МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ЕКОНОМІКО-ПРАВОВИЙ ФАКУЛЬТЕТ
КАФЕДРА СИСТЕМНОГО АНАЛІЗУ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

До захисту допустити:
В.о. зав. кафедри

Ганна МАРТИНЮК

«04» червня 2025 р.

«ПРИКЛАДНИЙ ПРОГРАМНИЙ ІНТЕРФЕЙС ДЛЯ МАРШРУТИЗАТОРА CISCO»

Кваліфікаційна робота
здобувача вищої освіти першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми
«Комп'ютерні науки»
Оксова Данила Григоровича
Науковий керівник:
Дрейс Юрій Олександрович,
кандидат технічних наук, доцент,
доцент кафедри системного аналізу та
інформаційних технологій
Рецензент:
Нечипорук Олена Петрівна,
доктор технічних наук, професор,
завідувач кафедри інтелектуальних кібернетичних систем Державного університету «Київського авіаційного університету»

Кваліфікаційна робота захищена
з оцінкою задовільно 67 (D)
Секретар ЕК

«11» червня 2025 р.

Київ – 2025

ЗМІСТ

ВСТУП

Стрімкий поступ мережевих технологій та ускладнення сучасних мереж ставлять перед дослідниками, освітянами й фахівцями нові виклики. Для успішного проектування, оптимізації та забезпечення безпеки мережевих інфраструктур необхідні високоякісні інструменти й методології, здатні ефективно моделювати та емулювати різні сценарії. Проте багатий вибір доступного програмного забезпечення, кожне з унікальними функціями, можливостями та обмеженнями, значно ускладнює визначення найбільш підходящого рішення для конкретних завдань чи проектів.

У цьому контексті підкреслюється потреба у ґрунтовному аналізі інструментів для моделювання та емуляції мереж, що дозволить зацікавленим сторонам приймати обґрунтовані рішення. Відсутність чітких критеріїв та методів оцінювання таких інструментів часто спричиняє неефективність, неоптимальні рішення, а також упущення можливостей для впровадження інновацій і досягнення прогресу в галузі досліджень і розробок. Тому актуальність обраної теми пов’язана зі швидким розвитком мережевих технологій, коли зростає попит на програмні засоби, які можуть адаптуватися до нових викликів, забезпечувати масштабованість і точно відображати реалії сучасних мережевих середовищ.

Об’єктом кваліфікаційної роботи є дослідження актуальних проблем побудови комп’ютерних мереж, а також програмних засобів моделювання та емуляції мережі.

Предметом роботи є реалізація за допомогою середовища моделювання Cisco Packet Tracer методу блокування інформаційного ресурсу , який є частиною інформаційного простору України.

Мета роботи – проаналізувати існуючи методи та інструменти побудови і адміністрування комп’ютерних мереж, а також дослідити можливості Cisco Packet Tracer в реалізації методів блокування за допомогою прикладного програмного інтерфейсу маршрутизатора Cisco.

Для досягнення поставленої мети слід виконати такі завдання:

- Провести аналітичний огляд предметної області;

- Здійснити аналіз існуючих аналогів, призначених для блокування інформаційних ресурсів.

- Реалізувати метод блокування інформаційного ресурсу за допомогою програмного інтерфейсу маршрутизатора Cisco.

РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД ПРИНЦИПІВ ТА ІНСТРУМЕНТІВ ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

Нова технічна революція сприяла розвитку сучасних мережевих технологій. Сьогодні комп'ютерна мережа навіть того ж підприємства дозволяє набагато швидше і краще обмінюватися інформацією між різними його структурними підрозділами, прискорює рух документообігу, дозволяє користуватися інформацією та змінювати і оновлювати її в режимі реального часу.

1.1 Аналіз сучасних принципів побудови мережі

Комп'ютерна мережа — це система, яка об'єднує комп'ютери та інші пристрої для обміну інформацією між учасниками мережі без застосування додаткових фізичних носіїв даних.

Комп'ютерні мережі можна класифікувати за кількома основними критеріями:

1. Територіальна поширеність.
2. Приналежність за відомством.
3. Швидкість передачі даних.
4. Тип середовища передачі.

Типи мереж за територіальною поширеністю

- Локальні мережі - охоплюють невелику територію, зазвичай до 10 м².
- Регіональні мережі - покривають площу міста або області.
- Глобальні мережі - забезпечують зв'язок на рівні держав або навіть міжнародному масштабі. Прикладом глобальної мережі є Інтернет.

Приналежність

- Відомчі мережі створюються для використання в межах однієї організації та працюють на її території.
- Державні мережі використовуються урядовими установами для виконання їхніх функцій.

Швидкість передачі інформації

За цим критерієм мережі поділяють на:

- Низькошвидкісні,

- Середньошвидкісні,
- Високошвидкісні.

Тип середовища передачі

Мережі розрізняють за типом фізичного середовища, яким передають дані:

- Коаксіальні кабелі,
- Кабелі типу "витої пари",
- Оптоволоконне з'єднання,
- Радіоканали,
- Інфрачервоне випромінювання.

Комп'ютери в мережах можуть з'єднуватися різними способами, формуючи різні топології, такі як "зірка", "шина", "кільце" тощо.

Відмінності між комп'ютерними й термінальними мережами.

Комп'ютерні мережі забезпечують об'єднання комп'ютерів, кожен з яких може працювати повністю автономно. Натомість термінальні мережі з'єднують потужні обчислювальні пристрої (наприклад, мейнфрейми чи деякі персональні комп'ютери) із терміналами. Останні залежать від мейнфреймів і втрачають свою функціональність у випадку відсутності зв’язку з мережею.

Приклади термінальних мереж включають банкомати або системи продажу авіаквитків. Ці системи побудовані на інших принципах, ніж комп'ютерні мережі, і використовують відмінне обладнання та технології.

Зазвичай у класифікації мереж виділяють два основних типи: LAN і WAN.

1. LAN (Local Area Network) – це локальні мережі, що обмежені закритою інфраструктурою без виходу до зовнішніх постачальників послуг. LAN може охоплювати як невелику офісну мережу, так і велику мережу рівня підприємства, що простягається на кілька сотень гектарів. За західними стандартами зона високошвидкісного покриття LAN приблизно становить до 10 км у радіусі. Ці мережі зазвичай фізично прив'язані до одного об'єкта, наприклад, будівлі чи комплексу будівель, об'єднуючи комп'ютерні системи та пристрої. LAN об'єднують такі елементи, як жорсткі накопичувачі, стримери, принтери та інші периферійні пристрої в єдину систему для спільного використання даних і

ресурсообміну. Основні переваги локальних мереж – висока швидкість передачі даних, мінімальний рівень помилок та економічна ефективність завдяки дешевим засобам комунікації.

2. WAN (Wide Area Network) – це глобальна мережа, яка покриває великі території і може включати в себе локальні мережі (LAN), міські мережі (MAN) та інші телекомунікаційні системи. Прикладом WAN можуть бути мережі, такі як Frame Relay, що дозволяють взаємодію між різними комп’ютерними мережами. WAN може охоплювати цілі регіони, країни або навіть континенти. Для організації зв'язку в мережі зазвичай використовують телефонні лінії, супутниковий зв'язок, радіорелейні або мікрохвильові системи. Часто WAN створюють через об’єднання кількох LAN і MAN у єдину структуру, що є загальною тенденцією в сучасній сфері мережевих технологій.

WAN є комбінацією безлічі різноманітних технологій, тому їх можна умовно розглядати як багатокомпонентну інфраструктуру. У порівнянні з LAN глобальні мережі мають значно нижчу швидкість передачі даних та схильні до більшого рівня помилок. Однак новітні розробки у сфері WAN орієнтовані на вирішення цих проблем, спрямовуючи галузь на подальший розвиток.

У сфері побудови комп'ютерних мереж існує декілька загальноприйнятих підходів. Один із найтрадиційніших — це ієрархічна архітектура мережі, яка заснована на моделі взаємодії відкритих систем (OSI). Він передбачає розподіл мережі на різні рівні, кожен з яких виконує свою специфічну функцію. Попри свою популярність, цей метод стикається з певними обмеженнями, такими як негнучкість і складності при розширенні.

Інший спосіб, що здобув широке визнання останнім часом, це хмарні мережі. Вони використовують технології хмарних обчислень для створення і управління мережами, пропонуючи зручний доступ до спільного пулу обчислювальних ресурсів. Хмарні мережі мають безліч переваг: масштабованість, гнучкість і економічна ефективність; однак вони також стикаються з викликами у сфері безпеки та можливими проблемами продуктивності.

Програмно-визначена мережа (SDN) є відносно новим підходом, що отримав значну увагу останніми роками. Цей метод передбачає відокремлення керування мережею від передачі даних, що забезпечує централізоване та програмне управління. SDN дозволяє значно підвищити гнучкість і масштабованість, проте вимагає спеціалізованих навичок і може мати певні ризики безпеки. Незважаючи на ці труднощі, SDN стає все більш популярною і очікується, що вона відіграє значну роль у розвитку комп'ютерних мереж у майбутньому.

SDN розділяє керуючу площину (контролер та програмні програми) від площини передачі (мережні пристрої). Таке розмежування дозволяє керувати за допомогою програмного забезпечення інфраструктурою мережі.

Управління:

Контролер SDN виконує координацію роботи мережі, збираючи інформацію про її стан та передаючи команди мережевим пристроям для виконання завдань.

Програмна конфігурація:

SDN надає можливість налаштовувати мережні пристрої програмно, що автоматично спрощує керування мережею та прискорює процеси автоматизації.

Гнучкість та динамічність:

Завдяки SDN мережі здатні оперативно реагувати на вимоги, що змінюються, додавати нові сервіси і ефективно оптимізувати маршрути передачі даних.

Переваги SDN:

Спрощення управління:

SDN дозволяє значно знизити обсяг ручного налаштування, спростити адміністрування та скоротити експлуатаційні витрати.

Покращена автоматизація:

Технологія дозволяє автоматизувати безліч мережевих операцій, включаючи маршрутизацію, балансування трафіку та забезпечення безпеки.

Підвищена гнучкість:

SDN забезпечує адаптивність, що полегшує реалізацію нових вимог відповідно до зміни бізнес-цілей.

Використання віртуалізації:

SDN активно застосовує технології віртуалізації для створення ізольованих логічних мереж, що буде корисним при розмежуванні трафіку між різними бізнес-додатками.

Застосування SDN:

Хмарні послуги:

Хмарні провайдери використовують SDN для організації віртуальних мереж та підвищення рівня безпеки своїх інфраструктур.

Корпоративні мережі:

SDN для корпоративних мереж дозволяє досягти кращої керованості та підвищити гнучкість використовуваних рішень.

Мережі для ЦОДів:

Центри обробки даних активно впроваджують SDN для забезпечення надійності роботи та масштабування своєї інфраструктури.

Територіально-розподілені мережі:

SDN дає можливість створювати динамічні та гнучкі мережі, що охоплюють різні географічні регіони.

Приклад SDN-контролера:

Одним із найбільш популярних протоколів SDN виступає OpenFlow, який служить для взаємодії між контролером та мережевими пристроями.

1.2 Огляд програмних продуктів для моделювання мереж

У сучасній сфері комп'ютерних мереж, яка постійно розвивається, здатність точно моделювати, емулювати та симулювати мережеві середовища має вирішальне значення для просування досліджень, вдосконалення освіти та впровадження інновацій у різні галузі господарювання. Сучасні технології моделювання комп'ютерних мереж надають можливість використовувати ефективні інструменти для аналізу поведінки складних систем, оцінки

ефективності роботи протоколів мережі і тестування впроваджених рішень у контрольованих умовах.

Моделювання мережі відіграє незамінну роль у багатьох галузях, включаючи науку, освіту та промисловість. У дослідницькій діяльності ці методи надають ученим платформи для випробування інновацій, перевірки теорій і проведення тестування запропонованих архітектур, перш ніж вони будуть впроваджені в реальних умовах. за допомогою програмного забезпечення Моделювання різноманітних сценаріїв та робочих умов мережі, дозволяє дослідникам глибше розуміти її динаміку, виявляти можливі вузькі місця і оптимізувати її функціонування та при тому мінімізувати ризики і витрати.

Використання інструментів для моделювання комп'ютерних мереж у навчальних закладах є незамінним засобом для вивчення концепцій, протоколів і технологій у цій галузі. Завдяки експериментам у віртуальних мережевих середовищах студенти мають змогу краще зрозуміти принципи роботи мереж, розвинути необхідні навички конфігурування та усунення несправностей, а також дослідити вплив різних параметрів на загальну продуктивність системи. Ці платформи сприяють командному навчанню і спільній роботі над мережевими проектами, незалежно від географічного розташування учасників.

У промисловому секторі інструменти для моделювання комп'ютерних мереж широко застосовуються для планування, тестування і вдосконалення інфраструктури мережі, сервісів та додатків. Моделюючи реалізацію мереж або різні сценарії їх використання, організації оцінюють ефективність нових проектів, прогнозувати продуктивність технологій, а також заздалегідь виявляти слабкі місця чи потенційні загрози безпеці до внесення змін у реальні робочі середовища. Такі інструменти дозволяють інженерам, користувачам та адміністраторам тестувати вплив мережевих збоїв, пікових завантажень трафіку чи інших критичних ситуацій, що сприяє покращенню можливості оцінцювання стійкості та надійності мережевих архітектур та протоколів мережі.

Метою дослідження мережевих архітектур є аналіз функціональності, продуктивності й особливостей програмних засобів моделювання для їхнього

подальшого використання в освітніх, дослідницьких і промислових цілях. Основні завдання дослідження включають:

- оцінку широти можливостей, зручності у використанні та масштабованості обраних інструментів для мережевого моделювання;

- порівняння між собою кожного інструменту щодо, швидкості роботи, створення точних моделей та здатності підтримувати різноманітні мережеві сценарії;

- визначення потенційних сфер застосування досліджених інструментів у таких сферах, як освіта, наука та промисловість.

До списку програмного забезпечення, відібраного для аналізу, увійшли як комерційні продукти, так і інструменти з відкритим кодом: Cisco Packet Tracer, Cisco VIRL, UNetLab, Pnet Lab, EVE-NG, Boson NetSim, IMUNES, OPNET SIMULATOR, eNSP, CML, D-Link TP-Link simulator, NS-3, GNS3, OMNeT++, Mininet, QualNet, CORE тощо. Вибір цих інструментів здійснювався з урахуванням їхньої популярності серед фахівців у цій галузі та широкою функціональністю для вирішення завдань із моделювання мереж.

Відбір програмного забезпечення базувався на кількох важливих критеріях:

1. Функціональність. Інструменти повинні забезпечувати комплексний набір можливостей для моделювання мереж із підтримкою різноманітних протоколів, типів топологій і сценаріїв роботи.
2. Простота у використанні: Зручний інтерфейс та зрозумілий дизайн забезпечують доступність та легкість використання програмних інструментів. Це особливо важливо для користувачів із різними рівнями технічної підготовки, включаючи таких як дослідники, викладачі і професіонали галузі.
3. Масштабованість: Програмні засоби повинні підтримувати симуляції широкого діапазону складності: від невеликих мережевих конфігурацій до великих корпоративних середовищ.

4. Багатозадачність: Можливість одночасного виконання декількох симуляцій та ефективного керування обчислювальними ресурсами є критичною для підвищення продуктивності й пропускної здатності.
5. Доступність: Пріоритет віддається програмним продуктам, які легко доступні, добре задокументовані та мають активну підтримку розробників чи спільноти користувачів.
6. Ефективність програмного забезпечення оцінюється за кількома визначеними критеріями:
7. Швидкість моделювання: тривалість, необхідна для виконання симуляції та отримання результатів.
8. - Точність: відповідність отриманих результатів реальним даним або теоретичним очікуванням.
9. - Використання ресурсів: обсяг споживання процесорного часу, пам’яті та дискового простору.
10. - Надійність: стабільність і стійкість роботи інструменту за різних умов і сценаріїв.
11. - Зручність використання: простота, доступність і зрозумілість інтерфейсу й робочого середовища.

Ці параметри служать основою для кількісної оцінки й порівняння ефективності кожного програмного рішення. Це допомагає ухвалювати обґрунтовані рішення, базуючись на об’єктивних даних і емпіричних результатах досліджень.

Cisco Packet Tracer

Cisco Packet Tracer – це програмний інструмент для моделювання мереж, створений компанією Cisco Systems з метою навчання мережевих технологій (особливо тих, що базуються на Cisco). [8]

Packet Tracer забезпечує візуальний інтерфейс для створення, конфігурації та моделювання мережевих топологій. У ньому доступний широкий асортимент мережевих пристроїв і модулів, які дозволяють користувачам практикувати сценарії налаштування пристроїв та протоколів. [10]

Платформа підтримує поширені мережеві протоколи, характерні для середовищ Cisco, зокрема TCP/IP, UDP, IPv4/IPv6, OSPF, EIGRP і VLAN. [9]

Користувачі можуть створювати різноманітні мережеві структури – від локальних до глобальних мережевих топологій. За допомогою функції "перетягування" можна легко додавати пристрої та підключати їх імітованими кабелями.

Packet Tracer оптимізовано для освітніх цілей і підходить для проєктування малих і середніх мереж. Хоча щодо продуктивності він поступається професійним інструментам, це стабільний вибір для навчання основ мережевого адміністрування.

Інтуїтивний інтерфейс робить Packet Tracer доступним навіть для новачків. Він пропонує інтерактивні можливості симуляції та виконання керованих завдань, які допомагають опановувати налаштування обладнання й протоколів.

Cisco активно надає матеріали для навчання – інструкції, відеоуроки та посібники користувача. Завдяки широкій популярності серед освітніх закладів також легко знайти додаткові ресурси онлайн і отримати допомогу у спільноті користувачів.

Packet Tracer безкоштовно доступний для завантаження

Cisco Virtual Internet Routing Lab (VIRL) є спеціалізованою платформою для моделювання мереж від Cisco Systems. Вона забезпечує віртуальне середовище для дослідження мережевих пристроїв і протоколів Cisco. [8]

VIRL дає змогу створювати складні мережеві топології, що складаються з маршрутизаторів, комутаторів та інших пристроїв, із підтримкою таких протоколів маршрутизації, як OSPF, EIGRP і BGP. Також платформа працює з технологіями комутації, включаючи VLAN і STP. Вона підтримує широкий спектр мережевих протоколів, зокрема TCP/IP, UDP, IPv4/IPv6, MPLS тощо, що характерно для екосистеми Cisco. [9]

Це дозволить користуваам налаштовувати різноманітні мережеві топології, починаючи від локальних і закінчуючи глобальними та гібридними мережами. Гнучкість у проектуванні дозволяє створювати навіть складні

ієрархічні структури. Платформа також демонструє високу продуктивність та масштабованість, здатна ефективно обробляти моделі у середніх і великих мережах. Однак продуктивність залежить від виділених апаратних ресурсів і складності топологій.

Зручність використання – одна з ключових переваг VIRL. Інтуїтивний графічний інтерфейс із функцією перетягування спрощує додавання пристроїв і з'єднань для користувачів із різним рівнем досвіду. Також Cisco надає користувачам документацію, включаючи інструкції з налаштування, посібники, відеоуроки та доступ до широкої мережі підтримки й онлайн-спільнот.

Основними перевагами платформи є її відповідність мережевим стандартам і протоколам Cisco, що робить її оптимальним вибором для користувачів, знайомих із цими технологіями. Завдяки багатій документації та інтерактивному інтерфейсу VIRL підходить як для освітнього використання, так і для професійних потреб.

Проте є й недоліки. Модель ліцензування й вартість платформи можуть бути надто високими для окремих користувачів чи невеликих організацій. Крім того, орієнтованість на технології Cisco обмежує застосування платформи для моделювання середовищ інших виробників.

Cisco Modeling Labs (CML) — це інструмент від компанії Cisco Systems, призначений для моделювання мереж. Застосунок дозволяє створювати віртуальне середовище для проектування та тестування складних мережевих сценаріїв.

CML надає можливість користувачам будувати і моделювати мережеві топології з використанням пристроїв та технологій Cisco. Платформа підтримує різноманітні протоколи маршрутизації, технології комутації та мережеві сервіси, що є основними в інфраструктурі Cisco.

CML забезпечує роботу з повним спектром мережевих протоколів, популярних у мережах Cisco, таких як TCP/IP, OSPF, EIGRP, BGP, VLAN та інші.

За допомогою CML користувачі можуть створювати і налаштовувати різноманітні мережеві топології, включаючи архітектури «точка-точка», «зірка»,

«сітка». Зручний графічний інтерфейс дозволяє легко проектувати власні мережеві рішення будь-якої складності.

Платформа відзначається високою продуктивністю й здатна обробляти моделювання великих і складних мережевих сценаріїв. Таким чином продуктивність залежить від апаратного забезпечення хоста та складності симуляції.

Cisco Modeling Labs оснащена зручним графічним інтерфейсом для налаштування та використання мережевих симуляцій. Компоненти платформи інтуїтивно зрозумілі навіть для новачків, що робить її придатною для користувачів різного рівня підготовки.

Cisco забезпечує платформу вичерпними документами, що включають керівництва, інструкції для користувачів і технічні матеріали. Ця документація охоплює всі основні аспекти роботи з програмним забезпеченням: від інсталяції до виконання моделювань.

CML надає реалістичне середовище для тестування мережею із фокусом на технологіях Cisco. Інтуїтивно зрозумілий та зручний графічний інтерфейс підвищує рівень зручності й ефективності роботи навіть для тих, хто тільки починає своє знайомство із системою.

Основним недоліком є фінансово недоступною платформи для окремих дослідників або студентів через комерційну модель ліцензування. Крім того, платформа орієнтована переважно на технології Cisco, що може обмежувати її використання у сценаріях, які виходять за межі екосистеми компанії.

Unified Networking Lab (UNetLab) — це мережевий емулятор з відкритим вихідним кодом, який базується на основі платформ віртуалізації Dynamips та QEMU. Він пропонує можливості для емуляції різноманітних мережевих пристроїв та протоколів.

UNetLab надає користувачам змогу створювати віртуалізовані мережеві середовища, що включають маршрутизатори, комутатори, брандмауери та інші пристрої. Платформа підтримує широкий спектр мережевих протоколів і технологій, зокрема TCP/IP, UDP, VLAN та MPLS.

UNetLab забезпечує підтримку повного набору мережевих протоколів, що активно використовуються у сучасних комп’ютерних мережах. Це робить платформу ідеальною для моделювання різноманітних мережевих сценаріїв.

Підтримувані мережеві топології: Система пропонує високу гнучкість у проєктуванні та конфігуруванні мережевих топологій. Вона підтримує популярні архітектури, як-от hub-and-spoke, mesh і багаторівневі конфігурації, задовольняючи потреби як простих, так і складних проектів.

UNetLab відзначається гарною продуктивністю та здатністю до масштабування, дозволяючи легко моделювати середні й великомасштабні мережеві сценарії. Проте масштабованість напряму залежить від доступних апаратних ресурсів та складності симульованої топології.

Вебінтерфейс UNetLab забезпечує інтуїтивно зрозумілий спосіб управління мережевими топологіями й налаштування симуляцій. Його простота сприяє швидкому освоєнню платформи навіть новачкам.

Платформа пропонує документацію та посібники для користувачів, що полегшують перші кроки у роботі з UNetLab. Проте рівень детальності документації і ресурсів підтримки може не дорівнювати комерційним аналогам.

Pnet Lab – це платформа для моделювання мереж, розроблена компанією PnetLab LLC. Вона надає віртуалізоване середовище для створення та тестування мережевих конфігурацій з використанням реального мережевого обладнання [24].

Pnet Lab дозволяє користувачам емулювати мережеві топології, що складаються з фізичних і віртуальних мережевих пристроїв. Підтримує різні мережеві протоколи і технології, враховуючи TCP/IP, VLAN і MPLS.

Pnet Lab підтримує широкий спектр мережевих протоколів, які зазвичай використовуються в комп’ютерних мережах, що робить його придатним для моделювання різноманітних мережевих сценаріїв і середовищ.

Pnet Lab пропонує гнучкість у проектуванні та конфігуруванні мережевих топологій, підтримуючи різні конфігурації, такі як топологія «вузол – спиця», комірчаста та гібридна архітектури.

Pnet Lab забезпечує хорошу продуктивність і масштабованість для моделювання середньо- і великомасштабних мережевих сценаріїв. Його продуктивність може залежати від апаратних ресурсів, доступних на хост-машині, і складності симуляції.

Pnet Lab пропонує зручний графічний інтерфейс для проектування та управління мережевими топологіями. Він надає інтуїтивно зрозумілі інструменти для додавання пристроїв, налаштування з'єднань і запуску симуляцій.

Pnet Lab надає документацію та посібники користувача, щоб допомогти користувачам розпочати роботу з платформою. Однак наявність вичерпної документації та ресурсів підтримки може відрізнятися від комерційних рішень.

GNS3 (Graphical Network Simulator-3)

GNS3 – це потужний графічний симулятор мереж, створений для моделювання складних мережевих топологій із застосуванням віртуальних машин та реальних мережевих пристроїв.

GNS3 надає інтуїтивно зрозумілий графічний інтерфейс для проєктування і налаштування мережевих топологій. Інтеграція з платформами віртуалізації, такими як VMware і VirtualBox, дозволяє користувачам запускати віртуальні мережеві пристрої для моделювання реальних середовищ.

Програма сумісна з широким спектром мережевих протоколів, включаючи TCP/IP, UDP, IPv4/IPv6, MPLS, BGP і OSPF. Також забезпечується підтримка популярних операційних систем, таких як Cisco IOS і Juniper JunOS.

GNS3 підтримує створення складних мережевих топологій, включаючи віртуальні маршрутизатори, комутатори, брандмауери та інші мережеві компоненти. Серед доступних конфігурацій є topologies типу hub-and-spoke, full-mesh та ієрархічні топології.

GNS3 здатен моделювати мережі середнього та великого масштабу залежно від обчислювальних ресурсів хост-машини. Висока продуктивність залежить від потужності обладнання, виділеного для симуляції.

Завдяки зручному інтерфейсу GNS3 значно спрощує створення і налаштування топологій за допомогою функції перетягування елементів. Користувачі можуть легко додавати пристрої та підключати їх за допомогою віртуальних кабелів.

GNS3 пропонує розширену документацію, яка містить детальні інструкції зі встановлення, підручники та посібники. Активні форуми спільноти та численні онлайн-ресурси забезпечують додаткову підтримку користувачам.

Висновки до І розділу

У процесі вивчення питання побудови комп'ютерних мереж було проведено огляд та аналіз сучасних методів і технологій створення та адміністрування мереж. Розглянуто варіанти масштабування, забезпечення захисту від зловмисників і інших загроз, а також визначено шляхи вирішення цих проблем із врахуванням їхніх особливостей, переваг та недоліків.

Комплексний огляд різноманітних програмних продуктів для моделювання мереж надає важливу інформацію про їх функціональність, особливості використання та вплив на реальні сценарії. Кожен інструмент має унікальні можливості й функції, які відповідають окремим потребам користувачів у дослідницькій або навчальній чи промисловій діяльності.

Серед широкого спектра рішень виділяються такі продукти, як Cisco VIRL, UNetLab, EVE-NG і GNS3, які стали універсальними платформами для проектування, тестування мережевих архітектур. Ці інструменти пропонують багатий функціонал, включаючи графічні інтерфейси, підтримку віртуалізованих середовищ і великі бібліотеки мережевих пристроїв. Вони чудово вписуються в різні завдання, як-от міграція центрів обробки даних, оптимізація мережі та тестування протоколів. [15]

Для практичного навчання особливо підходять такі програми, як Boson NetSim, Cisco Packet Tracer і eNSP. Вони дозволяють інтерактивно виконувати лабораторні завдання, моделювати мережі з високою реалістичністю та вивчати технології Cisco. Це робить їх ідеальною платформою для здобуття практичних навичок і сертифікації. [12]

Для проведення досліджень і розробки нових мережевих технологій особливу цінність мають IMUNES, OPNET і Pnet Lab. Вони пропонують широкий спектр можливостей для експериментів із протоколами, аналізу продуктивності та оптимізації мережевих рішень. Завдяки адаптованим симуляційним середовищам ці інструменти дозволяють дослідникам випробовувати та аналізувати нові технології в есперементальних умовах. [18]

NS-3, OMNeT++ і Mininet є потужними інструментами моделювання для досліджень у сферах бездротових сенсорних мереж, мобільних ad hoc мереж і кібербезпеки. Вони забезпечують гнучке налаштування моделей, підтримку реалізації протоколів і детальний аналіз продуктивності. Завдяки цьому можна оцінювати складну поведінку систем і тестувати нові рішення у сфері мережевих технологій.

Під час вибору програмного забезпечення важливо враховувати конкретні цілі й вимоги проекту, масштаб завдань і рівень підготовки користувачів. Ключові етапи цього процесу включають визначення потреб та умов використання, вивчення характеристик ринку й аналіз функціональних можливостей програмного забезпечення. Також необхідно оцінити продуктивність, інтеграцію з іншими системами, доступну документацію, витрати та зручність використання.

Інструменти для моделювання мереж мають великий потенціал для вирішення завдань, пов’язаних із проектуванням, тестуванням, оптимізацією, освітньою діяльністю та дослідженнями. Їхнє правильне застосування сприяє успішному виконанню проектів будь-якої складності.

Майбутні дослідження можуть бути спрямовані на подоланні існуючих обмежень шляхом створення більш зручних і інтуїтивно зрозумілих інтерфейсів, підвищення ефективності, збільшення масштабованості та покращення сумісності з різними мережевими середовищами та технологіями.

Розглянуті програмні рішення знаходять широке застосування в різноманітних реальних сценаріях і галузях, таких як телекомунікації, кібербезпека, освіта, наукові дослідження та розробки. Наприклад:

- У телекомунікаціях ці інструменти можуть бути використані для розробки та оптимізації інфраструктури мережі, тестування нових протоколів зв’язку, а також для виявлення і усунення мережевих несправностей.

- У кібербезпеці вони сприяють моделюванню кібератак, перевірці заходів захисту та оцінці стійкості мереж до загроз і вразливостей.

- В освітній сфері ці інструменти можуть забезпечити краще практичне навчання через різноманітні лабораторні завдання, допомогти у підготовці до отримання сертифікацій у галузі мережевих технологій і підтримати освітні програми.

РОЗДІЛ 2. ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖІ

Дослідження та аналіз численних випадків інформаційного впливу та несанкціонованого доступу свідчать, що всі такі ситуації можна поділити на дві основні категорії: випадкові та навмисні. Щоб ефективно розробити засоби захисту інформації, необхідно визначити природу загроз, їхні форми, а також можливі шляхи виникнення та реалізації в системах. Для вирішення цього завдання всі різновиди загроз і шляхи їх впливу зводяться до базових форм, які відповідають їхнім численним проявам у системі.

На основі аналізу практичного досвіду проектування, створення, тестування та експлуатації систем було встановлено, що інформація під час введення, обробки та зберігання або передачі може бути піддана різноманітним випадковим впливам. Серед основних причин таких впливів виділяють:

– недбалість або неуважність персоналу;

– використання неліцензованого програмного забезпечення;

– DDoS-атаки (Distributed Denial-of-Service);

– віруси та шкідливе ПЗ;

– загрози з боку партнерів чи співвласників бізнесу;

– законодавчі суперечності;

– інші непередбачувані дії.

Навмисні загрози, як правило, пов’язані з людським фактором і можуть бути викликані невдоволенням матеріальним становищем, проблемами в особистому житті або, наприклад, прагненням перевірити власні навички, що характерно для хакерів. Без сумніву, організації майже неминуче зіткнуться зі спробами навмисного чи випадкового втручання у мережі. У зв’язку з цим ключовим є своєчасне впровадження ефективних заходів захисту.

У рамках обчислювальних систем можна виділити такі основні штатні канали доступу до інформації:

– користувацькі термінали, серед яких найбільш поширеними є робочі станції;

– термінал адміністратора системи;

– термінал оператора функціонального контролю;

– прилади для відображення інформації;

– засоби завантаження програмного забезпечення;

– засоби документування даних;

– носії інформації;

– зовнішні канали зв’язку.

2.1 Поняття інформаційної безпеки

Інформаційна безпека підприємства або компанії передбачає комплекс організаційних та технічних заходів, спрямованих на захист інформації, її ключових елементів, а також обладнання й систем, що забезпечують роботу з інформацією, її зберігання та передачу. Цей комплекс охоплює використання технологій, стандартів і методів управління інформацією, які гарантують її надійний захист.

Механізми забезпечення інформаційної безпеки спрямовані на охорону як самої інформації, так і інформаційної інфраструктури підприємства від шкідливих впливів. Такі загрози можуть бути навмисними або випадковими, походити як із внутрішніх джерел, так і із зовнішніх. Наслідком подібних втручань може стати втрата важливої інформації, її несанкціонована модифікація або використання сторонніми особами. Тому інформаційна безпека є ключовим компонентом у захисті бізнесу та забезпеченні його безперебійної діяльності.

Основні принципи впровадження систем інформаційної безпеки у компанії включають:

- конфіденційність;

- цілісність;

- доступність.

Конфіденційність передбачає організацію ефективного контролю для гарантування належного рівня захисту даних, активів та іншої інформації на всіх етапах бізнес-процесів. Це дозволяє запобігти несанкціонованому або небажаному розголошенню інформації. Дотримання конфіденційності є обов’язковим як під час зберігання, так і передачі даних будь-якого формату.

Цілісність охоплює механізми управління, що забезпечують узгодженість і достовірність даних як у межах організації, так і поза її межами. Гарантування цілісності дозволяє уникнути спотворення чи пошкодження даних на будь-якому етапі бізнес-операцій.

Доступність забезпечує повноцінний і своєчасний доступ до інформації для персоналу, який має відповідні повноваження. Важливим аспектом тут є стабільність та передбачуваність роботи мережевих середовищ, щоб потрібні дані могли бути отримані у потрібний момент. Одним зі значущих чинників доступності є можливість оперативного та повного відновлення роботи систем у разі збоїв, що дозволяє мінімізувати їх вплив на діяльність компанії.

2.2 Характеристика загроз в інформаційній безпеці

Загрози інформаційній безпеці представляють собою будь-які події, дії чи процеси, які можуть призвести до порушення конфіденційності, цілісності або доступності інформації, пошкодження систем чи порушення їхньої роботи. До найбільш поширених загроз належать несанкціонований доступ, витік даних, шкідливе програмне забезпечення, збої у роботі програм і апаратури, а також негативні наслідки стихійних лих.

Загрози інформаційній безпеці компанії можуть виникати у досить неочікуваний спосіб, а саме через дії звичайних співробітників, які часто не мають жодного злого умислу чи наміру викрасти важливі дані. Ненавмисні інциденти, пов’язані із витоком конфіденційних даних, здебільшого виникають через необережність або недостатню обізнаність працівників стосовно правил інформаційної безпеки. Наприклад, випадкове відкриття фішингового листа може завдати шкоди, перенісши шкідливе програмне забезпечення з особистого ноутбука на сервер компанії. Або ж співробітник може скопіювати конфіденційний файл на планшет, флешку чи інший пристрій для використання під час відрядження, що значно підвищує ризик витоку даних. Крім того, жіночий фактор, як-от відправлення файлів на невідповідну адресу через необачність, також може стати причиною проблем. У таких умовах секретна інформація стає легкою здобиччю для сторонніх зловмисників.

Окремою проблемою залишається економія на ліцензійному програмному забезпеченні. Використання неліцензійних продуктів не тільки не гарантує безпеки від атак, а й створює додаткові ризики крадіжки даних через вбудовані віруси. До того ж власник такого ПЗ позбавляє себе можливості отримати технічну підтримку та оновлення від розробників. Неформальними дослідженнями Microsoft встановлено, що у 7% програмного забезпечення без ліцензії було знайдено шкідливі компоненти для викрадення паролів і персональних даних. Таким чином, прагнення заощадити може призвести до значно більших втрат.

Окрему небезпеку становлять DDoS-атаки (розподілена відмова в обслуговуванні). Механізм цих атак базується на потоках помилкових запитів від численних географічно розподілених хостів. Вони блокують ресурс двома основними способами: через прямий вплив на канал зв'язку шляхом перевантаження зайвими даними або через атаку самого серверу. Наслідками таких нападів часто є недоступність або значне погіршення роботи веб-сервісів, що може тривати від кількох годин до кількох днів. Зазвичай DDoS-атаки застосовуються у конкурентній боротьбі, для вимагання викупу чи як спосіб відволікання уваги від інших протиправних дій, наприклад викрадення коштів із рахунків. За словами експертів, саме фінансова вигода найчастіше мотивує замовників таких атак. Особливо часто мішенями стає програмне забезпечення банківських установ – у близько половині зареєстрованих випадків вони зазнавали основного удару.

Домінуючою та найнебезпечніших загроз інформаційній безпеці сьогодні вважаються комп'ютерні віруси, що призводять до багатомільйонних збитків для компаній унаслідок кібератак. Зокрема, останніми роками значно зросла як частота таких атак, так і їхній економічний вплив. Експерти пояснюють це появою нових шляхів поширення вірусів. Найбільш вразливим каналом залишається електронна пошта, проте в сучасних умовах віруси все частіше проникають через месенджери на кшталт Telegram чи Viber. Окрім цього, збільшився перелік можливих об’єктів для таких злочинів. В попередні часи,

основними цілями були сервери веб-служб, то нині до вірусних атак піддаються між мережеві екрани, мобільні пристрої та маршрутизатори. Окремо варто згадати віруси-шифрувальники, активність яких помітно зросла. Наприклад, навесні та влітку 2017 року велика кількість користувачів постраждали від атак вірусів WannaCry, Petya та Misha. Ці випадки показали, що стати жертвою можна навіть не відкриваючи підозрілих листів. За даними Intel, вірус WannaCry уразив 530 тисяч комп'ютерів у всьому світі, а сумарні збитки перевищили 1 мільярд доларів. [3]

Загрози від співробітників компанії. Легальні користувачі нерідко стають джерелом витоків інформації у компаніях. Такі випадки називаються інсайдерськими атаками, а самих інсайдерів поділяють на такі категорії:

"Порушники" – це співробітники середньої ланки або топ-менеджери, які нехтують правилами інформаційної безпеки. Вони можуть використовувати робочі комп’ютери для ігор, онлайн-покупок або доступу до особистої електронної пошти. Хоча такі дії зазвичай не мають злого умислу, вони часто стають причиною інцидентів, наприклад, через завантаження шкідливих файлів із особистих поштових скриньок чи месенджерів.

"Злочинці" – це посадовці або працівники, які мають доступ до конфіденційної інформації й використовують його для порушення правил. Вони можуть самовільно встановлювати на робоче обладнання стороннє програмне забезпечення чи передавати чутливі дані зацікавленим третім сторонам.

"Кроти" – це співробітники, які зумисно викрадають важливу інформацію за грошову винагороду від конкурентів. Зазвичай це технічно обізнані користувачі, які ретельно приховують свої сліди, що значно ускладнює їхнє викриття.

Також існує група звільнених чи незадоволених працівників, які після розриву з компанією виносять із собою всі дані, до яких мали доступ. У більшості випадків ці дані згодом використовуються на їхньому новому місці роботи.

Законодавчі труднощі. Державні органи мають право конфісковувати обладнання і носії інформації під час перевірок. Оскільки ключова частина

корпоративних даних зберігається на серверах, тимчасове вилучення такого обладнання може паралізувати діяльність компанії. Затримка перевірки призводить до значних фінансових втрат і створює ризик банкрутства для бізнесу. Причиною конфіскації може стати будь-яке юридичне рішення – від постанови слідчого до судового ордера в межах кримінального провадження. Це робить вилучення обладнання однією з найбільш серйозних проблем сучасного бізнесу.

Основні характеристики загроз в інформаційній безпеці класифікуються таким чином:

1. Навмисні (умисні) - сюди відносяться злочинні дії, розробка і поширення шкідливого ПЗ, кібератаки та крадіжка даних.

2. Випадкові (ненавмисні) - включають помилки в програмному забезпеченні, проблеми з апаратурою, збої через перебої електроенергії або стихійні катастрофи.

3. Соціальні - причиною часто стає недбалість співробітників, шахрайство через підкуп чи шантаж.

4. Технологічні - недостатній рівень захисту ПЗ та апаратного забезпечення або ж вразливості у самих системах.

5. Природні - сюди входять пожежі, повені та інші стихійні лиха, які можуть вплинути на збереження та доступність інформації.

Найпоширеніші види загроз:

1. *Несанкціонований доступ* - отримання доступу до конфіденційної інформації або систем без дозволу.

2. *Витік інформації* - передача даних за межі дозволених зон через пошкодження носіїв або використання неавторизованих каналів зв’язку.

3. *Шкідливі програми* - віруси, трояни та черв’яки, які можуть пошкодити систему, викрасти або змінити дані.

4. *Збої та несправності* - проблеми в роботі програмного чи апаратного забезпечення, що призводять до втрати даних або тимчасового припинення роботи.

Мета впровадження заходів інформаційної безпеки:

1. Гарантувати конфіденційність даних.

2. Забезпечити цілісність інформації, запобігаючи її модифікації чи знищенню.

3. Зберігати доступність даних, щоб важлива інформація була у потрібний час у потрібному місці.

4. Ідентифікувати потенційні загрози та застосувати заходи для мінімізації ризиків і запобігання наслідкам.

Приклади заходів безпеки:

1. Використання надійних паролів і уникання простих або поширених варіантів.

2. Регулярне оновлення програмного забезпечення і встановлення антивірусних програм.

3. Захист мережних з’єднань шляхом шифрування і контролю доступу.

4. Проведення навчання персоналу щодо основ інформаційної безпеки.

5. Виявлення слабких місць у системах і оперативне усунення вразливостей.

6. Створення резервних копій даних із їхнім зберіганням у захищених місцях для швидкого відновлення у разі втрати.

Забезпечення інформаційної безпеки є критично важливим для сучасних організацій та окремих користувачів, адже воно допомагає захищати цінні дані та мінімізувати ризики втрат чи порушень роботи систем.

2.3 Загальні рекомендації по захисту мережі

Регулярне оновлення системи комп’ютера є ключовим кроком для забезпечення надійного захисту в мережі. Увімкнення автоматичного оновлення на кожному пристрої дозволяє операційній системі Windows встановлювати важливі та рекомендовані патчі або тільки ті, які є критично необхідними.

Важливі оновлення значно покращують безпеку та стабільність роботи комп’ютера, тоді як рекомендовані спрямовані на вирішення менш критичних проблем і загалом оптимізують функціональність системи. Необов’язкові

оновлення при цьому не інсталюються автоматично. Служба Windows Update допомагає визначати специфіку вашого обладнання, версії операційної системи та використовуваного програмного забезпечення Microsoft для максимально точного вибору відповідних оновлень.

Брандмауер Windows є важливим інструментом для захисту комп'ютера від загроз мережі та інтернету, таких як атаки хакерів або шкідливе ПЗ (наприклад, комп'ютерні черв'яки). Він не тільки блокує спроби проникнення, але й перешкоджає поширенню шкідливих програм з вашого пристрою до інших користувачів. Без належного брандмауера комп'ютер стає вразливим до багатьох загроз, що можуть призводити до витоку інформації.

Активний брандмауер забезпечує численні переваги. Хоча він може генерувати кілька додаткових повідомлень і попереджень, його внесок у кібербезпеку значно переважає будь-які незручності.

Переваги використання брандмауера включають:

1. Моніторинг онлайн-доступу та контроль мережевого трафіку, що дозволяє виявляти потенційно незахищені дії або передачу конфіденційних даних;

2. Повідомлення про заблоковані пакети даних зі спливаючими вікнами, які інформують користувача про будь-які фільтрації мережевих з'єднань;

3. Наявність додаткових функцій для посилення кібербезпеки в деяких рішеннях.

Використання актуальних оновлень та активного брандмауера значно знижує ризики кіберзагроз, забезпечуючи стабільну та безпечну роботу комп'ютера.

Недоліки:

Брандмауер служить точкою контролю безпеки для даних, які пересуваються в і з вашої мережі. Як і будь-яка інша система безпеки, він може викликати хибні спрацьовування. Користувач може зіткнутися з тим, що

брандмауер випадково блокує безпечний вебсайт, до якого потрібно отримати доступ.

Ця проблема не є унікальною лише для окремих користувачів. Згідно з бізнес-опитуванням, проведеним інтернет-безпеки компанією McAfee, третина організацій відключають функції брандмауера, щоб уникнути переривань робочого процесу через хибні тривоги. Деякі компанії вимикають певні функції, оскільки вони можуть надмірно завантажувати обчислювальні ресурси.

Брандмауери забезпечують захист комп'ютера від шкідливих програм і атак, але вони не є засобом для боротьби з вірусами. Тому потрібно також встановити антивірусне програмне забезпечення.

Віруси можуть бути у вкладеннях електронної пошти, на компакт-дисках, DVD або в файлах, завантажених з інтернету. Важливо переконатися, що антивірусне програмне забезпечення оновлене та налаштоване на регулярне сканування комп'ютера.

Використання маршрутизатора для спільного доступу до Інтернету доцільне, оскільки такі пристрої зазвичай оснащені вбудованими брандмауерами та іншими засобами безпеки, такими як перетворення мережевих адрес (NAT), що підсилюють захист мережі від хакерів.

Не варто входити в систему як адміністратор. Якщо програма потребує доступу до Інтернету, наприклад, браузер чи поштовий клієнт, рекомендується використовувати стандартний обліковий запис. Багато вірусів і шкідливих програм не можуть зберігатися або запускатися на комп'ютері від облікового запису з обмеженими правами.

Адміністратори Windows мають можливість змінювати параметри безпеки, встановлювати програми та обладнання та отримувати доступ до всіх файлів на комп'ютері. Вони також можуть змінювати налаштування інших облікових записів.

2.4 Засоби захисту та контроль за інформаційною безпекою

До засобів захисту інформації відносяться пристрої, обладнання, програмне забезпечення та організаційні заходи, покликані запобігати витоку інформації й забезпечувати її захист в умовах посилення загроз.

Залежно від механізмів їх реалізації, ці засоби поділяються на кілька основних категорій:

Організаційні. Включають набір заходів організаційно-правового та організаційно-технічного характеру. До першої групи відносяться законодавчі та нормативні акти, а також внутрішні локальні документи організацій. До другої – заходи з підтримки інформаційної інфраструктури об'єктів.

Апаратні (технічні). Спеціальні пристрої та обладнання, що забезпечують захист від витоку і доступу до IT-інфраструктури без відповідного дозволу.

Програмні. Спеціально розроблене програмне забезпечення, яке відповідає за захист, контроль і зберігання даних.

Програмно-апаратні. Поєднання спеціального обладнання з відповідним програмним забезпеченням для забезпечення захисту інформації.

Найпоширенішими на сьогодні є саме програмні засоби захисту інформації. Вони вважаються найбільш ефективними та актуальними, оскільки можуть регулярно оновлюватися для боротьби з новітніми загрозами.

Для захисту даних у сучасних мережах застосовується різноманітне спеціалізоване програмне забезпечення. Основними його типами є:

Антивірусне програмне забезпечення. Призначене для виявлення, нейтралізації та видалення шкідливих програм. Воно може виконувати перевірки за заданим розкладом чи в ручному режимі адміністратором. Програми здатні блокувати підозрілу активність у реальному часі, а також відновлювати заражені файли.

Хмарні антивіруси (CloudAV). Поєднують можливості стандартних антивірусів із хмарними технологіями, серед яких популярні сервіси Crowdstrike, Panda Cloud Antivirus, Immunet тощо. Основна частина функціоналу зосереджена на хмарному сервері, а на пристрої користувача встановлюється легке клієнтське

ПЗ. Це дозволяє ефективно захищати дані навіть на пристроях із низькою обчислювальною потужністю.

DLP-рішення (Data Leak Prevention). Це технології, які спрямовані на запобігання витоку конфіденційної інформації в компаніях. Впровадження та обслуговування таких рішень потребують значних фінансових і організаційних ресурсів. Проте їх використання значно знижує ризики втрати важливих даних для IT-інфраструктури підприємства.

Застосування цих засобів дозволяє мінімізувати можливості витоку інформації та посилює загальний рівень безпеки у світі сучасних цифрових загроз.

Системи криптографії, такі як DES (Data Encryption Standard) та AES (Advanced Encryption Standard), застосовуються для перетворення даних, які потім можуть бути розшифровані лише за допомогою відповідних ключів. Окрім цього, криптографія охоплює й інші інструменти для забезпечення захисту інформації, зокрема методи автентифікації, дайджести повідомлень, цифрові підписи, захищені мережеві комунікації, тощо. Сучасні технології шифрування, наприклад, Secure Shell (SSH), поступово замінюють старіші рішення, які не відповідають сучасним стандартам безпеки, такі як Telnet і протокол передачі файлів FTP. Для шифрування бездротового зв’язку використовуються протоколи WPA/WPA2, хоча старий протокол WEP також все ще застосовується, незважаючи на його слабку безпеку. Провідні комунікації, такі як ITU-T G.hn, шифруються за підтримки AES із підтримкою автентифікації та обміну ключами через X.1035. Для захисту електронної пошти застосовуються програми PGP та GnuPG. [19]

Фаєрволи виконують функцію фільтрації та блокування від небажаного трафіку, а також контролю доступу до мережі. Вони поділяються на мережеві та хостові. Мережеві фаєрволи зазвичай реалізується на шлюзах локальних (LAN), глобальних (WAN) або внутрішніх мереж. Міжмережевий екран зазвичай реалізований у форматі програмного рішення для звичайного комп'ютера або як спеціалізований апаратно-програмний пристрій з інтегрованими МСЕ. Окрім

базових функцій, фаєрволи пропонують додаткові можливості для внутрішніх мереж та працюють як сервер VPN або DHCP.

VPN забезпечують використання приватної мережі для передачі даних всередині загальнодоступного середовища, що гарантує ефективну захищеність використовуємих додатків. Вони дозволяють віддалене підключення до внутрішньої мережі або створення єдиної мережі для центрального офісу та його філій. Для звичайних користувачів VPN є корисним засобом для приховування свого місцезнаходження та забезпечення захисту діяльності в Інтернеті.

Проксі-сервер виконує роль посередника між комп'ютером користувача сервером. До того ж запит від користувача спершу надходить на проксі-сервер, який передає його цільовому серверу від свого імені, а відповідь повертається через той самий проксі-сервер. Однією з переваг проксі-серверів є їхній кеш, доступний усім користувачам, що підвищує швидкість роботи, адже популярні запити можуть оброблятися без додаткових звернень до зовнішніх серверів.

Sistema SIEM – це рішення для моніторингу та управління інформаційною безпекою. Таке спеціалізоване програмне забезпечення, яке бере на себе функції управління безпекою даних. SIEM збирає інформацію про події від багатьох джерел, які сприяють захисту, зокрема з антивірусного програмного забезпечення, IPS, мережевих екранів та операційних систем та інших. Окрім цього, SIEM аналізує зібрані дані та забезпечує їх централізоване зберігання. На основі даного аналізу система може виявляти потенційні збої, атаки, інші негаразди та інформаційні загрози.

Сьогодні завдяки значному використанню мобільних пристроїв, які працівники часто використовують поза межами підприємства для корпоративних цілей, цей фактор обов'язково має бути врахований у принципах інформаційної безпеки. Зазвичай для контролю мобільних пристроїв робітників та захисту інформації на підприємстві можна використовуються наступні програмні рішення: Blackberry Enterprise Mobility Suite, IBM MaaS360, VMware AirWatch та інші.

Аналіз програмних застосунків по забезпеченню захисту мереж.

SIEM (Security Information and Event Management) — системи для збору, управління та аналізу інформації, що стосується безпеки, а також подій, пов'язаних з інформаційною безпекою. Таке програмне забезпечення не було спеціально створене для захисту даних чи запобігання витоку інформації та інших кіберзагроз. Основна функція SIEM — збір даних із різних джерел, таких як DLP, IDS, антивіруси, маршрутизатори і тому подібне, їхній аналіз та повідомлення про аномалії, підозрілу активність та інші відхилення.

На ринку доступно чимало подібних рішень. Одним із прикладів є IBM QRadar Security Intelligence.

IBM QRadar Security Intelligence - платформа, яка об'єднує низку продуктів для виявлення загроз мережі, оцінки їхньої критичності та заходів протидії. Програмне забезпечення підтримує управління подіями, консолідацію безпекової інформації, виявлення аномалій, роботу з журналами подій та виконання інших завдань. Серед головних переваг цієї системи — комплексність та широкий функціонал.

Основні можливості:

- єдина архітектура для аналізу загроз, подій, журналів та інших індикаторів;

- розрахунок кореляцій та аномальних ситуацій майже в реальному часі;

- потужний інструментарій для аналізу мережевої активності;

- розширений аналіз дій користувачів та використаного програмного забезпечення;

- визначення пріоритетності загроз;

- автоматизоване формування звітності;

- збір та консолідація даних про зафіксовані загрози;

- масштабований контроль активності у межах організації;

- детальний аналіз із застосуванням технологій big date.

Недоліки:

- не всім зареєстрованим подіям присвоюється категорія;

- через масштабність системи можуть виникати труднощі з її інтеграцією.

Пропонується маленький пробний період, а також безкоштовне використання обмеженої версії програми. Мінімальна вартість ліцензії становить 800 доларів на місяць.

Splunk Enterprise Security є потужним інструментом для аналізу подій інформаційної безпеки для підприємств. Однією з його ключових особливостей є орієнтація на сучасні загрози та можливість адаптуватися до нових програмно-апаратних рішень, що дозволяє швидко виявляти загрози та сповіщати про них.

Інструмент пропонує такі основні можливості:

- безпековий моніторинг в системі реального часу;
- перевірку користувачів, мережі та програм;
- розпізнавання складних загроз;
- виявлення загроз з боку співробітників;
- розслідування інцидентів;
- автоматизація управління даними та їх вивантаження;
- виявлення шахрайських дій через аномалії.

Недоліки включають складність встановлення корпоративної версії та відсутність української локалізації в нових версіях програмного забезпечення. Вартість ліцензії починається від 1800 доларів на рік і варіюється залежно від складових компонентів.

McAfee Enterprise Security Manager наразі представляє свою систему як одну з найкращих за швидкістю та достовірністю обробки даних. Її можна розгорнути як у хмарних, так і в приватних мережах, що робить її особливо придатною для компаній, що працюють з великими обсягами даних. Продукт також має високий рівень інтеграції з стороннім програмним забезпеченням без API, які забезпечують побудову ефективних корпоративних систем інформаційної безпеки.

Його основні можливості включають:

- готові конфігурації з попередньо налаштованими варіаціями;
- вбудовані пакети даних для відстеження поведінки користувачів;

- спеціальний пакет функцій для моніторингу служб Windows;
- виявлення загроз у системі реального часу;
- система сповіщення про загрози;
- моніторинг хмарних даних і локальних мережах;
- збір та упорядкування подій;
- автоматичне формування звітів про події.

Недоліки враховують потребу у великих обчислювальних ресурсах та не завжди швидке усунення помилок. Значна вартість безстрокової ліцензії починається від 500 гривень, а для нових користувачів є безкоштовний 14-денний тестовий період.

DLP-система, що розшифровується як Data Leak Prevention, являє собою спеціалізоване програмне забезпечення, спрямоване на захист від витоків і крадіжки приватної інформації. Такі програми використовують технології блокування передачі даних, забезпечують інструменти моніторингу поведінки працівників і всіх учасників мережі, а також надають можливості контролю за діяльністю персоналу. Ринок DLP-систем є досить обширним, проте виділяються два провідних рішення.

Одним із таких є система InfoWatch Traffic Monitor, яка призначена для роботи під значним навантаженням, особливо при необхідності обробки великої кількості інформації. Це масштабоване рішення, яке однаково ефективне як для великих корпорацій, так і для невеликих офісів. Головними функціями є моніторинг і блокування передачі інформації. Унікальна перевага системи полягає у можливості виявлення та блокування документів і мультимедійних файлів навіть у випадку їх значної модифікації користувачами.

Ключові можливості:

- Виявлення трафіку приватної інформації різних типів;
- Блокування передачі чутливих даних;
- Визначення недобросовісних співробітників;
- Виявлення шахрайських дій;
- Виявлення нетипових загроз;

- Контроль шляхів поширення внутрішньої інформації організації.

Однак серед недоліків можна відзначити:

- Обмежений функціонал моніторингу активності користувачів;

- Відсутність кейлоггера;

- Використання модульної архітектури із розміщенням компонентів на окремих пристрояї.

Вартість продукту залежить конфігурації та пропонується індивідуально за запитом до розробника. Ліцензія на програмне забезпечення надається з річним оновленням.

DeviceLock DLP – хостова система захисту від втрати даних (DLP), створена для моніторингу інформаційних потоків та блокування несанкціонованого розповсюдження даних. Вона пропонує широкі можливості налаштування сценаріїв та політики контролю, що дозволяє цю інформацію інтегрувати в організації різних масштабів і профілів, вирішуючи більшість завдань, пов’язаних із захистом приватної інформації.

Функції:

– блокування доступу до інформації;

– заборона доступу до серверів та інших пристроїв;

– індивідуальне налаштування параметрів моніторингу та обмежень;

– контроль взаємодії користувачів із мережевими сервісами.

– обмежені можливості щодо моніторингу діяльності персоналу;

– необхідність ретельної настройки сценаріїв для коректного функціонування системи.

Вартість річної ліцензії починається від 80 доларів, але залежить від конкретної версії та конфігурації.

Ще один важливий напрямок у захисті інформації – програмне забезпечення для ідентифікації осіб, які викрали документи. Універсальні рішення пропонують різні підходи, проте справді ефективним слід вважати лише одне – програму EveryTag.

EveryTag – це інструмент, який з високою вірогідністю може визначити, співробітників, які несумлінно використав інформацію. Програма забезпечує спеціальне маркування документів, яке залишається непомітним на вигляд. Якщо інформація потрапляє у сторонні руки, достатньо завантажити копію у систему, щоб з'ясувати винуватця. Цей підхід є простим і дієвим.

Функції:

– захист електронних документів;

– запобігання несанкціонованому фотографуванню друкованих матеріалів;

– захист від доступу до інформації через знімки екрана;

– безпека друкованих документів.

Недоліки:

– вузька спеціалізація ПЗ, яке в основному спрямоване лише на ідентифікацію недобросовісних співробітників.

Ціна програми залежить від її конфігурації. Деталі вартості доступні лише за запитом до розробника.

Для всебічної інформаційної безпеки фірми важливо впроваджувати ефективний корпоративний антивірус. Таке програмне забезпечення захищає дані та обладнання від небезпечних програм, вірусів і кіберзагроз. На ринку доступна значна кількість якісних рішень цього типу. Далі розглянемо деякі популярні варіанти.

Kaspersky Small Office Security — це надійний антивірус, який забезпечує швидке оновлення баз даних і високий рівень захисту від різноманітних загроз. Програмне забезпечення ідеально підходить для маленьких компаній, але також може використовуватися у великих організаціях. Його ключова перевага — розширений можливості, які охоплюють практично всі аспекти взаємодії компанії з зовнішніми цифровими мережами.

Функції:

- файловий антивірус;

- веб-антивірус;

- захист від збору даних;

- контроль оновлень застосунків;
- захист веб-камер;
- фільтрування доступу користувачів;
- контроль установлених програм;
- захист грошової інформації;
- блокування реклами;
- шифрування даних.

Недоліки:

- орієнтованість в основному на невеликі офіси;
- обмежений функціонал веб-панелі для управління.

Вартість ліцензії починається від 23 доларів для конфігурації з підтримкою одного ПК.

McAfee Endpoint Protection Essential — корпоративний антивірус, який характеризується потужним набором інструментів для захисту від мережевих і програмних загроз. Програма оптимізована для вирішення задач бізнесу, проста в налаштуванні та управлінні, а також забезпечує часті оновлення інформаційних баз. Її головними перевагами є швидке виявлення загроз та здатність формування звітів.

Функції:

- брандмауер;
- моніторинг інформації;
- захист від вірусів;
- захист ПК;
- контроль веб-трафіку;
- автентична реакція на потенційні загрози.

Недоліки:

- складна установка та налаштування;
- високі вимоги до обладнання під час повного системного сканування.

Вартість ліцензії починається від 100 доларів і залежить від обраної конфігурації.

Системи обліку робочого часу (СОРВ) – елемент програмного забезпечення, який надає ефективний захист даних фірми. Однак слід звертати увагу лише на ті СОРВ, функціонал яких доповнений інструментами для моніторингу дій працівників за комп'ютерами. У цьому контексті програма Kickidler є беззаперечним лідером, адже саме вона пропонує найширший набір можливостей для аналізу роботи співробітників.

Винахідливість недобросовісних працівників у прагненні обійти системи контролю або вчинити корпоративні злочини не варто недооцінювати. Вони постійно розробляють нові схеми обходу програм для блокування та моніторингу інформації. Однак потенційні проломи у системі можна усунути завдяки контролю не лише за самими корпоративними даними, але й за діями працівників.

Kickidler пропонує набір ключових функцій, таких як запис відео з екранів, кейлоггер, онлайн-моніторинг та контроль часу роботи за ПК. Реальний приклад з досвіду компанії – виявлення інсайдера, який незаконно передавав базу клієнтів, демонструє високу ефективність цього інструменту.

Також варто зазначити, що усвідомлення того, що кожна дія працівника фіксується та зберігається, значною мірою зменшує ймовірність спроб крадіжки даних чи іншого порушення. У спірних випадках оцінку можна провести на основі кількох параметрів одночасно, наприклад, проаналізувавши дані кейлоггера разом з відеозаписом екрана.

Основні можливості Kickidler включають:

– онлайн-моніторинг екранів співробітників у реальному часі;

– кейлоггер для запису кожного натискання клавіш;

– безперервний запис відео з екрана користувача;

– автоматичну реєстрацію часу початку та завершення роботи, а також пауз;

– віддалений доступ до ПК;

– сповіщення про порушення на роботі.

До недоліків можна віднести:

– немає мобільної версії;

– відсутність інтеграції з хмарними сервісами.

Програмне забезпечення пропонується у вільний версії до 6 підключень. Передбачено двотижневий період для ознайомлення з повною версією. Ліцензія коштує 4 долари за кожен ПК.

Підсумовуючи, SIEM-система відповідає за аналіз інформації, виявлення загроз і їх попередження. DLP-система контролює обмін даними та запобігає їх несанкціонованому поширенню. Програмні застсунки для захисту документів блокує спроби викрадення будь-якими шляхами. Цей антивірус протидіє шкідливим застосункам. У свою чергу, СОРВ контролює поведінку співробітників.

Контроль за інформаційною безпекою.

Забезпечення ефективної та надійної інформаційної безпеки підприємства можливе лише за умов застосування комплексного й системного підходу. Система захисту інформації має бути побудована з урахуванням актуальних загроз і вразливостей, а також тих викликів, які можуть виникнути в майбутньому. Це вимагає підтримки постійного моніторингу, який має функціонувати безперервно — цілодобово, кожного дня. Важливим аспектом є організація контролю на всіх етапах життєвого циклу інформації: від моменту її надходження до інфраструктури компанії до втрати актуальності чи знищення даних.

Для ефективного управління ризиками в інформаційній сфері та підтримання їх на прийнятному рівні існують різні види контролю. Вони включають:

- адміністративний контроль;

- логічний контроль;

- фізичний контроль.

Адміністративний контроль у системі інформаційної безпеки є комплексом правил, стандартів і процедур, які забезпечують управління бізнес-процесами та персоналом. Він охоплює законодавчі й нормативні акти,

корпоративну політику безпеки, процедури найму працівників, дисциплінарні заходи та інші регламенти.

Логічний контроль передбачає використання технічних засобів для захисту інформаційних систем від несанкціонованого доступу. До таких засобів належать спеціальне програмне забезпечення, брандмауери, системи паролювання тощо.

Фізичний контроль концентрується на захисті робочих місць і апаратного забезпечення. Він включає забезпечення належного функціонування інженерних систем будівель (наприклад, опалення, кондиціювання, протипожежний захист), що можуть впливати на зберігання й передачу даних. Іншою важливою складовою фізичного контролю є системи управління доступом до об’єктів підприємства.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ МЕТОДУ БЛОКУВАННЯ СЕРВЕРУ

3.1 Опис середовища моделювання Cisco Packet Tracer версії 8.2.2

Cisco Packet Tracer — це потужний інструмент для вивчення мережевих технологій, який поєднує реалістичне моделювання та візуалізацію з оцінюванням знань, створенням освітнього контенту, а також можливостями командної співпраці та змагань. Завдяки інноваційним функціям Packet Tracer студенти та викладачі можуть ефективно співпрацювати, вирішувати завдання та поглиблювати компетенції у динамічному навчальному середовищі. Основні переваги програми включають:

• Реалістичне середовище моделювання та візуалізації, яке доповнює роботу з фізичним обладнанням, забезпечуючи доступ до процесів у реальному часі, прихованих у справжніх пристроях.

• Можливість синхронної багатокористувацької співпраці та організації змагань для інтерактивного навчання.

• Інструменти для створення локалізованих навчальних матеріалів: лабораторних робіт, демонстрацій, вікторин, іспитів та ігор.

• Забезпечення студентів платформою для вивчення концепцій, проведення експериментів та перевірки знань у побудові мережі.

• Функції проектування, створення, налаштування та усунення несправностей складних мереж через симуляцію за допомогою віртуального обладнання.

• Підтримку різноманітних підходів до навчання: лекцій, командних чи індивідуальних лабораторних занять, домашніх завдань, ігрових активностей та конкурсів.

Забезпечує розширення функціоналу через інтеграцію зовнішніх програм за допомогою API, що дозволяє вдосконалити роботу Cisco Packet Tracer у таких напрямках, як навчальні програми та оцінювання, гейміфікація, доступність, а також взаємодія зі справжнім обладнанням [14].

3.2 Створення простої мережі в середовище логічної топології

Для реалізації завдання розробки програмного інтерфейсу для маршрутизатора Cisco в першу чергу необхідно побудувати топологію мережі. Для цього скористаємося Cisco Packet Tracer.

Після відкриття програми відображається порожня робоча область для побудови топології, як показано на рис. 3.1

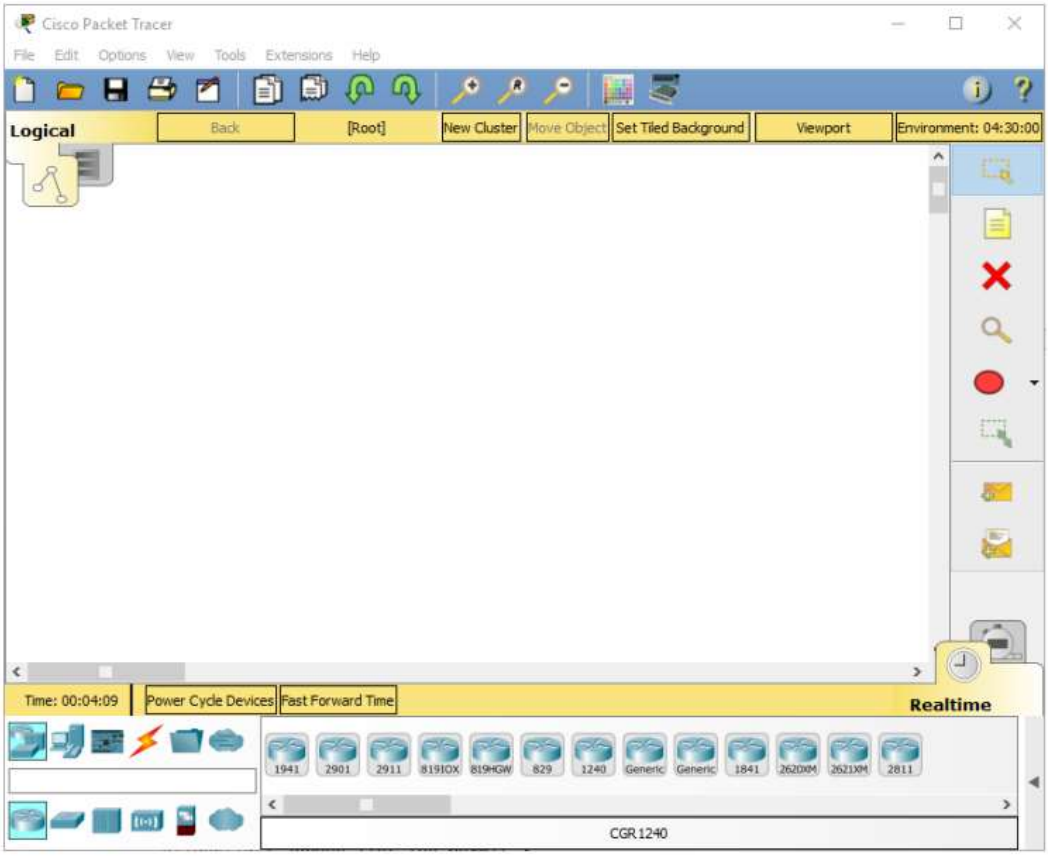

Рис. 3.1 Робоча область логічної топології Cisco Packet Tracer.

Далі на робочу область додаємо мережеві пристрої. Для створення топології мережі обираємо: два сервера (Server-PT Yandex та Server-PT Google), роутер Cisco 2911 та один ПК.

Щоб розмістити пристрої спочатку обираємо тип пристрою у вікні вибору типу пристрою, а потім обираємо потрібну модель у полі вибору конкретного пристрою. Далі змінюємо назву пристроїв використовуючи відповідну вкладку, як показано на рис. 3.3

Рис.3.3 Вікно налаштувань пристрою Cisco Packet Tracer

Наступним кроком додаємо фізичну проводку між обраними пристроями на робочій області. В результаті конфігурація має наступний вигляд рис. 3.4

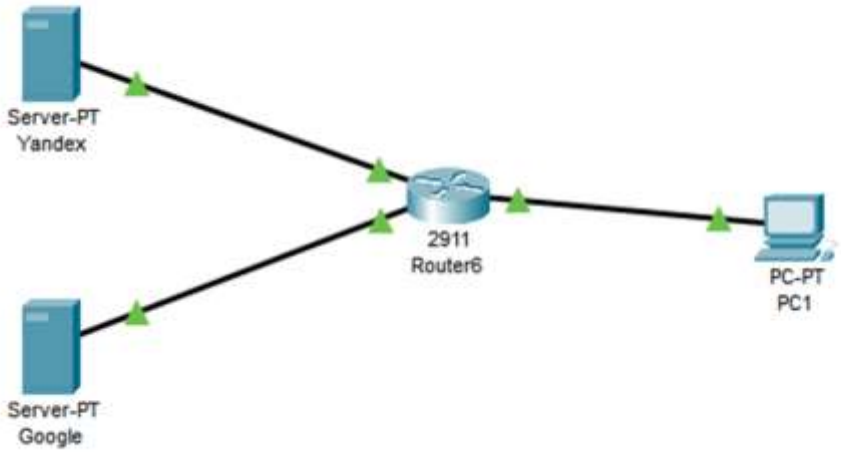

Рис. 3.4 Топологія мережі для маршрутизатора Cisco

Після створення топології необхідно виконати налаштування обладнання мережевих пристроїв.

3.3 Налаштування мережевих пристроїв

Наступним кроком після створення топології, потрібно виконати налаштування мережевих пристроїв.

Починаємо з конфігурації інтерфейсів на роутері. Інтерфейс gigabitEthernet 0/0 для трафіку з ПК1.

Для цього необхідно увійти в CLI (інтерфейс командного рядка), командою enable, а після в режим глобальної конфігурації configure terminal, режим конфігурації інтерфейса: interface gigabitEthernet 0/0.

Задаємо ip на цьому інтерфейсі 192.168.1.1 255.255.255.0 (24 маска), командою no shutdown активуємо інтерфейс (рис. 3.5).

```
Router>
Router>ena
Router>enable
Router#conf
Router#configure ter
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int
Router(config)#interface gi
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ipadd
Router(config-if)#ip add
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

Рис. 3.5. Налаштування роутера

Аналогічні налаштування робимо для gigabitEthernet 0/1 для трафіку з сервером Yandex, тільки задав ip 10.0.1.1 (рис. 3.6).

```
Router(config-if)#exit
Router(config)#int
Router(config)#interface gig
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip add
Router(config-if)#ip address 10.0.1.1 255.255.255.0
Router(config-if)#no shu
Router(config-if)#no shutdown
```

Рис. 3.6. Налаштування для трафіку з сервером Yandex

І так само робимо налаштування для gigabitEthernet 0/2 для трафіку з сервером Google, тільки задаємо ip 10.0.2.1 (рис. 3.7).

```
Router(config-if)#exit
Router(config)#int
Router(config)#interface gig
Router(config)#interface gigabitEthernet 0/2
Router(config-if)#ip add
Router(config-if)#ip address 10.0.2.1 255.255.255.0
Router(config-if)#no shu
Router(config-if)#no shutdown
```

Рис. 3.7. Налаштування для трафіку з сервером Google

Далі переходимо до налаштувань ПК1 через інтерфейс Cisco Packet Tracer. У вкладці INTERFACE > FastEthernet0 задаємо статичну ip 192.168.1.10/24 (Рис. 3.8).

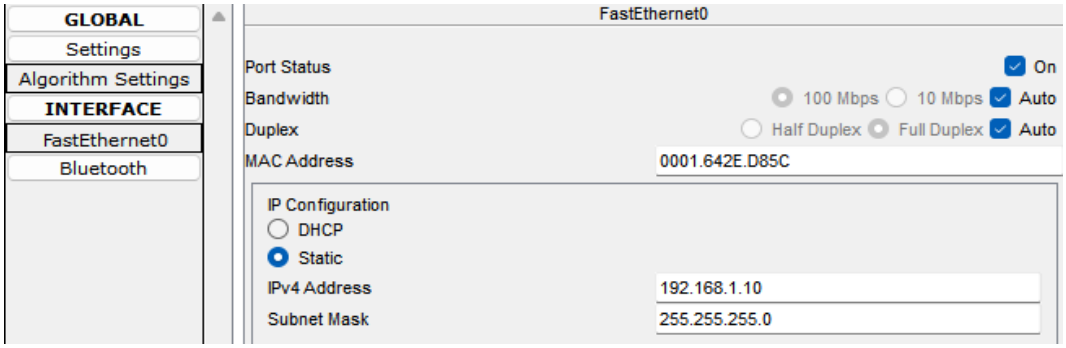

Рис.3.8 Налаштування ПК через вкладку INTERFACE

А у вкладці global > setting встановлюємо шлюз за замовчуванням 192.168.1.1 (Рис. 3.9).

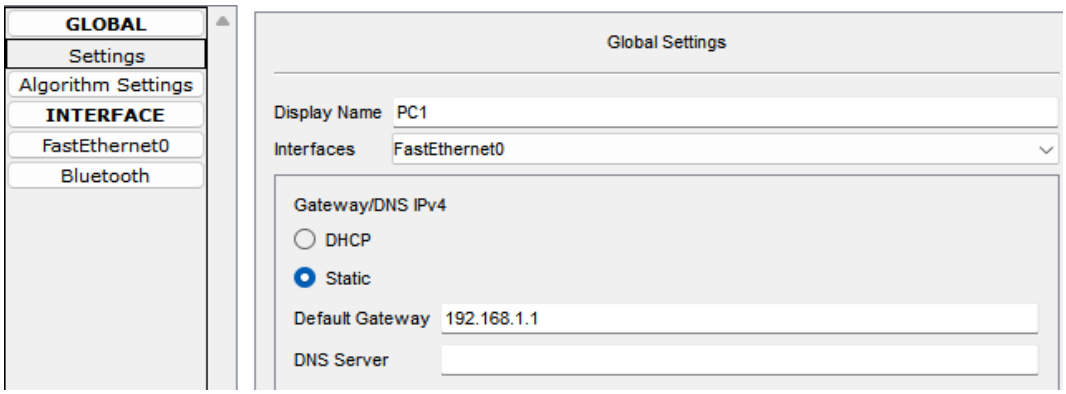

Рис 3.9 Налаштування ПК через вкладку GLOBAL

І по аналогії налаштовуємо сервер Yandex через інтерфейс Cisco Packet Tracer тільки з ip 10.0.1.10/24. А шлюз за замовчуванням встановлюємо 10.0.1.1 (рис. 3.10, 3.11).

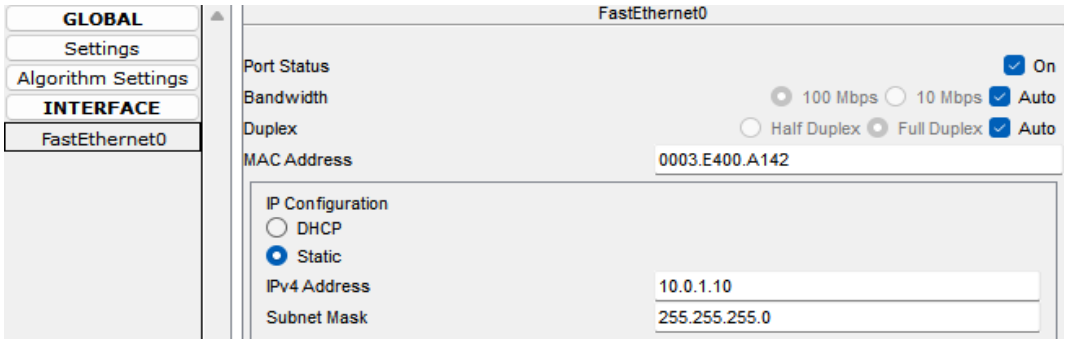

Рис.3.10 Налаштування сервер Yandex через вкладку INTERFACE

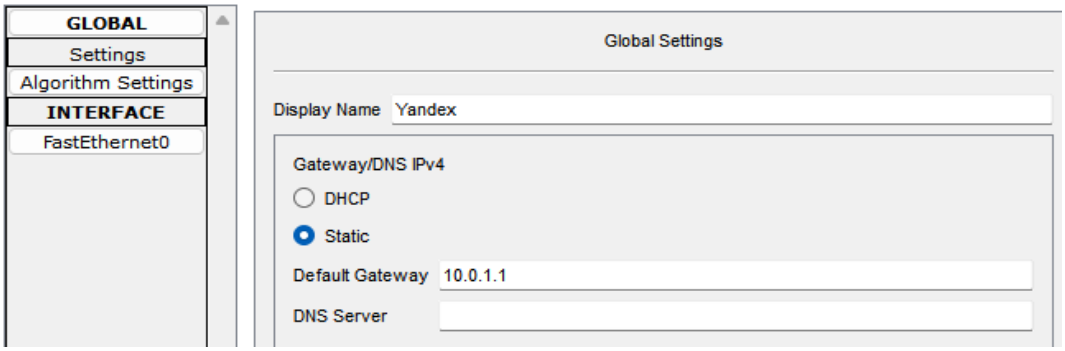

Рис 3.11 Налаштування серверу Yandex через вкладку GLOBAL

Так само налаштовуємо сервер Google задаємо ip 10.0.2.10/24. Шлюз - 10.0.2.1 (3.12, 3.13)

Рис.3.12 Налаштування сервер Yandex через вкладку INTERFACE

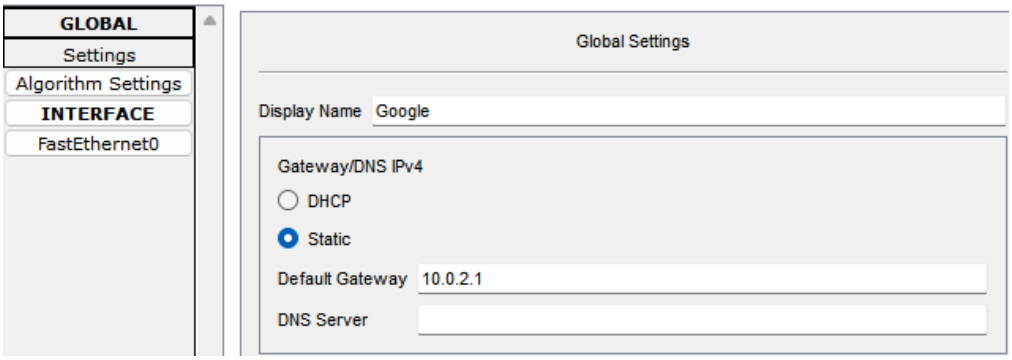

Рис 3.13 Налаштування серверу Yandex через вкладку GLOBAL

3.4 Блокування серверу Yandex

У Packet Tracer доступ до сервера можна обмежити різними методами. Основні з них включають фільтрацію пакетів (ACL) на маршрутизаторах та налаштування брандмауера безпосередньо на сервері. Крім того, можливості інтерфейсу командного рядка (CLI) дозволяють налаштувати аналогічно тому, як це відбувається на реальних пристроях Cisco.

Розглянемо кожний з цих методів:

Перший фільтрування пакетів (ACL) на маршрутизаторі.

Access Control List (ACL) є набором правил, який маршрутизатор використовує керувати потоком мережного трафіку. За допомогою цих правил можна дозволяти або блокувати пакети на основі певних характеристик, таких як IP-адреси, номери портів та типи протоколів.

Розглянемо як налаштувати ACL у Packet Tracer:

На маршрутизаторі, який знаходиться на маршруті до цільового сервера, переходимо до інтерфейсу командного рядка (CLI), далі активуємо режим глобальної конфігурації за допомогою команди (configure terminal). Створюємо нову ACL, наприклад: ip access-list standard BLOCK_SERVER. Додаємо потрібні правила, щоб заборонити пакети, спрямовані на сервер. Наприклад, правило для джерела: match source 192.168.1.0 0.0.0.255, або правило для обмеження протоколу: match protocol tcp eq 80. Призначаємо створену ACL відповідному інтерфейсу маршрутизатора (тому, через який здійснюється доступ до сервера). Для цього використовуємо команду: ip access-group BLOCK_SERVER in.

Другий метод Фаєрвол на сервері:

Фаєрвол – це програмне забезпечення, яке керує вхідним та вихідним трафіком на сервері.

Для налаштування фаєрволу у Packet Tracer: необхідно перейти до сервера, відкрити інтерфейс командного рядка (CLI) або графічний інтерфейс користувача (GUI) та встановити правила фаєрволу для обмеження доступу до певних портів або IP-адрес.

Робота з інтерфейсом командного рядка (CLI):

У Packet Tracer, як і на реальних пристроях Cisco, доступ до інтерфейсу командного рядка (CLI) здійснюється через консольний порт або протоколами SSH/Telnet. Це дозволяє налаштовувати маршрутизатори та сервери для реалізації різних заходів безпеки, таких як обмеження або блокування доступу.

Наприклад, якщо, сервер має IP-адресу 192.168.1.100, і потрібно обмежити доступ до нього з мережі 192.168.2.0/24.

Змінюємо налаштування на маршрутизаторі:

Спочатку створюємо ACL (список контролю доступу), який забороняє трафік із мережі 192.168.2.0 до сервера з IP 192.168.1.100.

Після цього застосовуємо створений ACL до інтерфейсу маршрутизатора до мережі 192.168.2.0.

Для виконання завдання по блокуванню серверу Yandex будемо використовувати метод ACL.

У режимі глобальної конфігурації створюємо extended Access Control List (ACL) з назвою block_yandex. Є два основні типи ACL: Standard та Extended Standard фільтрує тільки за IP-адресою джерела.

Extended Фільтрує за IP-адресою джерела та призначення, протоколом, портами (рис 3.14).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended block_yandex
Router(config-ext-nacl)#deny ip any host 10.0.1.10
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
```

Рис 3.14 Фільтрація за IP-адресою серверу Yandex

Створюємо правило, щоб заблокувати доступ до сервера з ip 10.0.1.10 командою deny ip any host 10.0.1.10, командою permit ip any any дозволяю увесь інший трафік (тобто доступ до сервера google).

Наступним кроком буде застосування ACL до інтерфейса, який підключений до ПК1 (Рис.3.15).

```
Router(config)#int
Router(config)#interface gig
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip ac
Router(config-if)#ip access-group block_yandex in
```

Рис.3.15 Застосування ACL до інтерфейса ПК1

Переходимо на інтерфейс 0/0 і командою ip access-group block_yandex in застосовуємо ACL на вхідний трафік з цього інтерфейса.

3.5 Перевірка методу

Тепер треба перевірити доступність серверів за допомогою команди Ping з ПК1.

Пінгуємо заблокований сервер 10.0.1.10 і отримуємо (Рис.3.16):

```
C:\>ping 10.0.1.10

Pinging 10.0.1.10 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 10.0.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис. 3.16 Результати перевірки заблокованого серверу Yandex

Пінгуємо розблокований сервер 10.0.2.10 і отримуємо(Рис.3.17).:

```
C:\>ping 10.0.2.10

Pinging 10.0.2.10 with 32 bytes of data:

Reply from 10.0.2.10: bytes=32 time<1ms TTL=127
Reply from 10.0.2.10: bytes=32 time<1ms TTL=127
Reply from 10.0.2.10: bytes=32 time<1ms TTL=127
Reply from 10.0.2.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рис. 3.17 Результати перевірки розблокованого серверу Google

В середовище моделювання Cisco Packet Tracer було протестовано та реалізовано механізм блокування інформаційного ресурсу за допомогою програмного інтерфейсу маршрутизатора Cisco. Для перевірки ефективності блокування використано утиліту ping.