка VPN, NAT і віддаленого доступу.
- Інтеграція з системами виявлення та запобігання вторгнень (IDS/IPS).
- Можливість розширеної фільтрації трафіку і глибокого аналізу пакетів.

Засіб має високий рівень безпеки з використанням сучасних технологій захисту з можливість управління великими мережами, але недоліком є висока вартість обладнання та ліцензування.

Існує безліч різних способів реалізації міжмережевих екранів, від простих програмних рішень, таких як iptables і UFW, до потужних апаратних рішень від Cisco та Fortinet. Вибір залежить від конкретних потреб організації, рівня безпеки, продуктивності та вартості впровадження. Програмні рішення зазвичай використовуються в малих і середніх мережах, тоді як великі підприємства часто звертаються до апаратних рішень з вищим рівнем інтеграції безпеки.

2.3 Проблемні питання вибору міжмережевого екрану

Вибір міжмережевого екрану є важливим рішенням для будь-якої організації, оскільки він забезпечує першу лінію захисту мережі. Однак існує кілька проблемних аспектів, які виникають при виборі відповідного рішення.

Ці питання стосуються як технічних характеристик, так і економічних факторів, а також специфічних вимог конкретної мережі [36]. Розгляну основні питання при виборі міжмережевого екрану:

1) Визначення потреб організації.

Великі підприємства з багатошаровою мережею потребують потужних рішень із глибокою перевіркою пакетів і контролем стану з'єднань. Для невеликих організацій достатньо базових рішень, таких як пакетні фільтри або шлюзи.

Якщо в мережі активно використовуються певні протоколи або програми, міжмережевий екран повинен мати можливість обробляти їх ефективно. Наприклад, якщо організація працює з шифрованим трафіком TLS [37].

2) Продуктивність і пропускна здатність.

Продуктивність міжмережевого екрану є ключовою проблемою, особливо для великих організацій.

Проблема виникає, коли екран має низьку пропускну здатність і не може обробляти великий обсяг трафіку без затримок. Це може призвести до сповільнення роботи мережі та зниження ефективності роботи бізнесу.

Мережа може зростати, а разом із нею і обсяг трафіку. Міжмережевий екран повинен підтримувати масштабування без втрати продуктивності, що вимагає обирати рішення з резервом потужності або здатністю до горизонтального масштабування (кластеризація).

3) Функціональність та інтеграція.

Деякі організації можуть потребувати фільтрації не лише заголовків пакетів, а й їхнього вмісту. Це особливо важливо для захисту від складних загроз, таких як шкідливе ПЗ або атаки на рівні додатків.

Міжмережевий екран має легко інтегруватися з системами виявлення вторгнень (IDS/IPS), антивірусним ПЗ, VPN, SIEM, і системами керування ідентифікацією (IAM) [38].

Невідповідність міжмережевого екрану з іншими засобами безпеки може ускладнити управління мережею та зробити її вразливою.

4) Управління та зручність використання.

Адміністрування міжмережевого екрану може бути складним завданням, особливо для невеликих організацій із обмеженими ресурсами.

Деякі міжмережеві екрани (наприклад, iptables) можуть бути занадто складними для адміністраторів, які не мають глибоких знань у мережевій безпеці. Простіші інструменти, такі як UFW або інтерфейси користувача, полегшують налаштування [39].

Для великих організацій важливо мати можливість централізовано керувати всіма міжмережевими екранами через єдиний інтерфейс. Якщо міжмережевий екран не підтримує таку функцію, це ускладнює моніторинг і адміністрування.

5) Безпека та можливість оновлень.

Технології безпеки швидко розвиваються, і нові загрози з'являються щодня.

Міжмережевий екран повинен підтримувати регулярні оновлення для виявлення нових загроз і уразливостей [40].

Міжмережевий екран повинен мати чітку підтримку політик безпеки, таких як контроль доступу до мережевих ресурсів, аутентифікація та авторизація користувачів.

6) Вартість та ліцензування.

Ціна є важливим фактором при виборі міжмережевого екрану, особливо для малих та середніх підприємств.

Апаратні рішення зазвичай коштують дорожче, ніж програмні. Проте програмні рішення також можуть мати значні витрати на налаштування, підтримку та управління.

Модель ліцензування. Деякі міжмережеві екрани використовують моделі підписки, де користувачі мають сплачувати щорічні внески за підтримку та доступ до оновлень. Це потрібно врахувати при довгостроковому плануванні бюджету.

7) Юридичні та нормативні вимоги.

Організаціям, що працюють у регульованих галузях (наприклад, фінансові установи або охорона здоров'я), важливо враховувати відповідність нормативам.

Рішення повинне відповідати таким стандартам, як GDPR, HIPAA, PCI DSS або ISO 27001, якщо це вимагається законодавством або політикою організації [41].

8) Підтримка мобільних та віддалених користувачів.

З поширенням віддаленої роботи та мобільних пристроїв важливо, щоб міжмережевий екран підтримував роботу з такими користувачами:

Організація повинна забезпечити безпечне підключення віддалених співробітників через VPN. Міжмережевий екран повинен мати можливість інтеграції з VPN-рішеннями або підтримувати вбудовані функції VPN [42].

Підтримка політики BYOD (Bring Your Own Device) вимагає ретельного контролю доступу мобільних пристроїв до корпоративних ресурсів, що також повинно враховуватися при виборі міжмережевого екрану [43].

3 МЕТОДИ ПРИЙНЯТТЯ РІШЕНЬ В УМОВАХ НЕВИЗНАЧЕНОСТІ

3.1 Огляд поширених методів прийняття рішень в умовах невизначеності

Аналіз прийняття рішень в умовах невизначеності — це процес вибору оптимального варіанту дії або рішення за наявності неповної, неоднозначної або суперечливої інформації. У контексті вибору міжмережевого екрану, це може бути особливо важливо, оскільки рішення про те, який інструмент безпеки використовувати, може залежати від безлічі факторів, не всі з яких є точно визначеними на момент прийняття рішення [44].

Невизначеність щодо майбутніх загроз, оскільки загрози безпеці постійно еволюціонують, не можна точно передбачити, які загрози стануть актуальними в майбутньому. Це робить складним вибір міжмережевого екрану, який здатен забезпечити довготривалий захист.

Невизначеність щодо потреб мережі. Наприклад, компанія може не знати точно, яким буде обсяг трафіку через кілька років або які нові сервіси з'являться, що вимагатимуть додаткових функцій безпеки. Це ускладнює прогнозування необхідної пропускної здатності або потреби в додаткових функціях, таких як глибока перевірка пакетів (DPI) або інтеграція з іншими системами безпеки.

Обмежена інформація щодо ефективності рішень. Часто при виборі міжмережевого екрану організація стикається з недостатньою кількістю інформації про реальну продуктивність або надійність рішення в їхньому середовищі. Тестування не завжди відображає реальні умови експлуатації, що також вносить елемент невизначеності.

У практиці існує декілька підходів до вирішення таких задач:

- Метод максиміну (Minimax). Цей підхід передбачає вибір альтернативи, яка мінімізує максимальні можливі втрати. Його часто використовують у випадках, коли рішення пов'язане з великими ризиками.
- Метод максимаксу (Maximax). На відміну від максиміну, максимакс орієнтований на вибір альтернативи, яка може дати максимальний виграш. Цей метод підходить для ситуацій, коли ризик прийнятний, і є потенціал для значних вигод.
- Метод очікуваної корисності (Expected Utility Method). В цьому підході використовується ймовірнісний аналіз, щоб знайти рішення, яке максимізує очікувану корисність. Цей метод підходить для ситуацій, де можна оцінити ймовірність кожного результату.
- Метод нечіткої логіки (Fuzzy Logic Method). Цей підхід застосовується, коли інформація про критерії або альтернативи є нечіткою або неповною. Нечітка логіка дозволяє враховувати невизначеність у вихідних даних.
- Метод аналізу чутливості (Sensitivity Analysis). Дозволяє оцінити вплив змін в початкових даних на результат вибору. Цей метод корисний для визначення того, наскільки результат залежить від певних припущень або змін у вагових коефіцієнтах.

Одним з основних напрямів вирішення проблеми вибору в умовах невизначеності є застосування багатокритеріальних методів прийняття рішень. В таких методах кожна альтернатива оцінюється за декількома критеріями, що дозволяє більш комплексно підійти до аналізу і забезпечити більш обґрунтований вибір. Багатокритеріальні методи часто використовують у тих галузях, де рішення повинні враховувати кілька різних аспектів, таких як ефективність, безпека, вартість, масштабованість тощо, далі оглянуто основні з них.

Метод аналізу ієрархій дозволяє структурувати задачу у вигляді ієрархії, де на верхньому рівні знаходиться основна мета, а на нижньому — різні альтернативи. Кожен рівень включає критерії, які впливають на прийняття рішень. AHP також дозволяє оцінити вагові коефіцієнти для кожного критерію, що допомагає визначити їхню важливість для рішення.

Метод вагових коефіцієнтів передбачає визначення ваг для кожного критерію і порівняння альтернатив на основі цих ваг. Важливість кожного критерію визначається за допомогою вагових коефіцієнтів, після чого альтернативи оцінюються і порівнюються.

Методи аналізу ієрархій і вагових коефіцієнтів є двома найбільш розповсюдженими багатокритеріальними методами, які ефективно застосовуються для вирішення проблем у сфері мережевої безпеки, зокрема при виборі міжмережевих екранів. AHP дозволяє структурувати процес прийняття рішень на кількох рівнях і забезпечує глибокий аналіз важливості критеріїв, тоді як метод вагових коефіцієнтів є простішим і швидшим в реалізації, але менш гнучким у складних задачах.

Обидва методи можуть бути успішно використані для прийняття рішень в умовах невизначеності, однак вибір конкретного підходу залежить від складності задачі і доступності інформації для оцінки альтернатив. Далі в роботі будуть оглянуті саме ці два багатокритеріальних методи.

3.2 Метод аналіза ієрархій

Метод аналізу ієрархій (AHP, Analytic Hierarchy Process) – це широко використовувана методика для прийняття рішень у складних багатокритеріальних ситуаціях. Цей метод дозволяє структурувати проблему, що потребує прийняття рішення, на декілька рівнів, аналізувати її за допомогою парних порівнянь і на основі цього отримати раціональне рішення, навіть у випадках, коли частина інформації є невизначеною або суперечливою [45].

Основні етапи методу аналізу ієрархій:

1) Побудова ієрархії проблеми.

Першим етапом AHP є побудова ієрархії критеріїв, яка розбиває проблему на кілька рівнів:

- На верхньому рівні ієрархії знаходиться головна мета – це проблема або рішення, яке потрібно прийняти. Наприклад, для вибору міжмережевого екрану метою буде "Вибір найкращого міжмережевого екрану для компанії".
- На середньому рівні знаходяться ключові критерії, які впливають на прийняття рішення. У випадку вибору міжмережевого екрану це можуть бути критерії, такі як продуктивність, вартість, функціональність, надійність, підтримка інтеграції з іншими системами.
- На нижньому рівні знаходяться варіанти, які розглядаються для прийняття рішення. Наприклад, конкретні моделі міжмережевих екранів: Cisco ASA, Palo Alto Networks, Fortinet і т.д.

Ця ієрархічна структура дозволяє чітко визначити, які фактори впливають на кінцевий вибір, і які з них мають більшу або меншу вагу в контексті загальної мети.

2) Парне порівняння критеріїв.

Після побудови ієрархії необхідно провести парні порівняння між критеріями на кожному рівні. Для цього кожен критерій порівнюється з іншими за важливістю відносно конкретної мети. Наприклад, критерій "Продуктивність" може бути більш важливим, ніж критерій "Вартість", якщо ваша компанія обробляє великий обсяг трафіку.

Парні порівняння здійснюються на основі 9-бальної шкали, розробленої Сааті:

1 – критерії рівнозначні.

3 – один критерій слабко перевершує інший.

5 – один критерій значно перевершує інший.

7 – один критерій суттєво перевершує інший.

9 – один критерій абсолютно переважає інший.

Значення 2, 4, 6 і 8 використовуються для проміжних оцінок. Таким чином, можна провести порівняння кожного критерію з іншими та визначити відносну важливість критеріїв для загальної мети.

3) Розрахунок локальних пріоритетів (ваг).

На основі парних порівнянь проводиться розрахунок локальних пріоритетів для кожного критерію за допомогою власного вектора (eigenvector). Це математичний метод, який допомагає визначити відносні ваги критеріїв у відсотках. Наприклад, якщо продуктивність отримає вагу 0.5 (50%), це означає, що вона вдвічі важливіша за вартість, яка може мати вагу 0.25 (25%).

Сума всіх локальних пріоритетів для кожного рівня ієрархії дорівнює 1. Це дозволяє стандартизувати ваги для подальшого аналізу та порівняння.

4) Парне порівняння варіантів рішень за кожним критерієм.

Наступним кроком є парне порівняння варіантів рішень за кожним із критеріїв, які вже мають визначені ваги. Це дозволяє оцінити, наскільки кожен варіант виконує конкретний критерій. Наприклад, варіанти міжмережевих екранів можна порівняти за критерієм "Продуктивність" або "Вартість", використовуючи ту саму 9-бальну шкалу.

5) Розрахунок глобальних пріоритетів.

Кінцевий етап – це розрахунок глобальних пріоритетів для кожного варіанту рішення. Для цього множаться локальні пріоритети варіантів рішень на ваги критеріїв, отримані на попередніх етапах. Після цього підсумовуються всі результати для кожного варіанту, що дозволяє отримати загальну оцінку для кожного варіанту і зробити раціональний вибір.

6) Аналіз узгодженості.

Оскільки AHP використовує парні порівняння, можливе виникнення суперечливих суджень. Для цього Сааті розробив індекс узгодженості (CI – Consistency Index), який дозволяє перевірити, наскільки логічними є порівняння. Якщо CI є занадто високим, це свідчить про суперечливість у порівняннях, і їх потрібно переглянути.

Метод аналізу ієрархій дозволяє перевірити узгодженість суджень за допомогою відношення узгодженості (CR – Consistency Ratio). Якщо CR менше 0.1, це свідчить про прийнятний рівень узгодженості.

Приклад застосування AHP у виборі міжмережевого екрану:

Представлена ситуація, де компанія обирає між трьома міжмережевими екранами: Firewall A, Firewall B, і Firewall C.

Основними критеріями вибору є продуктивність, вартість, функціональність, і зручність адміністрування.

Ієрархія вибору:

- Головна мета: Вибір найкращого міжмережевого екрану.
- Критерії: Продуктивність, Вартість, Функціональність, Зручність адміністрування.
- Варіанти: Firewall A, Firewall B, Firewall C.

Парне порівняння критеріїв:

- Продуктивність проти Вартість: Продуктивність значно важливіша (оцінка 5).
- Продуктивність проти Функціональність: Продуктивність трохи важливіша (оцінка 3).
- І так далі, поки всі критерії не порівняні між собою.

Парне порівняння варіантів за кожним критерієм:

- Firewall A проти Firewall B за продуктивністю: Firewall A значно кращий (оцінка 5).
- Firewall A проти Firewall C за продуктивністю: Firewall A трохи кращий (оцінка 3).
- Аналогічно порівнюються варіанти за іншими критеріями.

Розрахунок локальних та глобальних пріоритетів. Після цього система дозволяє розрахувати підсумкові оцінки для кожного варіанту. Наприклад, Firewall A може отримати загальну оцінку 0.45, Firewall B – 0.35, а Firewall C – 0.2.

Переваги методу аналізу ієрархій:

- Структурований підхід. Метод дозволяє чітко структуризувати процес прийняття рішень, розбиваючи його на етапи.
- Прозорість процесу. Кожен етап методики, від побудови ієрархії до розрахунку ваг і пріоритетів, є прозорим і чітко документованим. Це дозволяє зрозуміти, які критерії і як впливають на кінцевий вибір, що робить рішення більш обґрунтованим.
- Гнучкість. AHP можна застосовувати до будь-яких типів багатокритеріальних задач. Це універсальний метод, який можна використовувати в багатьох сферах – від технічних до стратегічних рішень, що робить його дуже зручним інструментом у багатьох галузях.
- Можливість включення суб'єктивних факторів. Методика дозволяє врахувати як об'єктивні дані, так і суб'єктивні експертні оцінки.
- Аналіз узгодженості. AHP містить механізми для перевірки узгодженості суджень, що знижує ймовірність суперечливих рішень і робить процес прийняття рішень більш раціональним.
- Залучення багатьох варіантів. Метод дозволяє одночасно аналізувати кілька альтернатив та робити вибір між ними, що особливо корисно при виборі продуктів, послуг або стратегічних рішень.

- Підтримка групових рішень. AHP можна використовувати для прийняття рішень в командах або комітетах, де різні учасники мають різні погляди на важливість критеріїв.

Недоліки методу аналізу ієрархій [45]:

- Суб'єктивність парних порівнянь. Навіть якщо методика дозволяє провести структуроване порівняння критеріїв, деякі аспекти рішення все ще можуть залишатися суб'єктивними, оскільки парні порівняння ґрунтуються на думці експертів або осіб, що приймають рішення.
- Часовитратність. Якщо кількість критеріїв або варіантів значна, процес парних порівнянь може зайняти багато часу.
- Можливість появи суперечливих результатів. Якщо порівняння зроблені недбало або критерії конфліктують між собою, результат може бути нелогічним або суперечливим.
- Вразливість до змін у судженнях. Зміна навіть кількох парних порівнянь може значно вплинути на кінцевий результат, що робить AHP чутливим до незначних змін у судженнях.
- Лінійність моделі. Метод аналізу ієрархій передбачає лінійність між критеріями та варіантами рішень, що не завжди відповідає реальним умовам.
- У складних системах критерії можуть бути пов’язані між собою складнішими залежностями, які не завжди можуть бути враховані простою лінійною моделлю.

3.3 Метод вагових коефіцієнтів

Метод вагових коефіцієнтів — це один із найпоширеніших методів для прийняття рішень у багатокритеріальних задачах. Він використовується для визначення пріоритетів серед альтернативних варіантів на основі кількох критеріїв.

Цей метод базується на тому, що кожному критерію надається певна вага (коефіцієнт), яка відображає його важливість для загального рішення [46].

В кінцевому підсумку, варіанти оцінюються за кожним критерієм, і підсумкова оцінка варіанту розраховується на основі вагових коефіцієнтів.

Основні етапи методу вагових коефіцієнтів:

1) Визначення критеріїв.

Перший етап полягає у визначенні ключових критеріїв, за якими будуть оцінюватися всі варіанти. Це ті фактори, що впливають на вибір і відображають специфічні вимоги або цілі, які ви намагаєтеся досягти. Наприклад, для вибору міжмережевого екрану такими критеріями можуть бути:

- Продуктивність (швидкість обробки трафіку, пропускна здатність).
- Безпека (захист від атак, підтримка сучасних методів шифрування).
- Вартість (придбання, впровадження, технічна підтримка).
- Зручність адміністрування (легкість налаштування, інтеграція з іншими системами).

Цей етап є дуже важливим, оскільки від правильності вибору критеріїв залежить якість і точність кінцевого рішення.

2) Призначення вагових коефіцієнтів.

Після того, як визначені критерії, необхідно кожному з них присвоїти вагу, яка буде відображати відносну важливість цього критерію в контексті загального вибору. Вагові коефіцієнти зазвичай призначаються у відсотках або у вигляді числових значень, які сумарно повинні дорівнювати 1 (або 100%).

Наприклад, ваги можуть бути розподілені так:

- Продуктивність: 0.4 (40%).
- Безпека: 0.3 (30%).

- Вартість: 0.2 (20%).
- Зручність адміністрування: 0.1 (10%).

Це означає, що продуктивність є найважливішим критерієм у процесі вибору, а зручність адміністрування має менший вплив на кінцеве рішення.

3) Оцінка варіантів за кожним критерієм.

Наступний етап — це оцінка кожного варіанту (альтернативи) за кожним критерієм. Для цього можуть використовуватися різні методи оцінки, включаючи експертні думки або кількісні показники. Варіанти оцінюються за шкалою, наприклад, від 1 до 10, де 10 — це максимальна відповідність критерію, а 1 — мінімальна.

Приклад оцінки трьох варіантів міжмережевих екранів:

Firewall A:

- Продуктивність: 8.
- Безпека: 9.
- Вартість: 6.
- Зручність адміністрування: 7.

Firewall B:

- Продуктивність: 7.
- Безпека: 7.
- Вартість: 8.
- Зручність адміністрування: 6.

Firewall C:

- Продуктивність: 9.
- Безпека: 8.
- Вартість: 7.

- Зручність адміністрування: 9.

4) Розрахунок підсумкових оцінок для кожного варіанту.

Після того, як варіанти оцінені за кожним критерієм, необхідно обчислити підсумкову оцінку для кожного варіанту.

Для цього оцінки варіантів за кожним критерієм множаться на вагу цього критерію, після чого результати підсумовуються.

Таким чином, кожен варіант отримує зведену оцінку, яка враховує як важливість критеріїв, так і відповідність варіанту цим критеріям.

Формула для розрахунку виглядає так:

Підсумкова оцінка варіанту = ∑ (Оцінка варіанту за критерієм × Вага критерію)

Наприклад, для Firewall A розрахунок виглядатиме так:

- Продуктивність: 8 × 0.4 = 3.2
- Безпека: 9 × 0.3 = 2.7
- Вартість: 6 × 0.2 = 1.2
- Зручність адміністрування: 7 × 0.1 = 0.7

Підсумкова оцінка для Firewall A: 3.2 + 2.7 + 1.2 + 0.7 = 7.8

Аналогічно розраховуються підсумкові оцінки для інших варіантів:

Firewall B: (7 × 0.4) + (7 × 0.3) + (8 × 0.2) + (6 × 0.1) = 2.8 + 2.1 + 1.6 + 0.6 = 7.1

Firewall C: (9 × 0.4) + (8 × 0.3) + (7 × 0.2) + (9 × 0.1) = 3.6 + 2.4 + 1.4 + 0.9 = 8.3

5) Вибір найкращого варіанту.

Остаточним кроком є вибір варіанту з найбільшою підсумковою оцінкою. У нашому прикладі Firewall C отримав найбільшу підсумкову оцінку 8.3, тому він є найкращим варіантом для обраної мети.

Переваги методу вагових коефіцієнтів:

- Простота у використанні. Метод вагових коефіцієнтів відносно простий у реалізації і не вимагає складних математичних обчислень. Він підходить для ситуацій, де необхідно швидко отримати обґрунтоване рішення на основі кількох критеріїв.
- Гнучкість у виборі критеріїв. Метод дозволяє використовувати будь-які критерії та варіанти, які є важливими для конкретної задачі. Це робить його універсальним у різних сферах, від вибору обладнання до стратегічного планування.
- Чіткість і прозорість. Метод дозволяє чітко бачити, як кожен критерій впливає на кінцеве рішення, і як оцінки варіантів впливають на підсумковий результат. Ваги критеріїв та оцінки варіантів можна легко перевірити і обґрунтувати, що робить процес прийняття рішень прозорим і зрозумілим для всіх учасників.
- Можливість врахування різних типів даних. Метод дозволяє враховувати як кількісні, так і якісні критерії, що робить його універсальним для різних задач.
- Зручність для групових рішень. Метод вагових коефіцієнтів добре підходить для роботи в командах або комітетах, де кілька людей мають різні погляди на важливість критеріїв. Команді легко узгодити ваги критеріїв на основі спільного консенсусу і отримати збалансоване рішення.

Недоліки методу вагових коефіцієнтів [46]:

- Суб'єктивність у визначенні ваг. Ваги критеріїв часто визначаються експертами або зацікавленими сторонами, що може вносити суб'єктивність у процес.
- Неможливість врахування взаємозалежностей між критеріями. Метод вагових коефіцієнтів передбачає, що всі критерії є незалежними один від одного, що не завжди відповідає реальності.

- Лінійність оцінок. Метод передбачає, що вплив кожного критерію на кінцеве рішення є лінійним, що не завжди відповідає складним реальним процесам.
- Трудомісткість при великій кількості варіантів і критеріїв. Якщо кількість критеріїв і варіантів велика, то процес оцінювання може стати складним і тривалим.
- Чутливість до зміни ваг. Зміна навіть незначної ваги одного з критеріїв може суттєво вплинути на кінцевий результат, що робить метод вразливим до маніпуляцій або непередбачуваних змін у судженнях.

3.4 Обґрунтування вибору методу прийняття рішень

Аналіз прийняття рішень в умовах невизначеності є складним і багатофакторним процесом, особливо у сфері інформаційної безпеки. Використання таких методів, як аналіз ієрархій і методи вагових коефіцієнтів, дозволяє структурувати процес прийняття рішень і врахувати різні критерії, що впливають на вибір міжмережевого екрану. Ці методи допомагають зменшити суб'єктивність і забезпечити системний підхід до прийняття рішень в умовах, коли інформація є неповною або невизначеною.

Для розробки методики вибору міжмережевих екранів найкраще підходить метод аналізу ієрархій. На відміну від інших цей метод дозволяє враховувати багатокритеріальні вимоги, надає структурований підхід до збору експертних оцінок, дозволяє враховувати взаємозалежності між критеріями та забезпечує точніший результат в умовах невизначеності.

Метод аналізу ієрархій є ефективним інструментом для вирішення складних багаторівневих завдань вибору, де важливим є врахування як кількісних, так і якісних аспектів. Це робить його оптимальним вибором для систематизації процесу вибору міжмережевих екранів, що забезпечить найбільш ефективну побудову системи мережевої безпеки.

4. РОЗРОБКА МЕТОДИКИ ВИБОРУ ЗАСОБІВ МІЖМЕРЕЖЕВОЇ БЕЗПЕКИ

Вибір оптимального рішення серед широкого спектру доступних міжмережевих екранів є складним завданням, що вимагає врахування великої кількості різноманітних критеріїв. До цих критеріїв можуть належати як технічні характеристики, так і фінансові аспекти, а також рівень підтримки вендора, можливість інтеграції з іншими системами, масштабованість та відповідність специфічним потребам організації.

Метод аналізу ієрархій є особливо ефективним у тих випадках, коли необхідно враховувати як кількісні, так і якісні характеристики продуктів. За допомогою цього методу можна розподілити ваги між критеріями на основі експертних оцінок та інших даних, що забезпечує прозорість і точність процесу прийняття рішень. Основна перевага AHP полягає в тому, що він дозволяє виявити пріоритети між різними критеріями, враховуючи взаємозв'язки та впливи між ними, що є важливим при виборі міжмережевого екрану.

У даному розділі поетапно розроблена методика вибору міжмережевого екрану, з детальним описом кожного етапу — від визначення ключових критеріїв до фінального оцінювання альтернатив. Особливу увагу приділено методам парного порівняння критеріїв, встановленню їх вагових коефіцієнтів та розрахунку підсумкових оцінок для кожного варіанту.

4.1 Визначення основних критеріїв вибору міжмережевого екрану

Вибір міжмережевого екрану для побудови системи мережевої безпеки є складним багатокритеріальним завданням, оскільки цей елемент інфраструктури має забезпечувати надійний захист мережі, високий рівень продуктивності та відповідати вимогам конкретної організації. Для прийняття обґрунтованого рішення

необхідно визначити ключові критерії, які впливають на ефективність та доцільність використання того чи іншого міжмережевого екрану. Наведу основні критерії, які є найбільш важливими під час вибору.

Продуктивність міжмережевого екрану відіграє ключову роль, особливо у великих і високо навантажених мережах. Цей критерій включає такі показники, як швидкість обробки трафіку, затримка при аналізі пакетів, здатність підтримувати високий обсяг одночасних з'єднань та пропускну здатність. Важливо, щоб міжмережевий екран не ставав вузьким місцем у мережі та не знижував її загальну продуктивність.

Показники продуктивності — швидкість обробки трафіку, підтримка великої кількості одночасних з'єднань, затримка при аналізі пакетів.

Основне завдання міжмережевого екрану — це забезпечення захисту мережі від зовнішніх загроз. До критеріїв безпеки належить здатність виявляти та блокувати несанкціоновані дії, підтримка сучасних технологій, захист від атак на прикладному рівні (наприклад, веб-додатків) та інтеграція з іншими системами захисту (IDS/IPS, антивіруси тощо). Міжмережевий екран також повинен забезпечувати надійний захист від DDoS-атак, вторгнень, зловмисного програмного забезпечення та інших кібератак.

Показники безпеки — рівень захисту від DDoS, інтеграція з IDS/IPS, наявність функцій DPI, захист на прикладному рівні.

Міжмережевий екран повинен бути здатним до масштабування відповідно до зростання мережі. Масштабованість передбачає можливість розширення функціональних можливостей пристрою або рішення в міру збільшення кількості користувачів, підключених пристроїв, а також збільшення мережевого трафіку.

Показники масштабованості — можливість масштабування без зниження продуктивності, підтримка віртуалізації, гнучкість налаштувань.

Вартість міжмережевого екрану включає початкові витрати на придбання, а також вартість впровадження, підтримки, оновлень і технічного обслуговування. Важливо враховувати загальну вартість володіння, оскільки дешевший пристрій може мати високі витрати на обслуговування або потребувати частих оновлень і ремонту.

Показники вартості — початкові витрати, витрати на підтримку, загальна вартість володіння.

Адміністрування та управління міжмережевим екраном є важливими критеріями, оскільки вони впливають на час і зусилля, які потрібні для його налаштування, моніторингу та підтримки. Важливо, щоб рішення було зручним для використання з точки зору інтерфейсу, мало широкий функціонал для централізованого управління та інтеграції з існуючими системами моніторингу.

Показники зручності — наявність централізованого управління, легкість у налаштуванні, автоматизація процесів.

Міжмережевий екран вимагає постійного оновлення та технічної підтримки. Важливо враховувати, як швидко вендор надає оновлення для захисту від нових загроз, чи є доступ до якісної технічної підтримки, а також можливості самостійного обслуговування системи. Це може вплинути на безперервність роботи міжмережевого екрану та швидкість реагування на нові загрози.

Показники підтримки — доступність оновлень, якість технічної підтримки, час реакції на проблеми.

Міжмережевий екран повинен легко інтегруватися з іншими засобами безпеки, такими як системи виявлення та запобігання вторгнень (IDS/IPS), VPN, SIEM-системи для моніторингу інцидентів безпеки та антивірусні програми. Важливим є те, наскільки легко та безпечно це рішення може бути інтегроване в існуючу інфраструктуру організації.

Показники інтеграції — сумісність з іншими системами, легкість інтеграції, доступність API для налаштування.

Критерії, які розглядаються при виборі міжмережевого екрану, охоплюють широкий спектр технічних, фінансових та організаційних аспектів. Визначення пріоритетності цих критеріїв допомагає створити чітку та структуровану методику вибору, що дозволить вибрати оптимальне рішення для захисту мережі відповідно до потреб організації.

4.2 Розробка ієрархічної структури вибору

Метод аналізу ієрархій базується на побудові ієрархічної моделі прийняття рішень, яка дозволяє структурувати складне багатокритеріальне завдання у вигляді чітко визначених рівнів. Цей підхід дає змогу розподілити завдання вибору міжмережевого екрану на окремі компоненти, що полегшує процес оцінювання та порівняння. У цьому розділі буде розроблена ієрархічна структура вибору міжмережевого екрану, що включає визначення основної мети, критеріїв, підкритеріїв та альтернатив.

Другий рівень ієрархії визначає варіанти та їх альтернативи при виборі міжмережевого екрану. Представлений рівень може загальними типами засобу, а саме апаратний, програмний або хмарний міжмережевий екран.

Третій рівень ієрархії складається з основних критеріїв, які впливають на вибір міжмережевого екрану.

На рисунку 4.1 сформована схема ієрархії рівнів прийняття рішень дослідження.

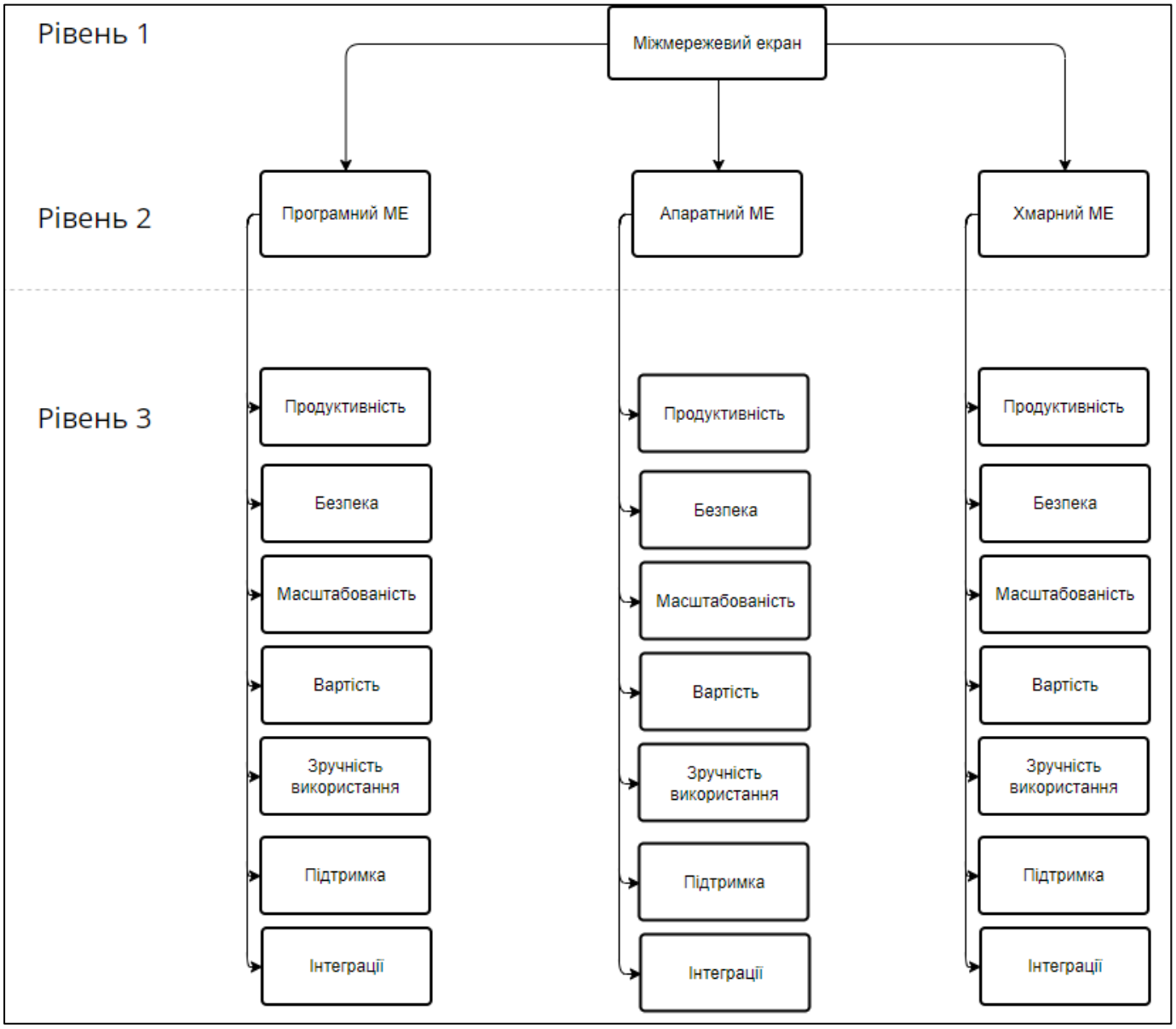

Рисунок 4.1 - Ієрархія рівнів прийняття рішень

4.3 Встановлення вагових коефіцієнтів критеріїв

Встановлення вагових коефіцієнтів є одним із ключових етапів методу аналізу ієрархій, що дозволяє визначити, наскільки кожен критерій впливає на загальне рішення. У цьому розділі буде описано процес визначення ваг для кожного критерію та підкритерію, а також розрахунок їх значущості для прийняття остаточного рішення щодо вибору міжмережевого екрану.

Кожен критерій має різний рівень важливості для вибору міжмережевого екрану. Наприклад, у великій корпорації продуктивність може бути важливішою за вартість, тоді як у невеликій організації вартість може мати пріоритет. Вагові коефіцієнти визначають, наскільки суттєвою є роль кожного критерію у кінцевому виборі.

Для цього використовуються парні порівняння між критеріями. У процесі порівнянь експерти оцінюють відносну важливість одного критерію порівняно з іншим за шкалою від 1 до 9, де:

1 – обидва критерії однаково важливі;

3 – один критерій дещо важливіший за інший;

5 – один критерій значно важливіший за інший;

7 – один критерій суттєво важливіший;

9 – один критерій абсолютно важливіший.

Проміжні значення 2, 4, 6, 8 використовуються для оцінок між зазначеними рівнями.

Процес парних порівнянь дозволяє визначити відносну вагу кожного критерію. У цьому етапі експерти порівнюють усі критерії попарно. Для прикладу, порівняємо продуктивність та безпеку:

- Якщо продуктивність оцінюється як важливіша за безпеку, то продуктивність отримує оцінку 5, а безпека – 1/5.
- Якщо обидва критерії рівні за важливістю, кожен з них отримує оцінку 1.

Таким чином формується матриця парних порівнянь, яка використовується для подальших розрахунків ваг.

Приклад парних порівнянь між основними критеріями для вибору міжмережевого екрану наведено в таблиці 4.1.

Таблиця 4.1 - Парні порівняння між основними критеріями для вибору міжмережевого екрану

Критерій	Продуктивність	Безпека	Масштабованість	Вартість	Зручність адміністрування	Підтримка	Інтеграція
Продуктивність	1	3	2	5	4	3	2
Безпека	1/3	1	2	4	3	2	3
Масштабованість	1/2	1/2	1	3	2	3	2
Вартість	1/5	1/4	1/3	1	2	3	4
Зручність адміністрування	1/4	1/3	1/2	1/2	1	3	2
Підтримка	1/3	1/2	1/3	1/3	1/3	1	2
Інтеграція	1/2	1/3	1/2	1/4	1/2	1/2	1

Після того як сформована матриця парних порівнянь, вагові коефіцієнти обчислюються шляхом нормалізації рядків і середнього значення для кожного критерію. Алгоритм розрахунку виглядає наступним чином:

- Сумування значень по кожному стовпцю матриці.
- Нормалізація матриці — ділення кожного елемента матриці на суму відповідного стовпця.

- Обчислення середнього значення для кожного рядка, яке стає ваговим коефіцієнтом для відповідного критерію.

Згідно з вищенаведеною таблиці парних порівнянь, після нормалізації та підсумування вагових коефіцієнтів, отримано наступні результати в таблиці 4.2.

Таблиця 4.2 – Розрахунок вагових коефіцієнтів для критеріїв порівняння

Критерій	Ваговий коефіцієнт
Продуктивність	0.32
Безпека	0.27
Масштабованість	0.15
Вартість	0.10
Зручність адміністрування	0.08
Підтримка	0.05
Інтеграції	0.03

Таким чином, на основі обчислень можна побачити, що продуктивність і безпека є найважливішими критеріями, тоді як інтеграція з іншими системами має відносно меншу вагу.

Для підтвердження достовірності отриманих результатів потрібно перевірити узгодженість таблиці парних порівнянь. Якщо узгодженість недостатньо висока, слід переглянути оцінки парних порівнянь і при необхідності внести корективи. Узгодженість оцінюється через індекс узгодженості (CI) та відношення узгодженості (CR), яке повинне бути менше 0.1 (10%) для визнання результатів прийнятними.

На етапі встановлення вагових коефіцієнтів критеріїв здійснюється формалізація важливості кожного фактора для процесу вибору міжмережевого екрану. Отримані ваги дозволяють прийняти обґрунтоване рішення, оскільки вони відображають реальні пріоритети організації.

Метод парних порівнянь у рамках AHP дає можливість врахувати як кількісні, так і якісні характеристики, що робить його надійним інструментом для прийняття складних рішень у сфері мережевої безпеки.

4.4 Оцінювання альтернатив міжмережевих екранів

Оцінювання альтернатив міжмережевих екранів є важливим етапом у процесі прийняття рішення. На основі визначених критеріїв та їхніх вагових коефіцієнтів, кожна альтернатива аналізується для вибору найкращого рішення, яке найбільше відповідає потребам організації. Цей розділ присвячений детальному розгляду можливих альтернатив і процесу їх оцінки згідно з методом аналізу ієрархій.

Першим кроком є визначення можливих альтернатив для вибору міжмережевого екрану. Ці альтернативи можуть охоплювати різні типи продуктів і рішень, представлені на ринку, як апаратні, так і програмні. Наприклад, можна обрати між:

- Альтернатива 1: Апаратний міжмережевий екран (наприклад, Cisco ASA, Fortinet FortiGate);
- Альтернатива 2: Програмний міжмережевий екран (наприклад, pfSense, OPNsense);
- Альтернатива 3: Хмарний міжмережевий екран (наприклад, AWS Firewall, Google Cloud Armor).

Кожна з цих альтернатив має свої переваги й недоліки залежно від технічних та фінансових вимог організації, а також від специфіки її інфраструктури.

Оцінювання здійснюється за шкалою від 1 до 9, де 1 означає дуже низьку відповідність вимогам, а 9 — дуже високу відповідність.

Продуктивність міжмережевого екрану визначається за такими параметрами, як пропускна здатність, затримка при обробці трафіку та можливість ефективної роботи під високим навантаженням. Апаратні міжмережеві екрани зазвичай мають

високу продуктивність, оскільки спеціалізоване обладнання дозволяє обробляти більший обсяг даних із мінімальними затримками. Програмні рішення можуть бути менш продуктивними, але вони є більш гнучкими в налаштуванні, тоді як хмарні рішення можуть масштабувати продуктивність відповідно до потреб організації.

- Альтернатива 1 (апаратний міжмережевий екран): 7/9 (висока продуктивність).
- Альтернатива 2 (програмний міжмережевий екран): 5/9 (середня продуктивність).
- Альтернатива 3 (хмарний міжмережевий екран): 8/9 (висока продуктивність, залежить від провайдера).

Безпека міжмережевого екрану оцінюється за здатністю забезпечувати захист мережі від зовнішніх загроз, зокрема за можливостями фільтрації трафіку, захисту від DDoS-атак, інтеграції з іншими інструментами безпеки та наявністю вбудованих механізмів виявлення і реагування на загрози.

- Альтернатива 1 (апаратний міжмережевий екран): 8/9 (високий рівень захисту, апаратні рішення мають власні механізми безпеки).
- Альтернатива 2 (програмний міжмережевий екран): 9/9 (залежить від налаштувань і конфігурації).
- Альтернатива 3 (хмарний міжмережевий екран): 6/9 (високий рівень захисту за рахунок сервісів постачальника).

Масштабованість визначається тим, наскільки просто можна збільшити потужність рішення у відповідь на зростання потреб організації. Хмарні рішення зазвичай пропонують високу масштабованість, апаратні рішення потребують додаткового обладнання, а програмні рішення можуть масштабуватися шляхом додавання нових інстанцій.

- Альтернатива 1 (апаратний міжмережевий екран): 6/9 (обмежена можливість масштабування).

- Альтернатива 2 (програмний міжмережевий екран): 7/9 (залежить від ресурсу сервера).
- Альтернатива 3 (хмарний міжмережевий екран): 5/9 (висока масштабованість за рахунок можливостей хмарних провайдерів).

Вартість оцінюється як загальні витрати на впровадження та обслуговування міжмережевого екрану.

Апаратні рішення зазвичай вимагають значних капітальних витрат на початковому етапі, тоді як програмні рішення дешевші у встановленні, але потребують ресурсів для підтримки.

Хмарні рішення пропонують модель оплати за використання, що може бути як перевагою, так і недоліком залежно від тривалості використання та обсягу трафіку.

- Альтернатива 1 (апаратний міжмережевий екран): 5/9 (високі капітальні витрати).
- Альтернатива 2 (програмний міжмережевий екран): 4/9 (відносно низькі витрати).
- Альтернатива 3 (хмарний міжмережевий екран): 8/9 (гнучка модель оплати, залежить від обсягу).

Зручність адміністрування міжмережевого екрану визначається простотою налаштувань, наявністю графічних інтерфейсів, а також можливістю централізованого управління.

- Альтернатива 1 (апаратний міжмережевий екран): 9/9 (зручні інтерфейси, можливість віддаленого керування).
- Альтернатива 2 (програмний міжмережевий екран): 7/9 (гнучкі налаштування, проте потребує технічних знань).
- Альтернатива 3 (хмарний міжмережевий екран): 6/9 (високий рівень зручності, хмарні сервіси часто мають прості інтерфейси).

Підтримка оцінюється за рівнем технічної підтримки, яку надають виробники чи постачальники, а інтеграція — за можливістю безшовного впровадження рішення в існуючу IT-інфраструктуру.

- Альтернатива 1 (апаратний міжмережевий екран): 6/9 (зазвичай має хорошу підтримку від виробника та можливості інтеграції).
- Альтернатива 2 (програмний міжмережевий екран): 8/9 (відкрите програмне забезпечення може мати меншу підтримку).
- Альтернатива 3 (хмарний міжмережевий екран): 7/9 (високий рівень підтримки та інтеграції).

Інтеграція оцінюється сумісністю з іншими системами, доступністю API для налаштування.

- Альтернатива 1 (апаратний міжмережевий екран): 5/9 (зазвичай сумісний з іншими системами).
- Альтернатива 2 (програмний міжмережевий екран): 6/9 (сумісний з іншими системами, має легку доступність API)
- Альтернатива 3 (хмарний міжмережевий екран): 7/9 (високий інтеграції та легкості).

Оцінювання різних альтернатив міжмережевих екранів здійснювалось при консультації з експертами після плідного обговорення та аналізу.

На етапі оцінювання альтернатив міжмережевих екранів здійснюється порівняння основних характеристик кожної альтернативи за визначеними критеріями.

Цей процес дозволяє побудувати повне уявлення про переваги та недоліки кожної альтернативи та підготувати основу для розрахунку підсумкових оцінок і вибору найкращого рішення, також допомагає у визначенні основних пріоритетів організації.

4.5 Розрахунок підсумкових оцінок та вибір найкращого варіанту

Останнім етапом методу аналізу ієрархій є розрахунок підсумкових оцінок для кожної альтернативи та вибір найкращого варіанту міжмережевого екрану на основі отриманих результатів. На цьому етапі, використовуючи вагові коефіцієнти, розраховані раніше, та оцінки альтернатив по кожному з критеріїв, ми отримуємо фінальні значення, які дозволяють зробити обґрунтоване рішення.

Наступним кроком формується таблиця 4.3, де кожна альтернатива порівнюється за кожним критерієм, враховуючи підкритерії.

Таблиця 4.3 – Порівняння альтернатив

Критерій	Ваговий коефіцієнт	Альтернатива 1 (Апаратний МЕ)	Альтернатива 2 (Програмний МЕ)	Альтернатива 3 (Хмарний МЕ)
Продуктивність	0.32	7	5	8
Безпека	0.27	8	9	6
Масштабованість	0.15	6	7	5
Вартість	0.10	5	4	8
Зручність використання	0.08	9	7	6
Підтримка	0.05	6	8	7
Інтеграція	0.03	5	6	7

Кожна альтернатива, яка представляє певний тип або модель міжмережевого екрану, оцінюється за всіма основними та додатковими критеріями, визначеними на попередніх етапах. Оцінки виставляються на основі експертних знань, результатів тестування, аналітичних даних або опублікованих характеристик продуктів.

Для кожної альтернативи оцінки по кожному критерію множаться на відповідні вагові коефіцієнти. Це дозволяє врахувати відносну важливість критеріїв у загальному процесі вибору. Наприклад, для Альтернативи 1 розрахунок виглядатиме так:

- Продуктивність: 7 × 0.32 = 2.24
- Безпека: 8 × 0.27 = 2.16
- Масштабованість: 6 × 0.15 = 0.9
- Вартість: 5 × 0.10 = 0.5
- Зручність адміністрування: 9 × 0.08 = 0.72
- Підтримка: 6 × 0.05 = 0.3
- Інтеграція: 5 × 0.03 = 0.15

Загальна підсумкова оцінка для Альтернативи 1 становить:

2.24 + 2.16 + 0.9 + 0.5 + 0.72 + 0.3 + 0.15 = 6.97

Те саме виконується для всіх інших альтернатив. Підсумкові оцінки для всіх варіантів порівнюються, і альтернатива з найвищою підсумковою оцінкою буде вважатися найкращою для впровадження в системі мережевої безпеки.

Наприклад:

- Альтернатива 1 (Апаратний МЕ) : 6.97
- Альтернатива 2 (Програмний МЕ): 6.35
- Альтернатива 3 (Хмарний МЕ): 7.04

На основі отриманих результатів найвищу оцінку отримала Альтернатива 3 із підсумковою оцінкою 7.04. Це означає, що Хмарний міжмережевий екран є найбільш відповідним варіантом для вибору згідно з визначеними критеріями та їх ваговими коефіцієнтами.

З огляду на результати, можна зробити кілька висновків:

- Продуктивність і безпека залишилися ключовими факторами, що мали вирішальний вплив на вибір. Альтернатива 3 продемонструвала високі оцінки за продуктивність і безпеку, що дозволило їй перевершити інші варіанти.
- Вартість та масштабованість також суттєво вплинули на підсумковий результат. Альтернатива 3 виявилася найекономічнішою та найбільш придатною до масштабування, що додатково підвищило її рейтингову оцінку.
- Зручність адміністрування та підтримка також мали важливе значення, особливо для організацій із великою кількістю користувачів та складною інфраструктурою.

Метод аналізу ієрархій дозволив структурувати складне завдання вибору міжмережевого екрану та перетворити його на процес, що базується на чисельних оцінках і об'єктивних даних.

Завдяки порівнянню альтернатив за різними критеріями та обчисленню вагових коефіцієнтів, вдалося обрати найкращу альтернативу, яка найбільше відповідає потребам і вимогам організації.

Альтернатива 3 є найкращим вибором, оскільки вона отримала найвищу підсумкову оцінку і забезпечує оптимальне співвідношення між продуктивністю, безпекою, вартістю та іншими важливими критеріями.

4.6 Аналіз чутливості результатів

Аналіз чутливості є важливим етапом у процесі прийняття рішення на основі методу аналізу ієрархій. Його мета — оцінити, як зміна вагових коефіцієнтів критеріїв впливає на підсумкові результати, і перевірити стабільність отриманих рішень. Аналіз чутливості допомагає виявити, чи залишається вибір найкращої

альтернативи незмінним при змінах у пріоритетах або чи існує ймовірність вибору іншої альтернативи за певних умов.

У реальних умовах, при оцінці міжмережевих екранів, вагові коефіцієнти критеріїв можуть бути визначені з певним ступенем суб'єктивності або залежати від обставин, що змінюються з часом. Наприклад, важливість вартості може зростати в умовах обмеженого бюджету, або ж підвищення рівня безпеки може стати основним критерієм у разі підвищення загрози кіберзлочинності. Тому важливо перевірити, як зміна пріоритетів критеріїв впливатиме на підсумковий вибір.

Аналіз чутливості передбачає поетапне варіювання вагових коефіцієнтів кожного з критеріїв та аналіз отриманих результатів. У процесі аналізу послідовно змінюються вагові коефіцієнти одного або декількох критеріїв, зберігаючи при цьому загальну суму ваг (яка повинна дорівнювати 1). Після цього проводиться повторний розрахунок підсумкових оцінок для кожної альтернативи, і результати порівнюються з базовим розрахунком.

Для кожного з критеріїв можна змінити вагові коефіцієнти, щоб оцінити вплив цих змін на кінцеві результати. Нижче представлено приклади того, як зміна ваг впливає на підсумкові оцінки.

Якщо організація вирішує, що продуктивність міжмережевого екрану має вищий пріоритет, ваговий коефіцієнт для цього критерію збільшується. Наприклад, якщо ваговий коефіцієнт для продуктивності змінюється з 0.32 на 0.40, результати можуть суттєво змінитися на користь альтернативи з найвищою продуктивністю. При цьому альтернативи з нижчими показниками продуктивності втрачають свої позиції.

- Базовий варіант: Альтернатива 3 є найкращою (7.04).
- Після зміни: Альтернатива 1, яка має вищу оцінку за продуктивність (8 балів), може стати найкращою за умови, що продуктивність отримує ваговий коефіцієнт більше 0.35.

Якщо безпека стає ключовим пріоритетом, ваговий коефіцієнт для цього критерію збільшується. Наприклад, якщо ваговий коефіцієнт критерію безпеки змінюється з 0.27 до 0.35, рішення, яке має найвищу оцінку за безпеку, стає більш конкурентоспроможним.

- Базовий варіант: Альтернатива 3 є найкращою.
- Після зміни: Альтернатива 1 або Альтернатива 2 можуть мати вищу оцінку, якщо безпека стає вирішальним фактором.

Зміна ваги критерію вартості є важливою для організацій, що працюють в умовах обмеженого бюджету. Якщо ваговий коефіцієнт вартості збільшується, наприклад з 0.10 до 0.20, тоді альтернативи, що мають нижчу вартість, можуть стати привабливішими, а дорогі рішення втрачають свої позиції.

- Базовий варіант: Альтернатива 3 є найкращою.
- Після зміни: Альтернатива 2, яка має нижчу вартість, може стати найкращою за умови підвищення вагового коефіцієнта критерію вартості.

Можна представити графічно за допомогою діаграм, які показують, як змінюється ранжування альтернатив залежно від зміни ваг критеріїв. Наприклад, на одній осі може бути відкладено ваговий коефіцієнт, а на іншій — підсумкові оцінки для кожної альтернативи. Такі діаграми наочно демонструють, за яких умов одна альтернатива може випередити іншу.

Аналіз чутливості дозволяє виявити критичні критерії, які мають найбільший вплив на підсумкові оцінки. У результаті аналізу можна зробити такі висновки:

- Продуктивність є одним із ключових критеріїв: при зміні ваги продуктивності кінцевий вибір може змінитися.
- Безпека також має суттєвий вплив на вибір: збільшення її ваги може значно підвищити оцінки певних альтернатив.

- Вартість може змінювати підсумкові результати в залежності від умов бюджету організації.

Оцінка стійкості прийнятого рішення дає можливість адаптувати вибір під змінні умови. Це дозволяє краще підготуватися до потенційних змін в умовах експлуатації системи мережевої безпеки.

Зміна вагових коефіцієнтів критеріїв впливає на вибір найкращого міжмережевого екрану. Він є важливим інструментом для перевірки стабільності результатів і допомагає прийняти більш обґрунтоване рішення в умовах невизначеності. Застосування цього аналізу забезпечує гнучкість і адаптацію вибору до змін у потребах та пріоритетах організації.

Таким чином, метод аналізу ієрархій продемонстрував свою ефективність як інструмент прийняття рішень у процесі вибору міжмережевого екрану. Цей метод дозволяє враховувати різні аспекти безпеки, продуктивності, вартості та інших факторів, що робить його придатним для застосування в умовах реальної експлуатації. Завдяки системному підходу та можливості оцінки альтернатив за кількома критеріями, організація може приймати обґрунтовані та оптимальні рішення щодо вибору засобів мережевої безпеки, забезпечуючи високий рівень захисту своїх інформаційних ресурсів.

5 ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДИКИ

5.1 Вимоги та призначення програмного застосунку

Після розробки методики вибору засобів побудови системи мережевої безпеки, в випадку даної роботи для вибору найкращого варіанту міжмережевого екрану потрібно провести автоматизацію даного процесу.

Програмний застосунок створений для автоматизації процесу вибору міжмережевого екрану на основі методу аналізу ієрархій. Основною метою є допомога організаціям у виборі найкращого рішення для захисту мережі, враховуючи їхні індивідуальні вимоги до ключових критеріїв, таких як продуктивність, безпека, масштабованість, вартість, зручність адміністрування, підтримка та інтеграція.

Користувач подає на вхід вагові коефіцієнти критеріїв через текстовий файл, а також вводить з клавіатури оцінки для кожної з альтернативних систем міжмережевих екранів, після чого програма обчислює та визначає найкращий варіант на основі введених даних.

Даний застосунок стане у нагоді для реалізації методики зацікавленими користувачами, тому далі розберу архітектуру програми, її основні методи та протестую створений додаток для візуалізації результатів з їх поясненням.

Розроблений код програмного застосунку розміщено у Додатку А.

5.2 Розробка архітектури системи прийняття рішень

Архітектура системи прийняття рішень у програмі для вибору міжмережевого екрану базується на методі аналізу ієрархій.

Основні компоненти:

1) Введення даних.

- Користувач вводить назви двох альтернатив міжмережевих екранів.
- Користувач вводить числові оцінки (від 1 до 9) для кожної альтернативи за визначеними критеріями.
- Програма зчитує вагові коефіцієнти критеріїв з текстового файлу (наприклад, продуктивність, безпека, масштабованість тощо).

2) Обробка даних.

- Завантажує вагові коефіцієнти критеріїв із зовнішнього текстового файлу. Забезпечує гнучкість і адаптованість системи для різних організаційних вимог.
- Приймає оцінки від користувача для кожної альтернативи за всіма критеріями.

3) Обчислення результатів.

- Програма використовує вагові коефіцієнти для кожного критерію та введені оцінки, щоб розрахувати загальну оцінку кожної альтернативи шляхом множення оцінок на відповідні вагові коефіцієнти та підсумування.

4) Виведення результатів.

- Підсумкові бали кожної альтернативи виводяться на екран.
- Програма автоматично визначає альтернативу з найвищим підсумковим балом і виводить її як найкращий вибір.

5) Користувацький інтерфейс.

- Інтерфейс програми реалізований через командний рядок (CLI), забезпечуючи простоту введення даних і інтерактивний процес роботи з програмою.

Окремо розгляну архітектурні елементи застосунку:

- Взаємодія з користувачем: введення даних і відображення результатів.
- Модуль обробки даних: зчитування файлів та обробка вагових коефіцієнтів.

- Модуль обчислення: застосування методу AHP для оцінки альтернатив.

Ця архітектура робить програму простою у використанні та модифікації, забезпечуючи надійний процес прийняття рішень на основі методу аналізу ієрархій.

Можливі поліпшення для створеного застосунку:

- Розширення кількості альтернатив та критеріїв. Програма може бути адаптована для роботи з більшою кількістю альтернатив та критеріїв.
- Перевірка узгодженості, додати перевірку узгодженості матриць порівнянь, як у методі AHP.
- Збереження результатів, додати можливість збереження результатів у файл для подальшого аналізу.

5.3 Реалізація основних функцій програми

Перед написанням функцій в програмі потрібно імпортувати бібліотеку Numpy, яка слугує розширенням математичних здібностей програми.

«import numpy as np»

Наглядний огляд функцій створеної програми на конкретних частинах коду з поясненням. Спочатку розглядається функція зчитування вагових коефіцієнтів:

- Функція read_weights зчитує критерії та їхні вагові коефіцієнти з файлу weights.txt.
- Перевіряється коректність формату файлу та сума вагових коефіцієнтів повинна дорівнювати 1.0. Якщо це не так, програма завершується з повідомленням про помилку.

Функція read_weights зображена на рисунку 5.1.

```python
def read_weights(file_path):

    criteria = []
    weights = []
    try:
        with open(file_path, 'r', encoding='utf-8') as file:
            for line in file:
                parts = line.strip().split(',')
                if len(parts) != 2:
                    print(f"Некоректний рядок у файлі: {line.strip()}")
                    continue
                criteria.append(parts[0].strip())
                weights.append(float(parts[1].strip()))
    except FileNotFoundError:
        print(f"Файл {file_path} не знайдено.")
        exit(1)
    except ValueError:
        print("Вага повинна бути числовим значенням.")
        exit(1)
    # Перевірка суми ваг
    total_weight = sum(weights)
    if not np.isclose(total_weight, 1.0):
        print(f"Сума ваг {total_weight} не дорівнює 1.0. Будь ласка, перевірте файл ваг.")
        exit(1)

    return criteria, weights
```

Рисунок 5.1 – Функція read_weights

Наступною розглядається функція отримання назв альтернатив:

- Функція get_alternative_names запитує у користувача назви двох альтернативних міжмережевих екранів.
- Перевіряється, щоб назви не були порожніми.

Вміст функції зображено на рисунку 5.2.

```python
def get_alternative_names():
    """
    Отримання назв альтернатив від користувача.
    """
    alternatives = []
    print("Введіть назви двох альтернативних міжмережевих екранів:")
    for i in range(1, 3):
        name = input(f"Назва Альтернативи {i}: ").strip()
        if not name:
            print("Назва не може бути порожньою.")
            exit(1)
        alternatives.append(name)
    return alternatives
```

Рисунок 5.2 – Функція get_alternative_names

Далі розглядається функція отримання оцінок за кожним критерієм:

- Функція get_scores запрошує користувача ввести оцінки для кожної альтернативи за кожним критерієм.
- Оцінки повинні бути числовими значеннями від 1 до 9. Якщо введено некоректне значення, користувачеві пропонується спробувати ще раз.

Вміст функції зображено на рисунку 5.3.

```
def get_scores(criteria, alternatives):
    """
    Отримання оцінок альтернатив за кожним критерієм від користувача.
    """
    scores = {alternative: [] for alternative in alternatives}
    print("\nВведіть оцінки для кожної альтернативи за кожним критерієм (від 1 до 9):")
    for criterion in criteria:
        print(f"\nКритерій: {criterion}")
        for alternative in alternatives:
            while True:
                try:
                    score = float(input(f"Оцінка для {alternative}: "))
                    if score < 1 or score > 9:
                        print("Оцінка повинна бути між 1 і 9. Спробуйте ще раз.")
                        continue
                    scores[alternative].append(score)
                    break
                except ValueError:
                    print("Будь ласка, введіть числове значення.")
    return scores
```

Рисунок 5.3 – Функція get_scores

Функцію розрахунку підсумкових оцінок обраних міжмережевих екранів:

- Функція calculate_final_scores обчислює підсумкові оцінки для кожної альтернативи, множуючи оцінки за критеріями на відповідні вагові коефіцієнти та підсумовуючи результати.

Вміст функції зображено на рисунку 5.4.

```python
def calculate_final_scores(scores, weights, criteria):
    """
    Розрахунок підсумкових оцінок для кожної альтернативи.
    """
    final_scores = {}
    for alternative, alt_scores in scores.items():
        total_score = sum([score * weight for score, weight in zip(alt_scores, weights)])
        final_scores[alternative] = total_score
    return final_scores
```

Рисунок 5.4 – Функція calculate_final_scores

Останньою йде функція виведення результатів, яка також є основною в програмі:

- Функція main виводить підсумкові оцінки для кожної альтернативи та визначає найкращу альтернативу на основі найбільшої підсумкової оцінки.

Вміст даної функції зображено на рисунку 5.5.

```python
def main():
    # Зчитування вагових коефіцієнтів з файлу
    weights_file = 'weights.txt'
    criteria, weights = read_weights(weights_file)

    # Отримання назв альтернатив від користувача
    alternatives = get_alternative_names()

    # Отримання оцінок від користувача
    scores = get_scores(criteria, alternatives)

    # Розрахунок підсумкових оцінок
    final_scores = calculate_final_scores(scores, weights, criteria)

    # Виведення підсумкових оцінок
    print("\nПідсумкові оцінки для кожної альтернативи:")
    for alternative, score in final_scores.items():
        print(f"{alternative}: {score:.4f}")

    # Вибір найкращої альтернативи
    best_alternative = max(final_scores, key=final_scores.get)
    print(f"\nНайкраща альтернатива: {best_alternative}")

if __name__ == "__main__":
    main()
```

Рисунок 5.5 – Функція main

На цьому огляд основних функцій завершено, наступним етапом є тестування створеного застосунку.

5.4 Тестування розробленої програмної реалізації відповідно до запропонованої методики прийняття рішень

Для проведення тестування створеної програми, спочатку створюється текстовий файл weights.txt, в який вкладається значення вагових коефіцієнтів, який відповідає вимогам конкретної організації. Вміст файлу зображено на рисунку 5.6.

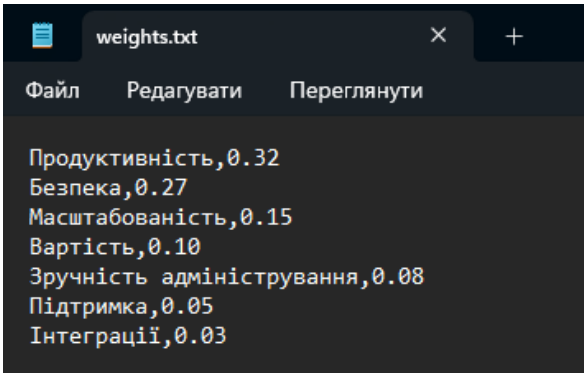

Рисунок 5.6 – Вміст файлу weights.txt

Далі компілюється створений програмний код, користувач проводить дії, які передбачені архітектурою даного застосунку. Результат роботи зображено на рисунках 5.7, 5.8.

```
Введіть назви двох альтернативних міжмережевих екранів:
Назва Альтернативи 1:
Cisco ASA
Назва Альтернативи 2:
Fortinet FortiGate

Введіть оцінки для кожної альтернативи за кожним критерієм (від 1 до 9):

Критерій: Продуктивність
Оцінка для Cisco ASA:
8
Оцінка для Fortinet FortiGate:
7

Критерій: Безпека
Оцінка для Cisco ASA:
9
Оцінка для Fortinet FortiGate:
8
```

Рисунок 5.7 – Результат роботи застосунку

```
Критерій: Масштабованість
Оцінка для Cisco ASA:
7
Оцінка для Fortinet FortiGate:
8

Критерій: Вартість
Оцінка для Cisco ASA:
5
Оцінка для Fortinet FortiGate:
7

Критерій: Зручність адміністрування
Оцінка для Cisco ASA:
6
Оцінка для Fortinet FortiGate:
7

Критерій: Підтримка
Оцінка для Cisco ASA:
5
Оцінка для Fortinet FortiGate:
6

Критерій: Інтеграції
Оцінка для Cisco ASA:
7
Оцінка для Fortinet FortiGate:
7

Підсумкові оцінки для кожної альтернативи:
Cisco ASA: 7.4800
Fortinet FortiGate: 7.3700

Найкраща альтернатива: Cisco ASA


** Process exited - Return Code: 0 **
Press Enter to exit terminal
```

Рисунок 5.8 - Результат роботи застосунку

У наведеному прикладі програма визначає, що Cisco ASA є найкращою альтернативою серед двох розглянутих міжмережевих екранів, з підсумковою оцінкою 7.48 проти 7.37 для Fortinet FortiGate. Це базується на введених оцінках за кожним критерієм та заданих вагових коефіцієнтах.

З наведених результатів видно, що програма працює без проблем, основні задачі виконано та основні функції реалізовані вірно.

ВИСНОВКИ

Безпека мережі є однією з найбільш актуальних і важливих проблем сучасного інформаційного середовища. У зв'язку з постійним розвитком технологій зростає також кількість загроз, які ставлять під загрозу конфіденційність, цілісність і доступність даних у мережах різного масштабу. Організації в усьому світі стикаються з серйозними проблемами щодо захисту своїх інформаційних ресурсів від хакерських атак, вірусів, шкідливих програм та інших кіберзагроз. Питання безпеки мережевої інфраструктури стає все більш актуальним, оскільки від цього залежить стабільність функціонування як окремих підприємств, так і критичних національних систем.

Одним із найефективніших інструментів захисту мережі є міжмережевий екран Він слугує першою лінією оборони, контролюючи вхідний і вихідний трафік та запобігаючи несанкціонованому доступу до мережевих ресурсів. Міжмережеві екрани забезпечують можливість фільтрації трафіку, створюючи бар'єри для шкідливих атак, захищають від різноманітних загроз, таких як DDoS-атаки, фішинг, та інші види вторгнень. У сучасному світі вони залишаються ключовим компонентом будь-якої системи безпеки, оскільки можуть бути налаштовані для відповіді на різні типи загроз і забезпечують масштабованість для адаптації до змінних умов.

Однак вибір міжмережевого екрану є складним завданням через велику кількість наявних варіантів та необхідність врахування безлічі технічних і бізнес-критеріїв. Для вирішення цього завдання був обраний метод аналізу ієрархій, який дозволяє систематично підходити до процесу прийняття рішень в умовах багатокритеріальної невизначеності. Метод аналізу ієрархій забезпечує можливість порівняння різних альтернатив шляхом структурування задачі у вигляді ієрархічної

моделі та визначення вагових коефіцієнтів для кожного з критеріїв, що важливі для організації.

У даній роботі розроблена методика вибору засобів побудови системи мережевої безпеки на основі методу аналізу ієрархій, яка враховує такі ключові критерії, як продуктивність, безпека, масштабованість, вартість, зручність адміністрування, підтримка та інтеграція. Методика дозволяє організаціям, враховуючи їхні пріоритети, обрати найкращий варіант міжмережевого екрану. Це досягається шляхом обчислення підсумкових оцінок для кожної альтернативи на основі вагових коефіцієнтів та введених користувачем оцінок. Результатом є можливість визначення найбільш підходящого рішення, яке відповідатиме специфічним вимогам організації.

Для розробленої методики створена програмна реалізація мовою програмування Python. Програма автоматизує процес вибору міжмережевого екрану, приймаючи від користувача необхідні дані про альтернативи та критерії, зчитуючи вагові коефіцієнти з текстового файлу. На основі цих даних програма розраховує підсумкові оцінки для кожної альтернативи та надає рекомендацію щодо найкращого вибору. Завдяки використанню методу аналізу ієрархій, програма здатна забезпечити об’єктивний та зважений процес прийняття рішень, зводячи до мінімуму суб’єктивні впливи на результат.

Під час тестування програмного продукту були отримані успішні результати. Програма коректно обробляла вхідні дані, виводила підсумкові оцінки для кожної альтернативи та визначала найкращий варіант на основі критеріїв, визначених організацією. Тестування показало, що система є надійною і точною у своєму розрахунку, а також забезпечує високий рівень зручності для користувача. Важливо зазначити, що гнучкість програми дозволяє легко змінювати вагові коефіцієнти та критерії, адаптуючи її під різні умови та вимоги.

Результатом роботи є успішно розроблена методика вибору міжмережевого екрану, що базується на методі аналізу ієрархій, а також програмне рішення, яке автоматизує цей процес. Робота демонструє важливість та необхідність структурованого підходу до вибору засобів мережевої безпеки, зокрема міжмережевих екранів, у сучасних умовах. Запропоновані методи та програмне забезпечення дозволяють приймати обґрунтовані рішення та оптимізувати процес захисту мережевої інфраструктури, що сприяє підвищенню загального рівня безпеки організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Мясіщев О. А., Мартинюк О. О., Гіневська Н. М. Аналіз захищеності комп'ютерних мереж на основі побудови дерева атак. *Вісник Хмельницького національного університету*. 2016. С. 243.
2. ISO/IEC 27001:2015. Інформаційні технології. методи захисту системи управління інформаційною безпекою. вимоги. Чинний від 2017-01-01. Вид. офіц. 2015.
3. НД ТЗІ 2.7-009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. Чинний від 2009-07-24. Вид. офіц. Київ, 2009. 231 с.
4. ISO/IEC 7498-1:1994. Information technology – open systems interconnection – basic reference model: the basic model. Чинний від 1994-11-01. Вид. офіц. 1994.
5. Wright B. Colonial System Back On Line After Cyberattack. JPT. Режим доступу:https://jpt.spe.org/colonial-system-back-on-line-after-cyberattack?gad_source=1&gclid=CjwKCAjw3624BhBAEiwAkxgTOpOuHyYuhrryOFuxJDl7CxX2w6Vq4oKXWjduJotS7isC1ofwH05ytBoC1sAQAvD_BwE (дата звернення: 13.10.2024).
6. Чи була кібератака на обленерго? - BBC News Україна. BBC News Україна. Режим доступу: https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc (дата звернення: 13.10.2024).
7. Mohan V. Network Security and Types of Attacks in Network // International Conference on Intelligent Computing, Communication & Convergence. - Procedia Computer Science 48 (2015) 503 – 506.
8. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст] : НД ТЗІ 1.1-003 – 1999. – Чин. 1999. 04.28. – К.: ДСТСЗІ СБ України, 1999. – 12 с.

9. Olifer V.G. Computer networks. Principles, technologists, protocols: Student for universities / V.G. Olifer, N.A. Olifer. - 5th ed. - SPb .: Peter, 2016. – 992 c.
10. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу // НД ТЗІ 1.1–002–99, ДСТСЗІ СБ України, Київ, 1999.
11. Грайворонський М. В. Безпека інформаційно-комунікаційнихсистем: підручник для ВНЗ / М. В. Грайворонський, О. М. Новіков ; М-вопраці та соц. політики України. Держнаглядохоронпраці України. - К. : ВНV, 2009. - 607 с.
12. Fundamentals of computer networks: textbook. allowance / Ed. L.G. Gagarina. - M .: Forum ": INFRA-M, 2012. – 272 c
13. Комплексна безпека інформаційних мережевих систем : навчальний посібник / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. – Тернопіль : Вид-во ТНТУ імені Івана Пулюя , 2016. – 256 с
14. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій. Х. : ХНУ імені В. Н. Каразіна, 2013. 632 с.
15. Whitman M. E. , Mattord H. J. Principles of Information Security, 6th Edition, Cengage Learning, 2017. 656 p.
16. Войтович В.С., Гриник Р.О. Дослідження надійності використання протоколу IPsec для створення VPN. Зб. тез доповідей Всеукраїнська науковопрактична інтернет-конференція ―Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку‖ (м. Черкаси, 13-19 березня 2017 р.). Черкаси, 2017. С. 66-68.
17. Балацька В.С., Шабатура М.М. Сканери вразливості комп'ютерної мережі. Захист інформації в інформаційно-комунікаційних системах: матеріали ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 28 листопада 2019 р. / ЛДУ БЖД. Львів, 2019.С. 34-36.
18. Wiegers K., Beatty J. Software requirements. Pearson Education, 2013. 637 p.

19. Сучасні інформаційно-комунікаційні технології / Г. Г. Швачич та ін. Дніпро : НМетАУ, 2017. 230 с.
20. Тестування та контроль якості (QA) вбудованих систем / І. А. Клименко та ін. Київ : КПІ ім. Ігоря Сікорського, 2022. 75 с.
21. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник. Київ: МК-Прес, 2004. 508 с.
22. Технології забезпечення безпеки мережевої інфраструктури / В. Л. Бурячок та ін. Київ : Київ. ун-т ім. Бориса Грінченка, 2019. 218 с.
23. Заплотинський Б. О. Основи інформаційної безпеки. Конспект лекцій. Київ : КІІВіП НУ “ОЮА”, 2017. 128 с.
24. Рондалєв Д., Нарежній О., Мелкозьорова О. Особливості функціонування корпоративного міжмережевого екрану та питання взаємодії з системою IDS. Харків : ХНУ ім. В.Н. Каразіна, 2019. 11 с.
25. Інформаційна безпека в комп’ютерних мережах / О. А. Смірнов та ін. Кропивницький : ЦНТУ, 2020. 295 с.
26. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека : підручник. Київ : Державний університет телекомунікацій, 2015. 288 с.
27. Жураковський Б.Ю., Зенів І.О. Розробка та реалізація мережних протоколів. Київ : КПІ ім. Ігоря Сікорського, 2020. 462 с.
28. Meghanathan N. Network security. *Network security technologies*. 2014. С. 174–203. Режим доступу: https://doi.org/10.4018/978-1-4666-4789-3.ch011 (дата звернення: 5.10.2024).
29. С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121- 124).

30. Комп'ютерні мережі: навчальний посібник / А.Г. Микитишин та ін. Львів: Магнолія 2006, 2013. 256 с.
31. Iptables tutorial: ultimate guide to linux firewall. *Knowledge Base by phoenixNAP*. Режим доступу: https://phoenixnap.com/kb/iptables-tutorial-linux-firewall (дата звернення: 7.10.2024).
32. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах. Київ : КПІ ім. Ігоря Сікорського, 2020. 213 с.
33. В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Основи інформаційної безпеки : навч. посібник. Дніпро : ДДУВС, 2020. 128 с.
34. Viega J., Howard M., LeBlanc D. 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. McGraw-Hill Osborne Media, 2005, 304 p.
35. Cisco IOS Quality of Service Solutions Configuration Guide. Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c.html (дата звернення: 8.10.2024).
36. Олещенко Л. М. Організація комп'ютерних мереж. Конспект лекцій. Київ : КПІ ім. Ігоря Сікорського, 2018. 225 с.
37. НД ТЗІ 2.5-004-99 — Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Режим доступу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf (дата звернення: 13.10.2024).
38. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Чинний від 1999-04-28. Вид. офіц. Київ : ДСТСЗІ СБ України, 1999. 21 с.
39. Матов О. Я. Модель загроз у розподілених мережах. Київ : Національний авіаційний університет, 2008. 92 с.

40. Корпань Я. В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. Черкаси, 2015. С. 1-8. Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131565/04-Korpan.pdf?sequence=1 (дата звернення: 11.10.2024).
41. Про електронні комунікації : Закон України від 16.12.2021 № 3549-1. Режим доступу: https://ips.ligazakon.net/document/JH2QL1AA?an=3 (дата звернення: 13.10.2024)
42. Lewis M. Comparing, Designing, And Deploying VPNs. Indianapolis: Cisco Systems, 2006. 1043 с.
43. Здещиц В. М., Здещиц А. В. Використання технології BYOD в освітньому процесі в умовах дистанційного навчання студентів-фізиків: навч. посібник. Кривий Ріг: Вид. Літерія, 2022. – 185 с.
44. Січко Т., Нескородєва Т., Римар П. (2022). МЕТОДИ ТА МОДЕЛІ ПРИЙНЯТТЯ РІШЕНЬ В УМОВАХ НЕВИЗНАЧЕНОСТІ. Computer Systems and Information Technologies, с. 47–51.
45. Манталюк, О. В. Застосування методу аналізу ієрархій до задач прийняття економічних рішень в умовах невизначеності цілей [Текст] / О. В. Манталюк // Вісник Хмельницького національного університету. Економічні науки. – 2014. – № 4, т. 2. – С. 272-275.
46. Žižović, M., Miljković, B., & Marinković, D. (2020). Objective methods for determining criteria weight coefficients: A modification of the CRITIC method. Decision Making: Applications in Management and Engineering, p.149–161.

ДОДАТОК А

Вихідний код програмної реалізації запропонованої методики

```
import numpy as np


def read_weights(file_path):
    """
    Зчитування вагових коефіцієнтів з файлу.
    Повертає список критеріїв та їх ваг.
    """
    criteria = []
    weights = []
    try:
        with open(file_path, 'r', encoding='utf-8') as file:
            for line in file:
                parts = line.strip().split(',')
                if len(parts) != 2:
                    print(f"Некоректний рядок у файлі: {line.strip()}")
                    continue
                criteria.append(parts[0].strip())
```

```
            weights.append(float(parts[1].strip()))
    except FileNotFoundError:
        print(f"Файл {file_path} не знайдено.")
        exit(1)
    except ValueError:
        print("Вага повинна бути числовим значенням.")
        exit(1)

    # Перевірка суми ваг
    total_weight = sum(weights)
    if not np.isclose(total_weight, 1.0):
        print(f"Сума ваг {total_weight} не дорівнює 1.0. Будь ласка, перевірте файл ваг.")
        exit(1)
    return criteria, weights


def get_alternative_names():
    """
    Отримання назв альтернатив від користувача.
    """
    alternatives = []
    print("Введіть назви двох альтернативних міжмережевих екранів:")
```

```
    for i in range(1, 3):
        name = input(f"Назва Альтернативи {i}: ").strip()
        if not name:
            print("Назва не може бути порожньою.")
            exit(1)
        alternatives.append(name)
    return alternatives


def get_scores(criteria, alternatives):
    """
    Отримання оцінок альтернатив за кожним критерієм від користувача.
    """
    scores = {alternative: [] for alternative in alternatives}
    print("\nВведіть оцінки для кожної альтернативи за кожним критерієм (від 1 до 9):")
    for criterion in criteria:
        print(f"\nКритерій: {criterion}")
        for alternative in alternatives:
            while True:
                try:
                    score = float(input(f"Оцінка для {alternative}: "))
                    if score < 1 or score > 9:
```

```
                print("Оцінка повинна бути між 1 і 9. Спробуйте ще раз.")
                continue
            scores[alternative].append(score)
            break
        except ValueError:
            print("Будь ласка, введіть числове значення.")
    return scores

def calculate_final_scores(scores, weights, criteria):
    """
    Розрахунок підсумкових оцінок для кожної альтернативи.
    """
    final_scores = {}
    for alternative, alt_scores in scores.items():
        total_score = sum([score * weight for score, weight in zip(alt_scores, weights)])
        final_scores[alternative] = total_score
    return final_scores

def main():
    # Зчитування вагових коефіцієнтів з файлу
    weights_file = 'weights.txt'
```

```
    criteria, weights = read_weights(weights_file)

    # Отримання назв альтернатив від користувача
    alternatives = get_alternative_names()

    # Отримання оцінок від користувача
    scores = get_scores(criteria, alternatives)
    # Розрахунок підсумкових оцінок
    final_scores = calculate_final_scores(scores, weights, criteria)

    # Виведення підсумкових оцінок
    print("\nПідсумкові оцінки для кожної альтернативи:")
    for alternative, score in final_scores.items():
        print(f"{alternative}: {score:.4f}")

    # Вибір найкращої альтернативи
    best_alternative = max(final_scores, key=final_scores.get)
    print(f"\nНайкраща альтернатива: {best_alternative}")

if __name__ == "__main__":
    main()
```