

МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “Розробка прототипу системи кіберзахисту комп'ютерної мережі
державної установи”

Здобувача вищої освіти другого (магістерського) рівня,
II курсу, групи КМІЗ-22-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології в економіці»



(підпис)

Ляховича Олександра
Леонідовича

(прізвище, ім'я, по батькові)

Науковий керівник



(підпис)

Редич Олександр
Володимирович, к.е.н.,
доцент

(прізвище, ім'я, по батькові, науковий
ступінь, вчене звання)

Керівник освітньо-
професійної програми



(підпис)

Горбовий Артур Юліанович,
д.т.н, професор

(прізвище, ім'я, по батькові, науковий
ступінь, вчене звання)

Допущено до захисту за рішенням кафедри
протокол від «28» грудня 2023 № 8

Завідувач кафедри



(підпис)

Філоненко Михайло
Миколайович, к.ф.-м.н.,

доцент

(прізвище, ім'я, по батькові,
науковий ступінь, вчене звання)

Реєстрація № 14

30.01.2024

(дата)



(підпис відповідальної особи)

Результати перевірки

до захисту

(до захисту, на доопрацювання)

30.01.2024

(дата)



(підпис)

Результат захисту

5 (відмінно)

(оцінка)

09.02.2024

(дата)



(підпис)

Голова комісії:



(підпис)

В.М. Франчук

Члени комісії:



(підпис)

А.Ю. Горбовий



(підпис)

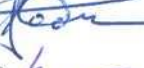
О.В. Редич



(підпис)

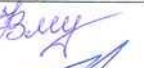
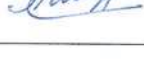
В.О. Ніжегородцев

БЛАНК ОЦІНЮВАННЯ ВИПУСКНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст випускної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	28		09.02.2024 Франчук В.М.  Горбовий А.Ю.  Редич О.В.  Ніжегородцев В.О.  Суховерхівка Л.П. 
2. Дотримання вимог щодо оформлення	від 0 до 10	9		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	4		
4. Рецензент	від 0 до 5	4		
РАЗОМ БАЛІВ	від 0 до 50	45		

Оцінювання кваліфікаційної роботи науковим керівником - 45 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
90	A	5 (відмінно)	09.02.2024	Франчук В.М.  Горбовий А.Ю.  Редич О.В.  Ніжегородцев В.О.  Суховерхівка Л.П. 

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	
50-59	E	3 (задовільно)
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій
Кафедра комп'ютерних та інформаційних технологій і систем

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 122 «Комп'ютерні науки»

Освітня програма: «Інформаційні управляючі системи та технології в економіці»

Затверджую

Завідувач кафедри  Філоненко М.М.

« 04 » 04 2023

Завдання на кваліфікаційну роботу
здобувачу вищої освіти

Ляховичу Олександрю Леонідовичу

1. Тема дипломної роботи

Розробка прототипу системи кіберзахисту комп'ютерної мережі
державної установи

Затверджена наказом ректора від 4 квітня 2023 р. №363

2. Строк здачі закінченої роботи: _____

3. Мета роботи: Провести дослідження принципів та підходів організації системи захисту комп'ютерних мереж, розробити прототип кіберзахисту комп'ютерної мережі державної установи.

Об'єкт дослідження: Інформаційне середовище та комп'ютерна мережа державної установи.

Предмет дослідження: Технології та активне устаткування Cisco для організації захисту комп'ютерної мережі.

Орієнтовна база дослідження комп'ютерна мережа державної установи Господарського суду міста Києва.

4. Вихідні дані до роботи: технічні параметри активного мережного обладнання Cisco, симулятора комп'ютерних мереж Packet Tracer

5. Перелік графічного матеріалу: рисунки, формули, що пояснюють суть застосованих методів, засобів та технологій; структурні схеми та, таблиці, графіки, результати апробації.

6. Зміст випускної кваліфікаційної (дипломної) роботи (перелік питань за кожним розділом) :

РОЗДІЛ 1. ІСТОРІЯ ДЕРЖАВНОГО КІБЕРЗАХИСТУ В УКРАЇНІ

1.1. Історія та зародження державного кіберзахисту в Україні.

1.2. Розвиток кіберзахисту в світі та його вплив на Україну.

1.3. Стан державного кіберзахисту в Україні.

РОЗДІЛ 2. ТЕОРЕТИЧНІ АСПЕКТИ КІБЕР ЗАХИСТУ В ДЕРЖАВНИХ УСТАНОВАХ

2.1. Розробка політик безпеки інформації

2.2 Основні принципи та підходи до кіберзахисту

2.3 Особливості застосування кіберзахисту в державних установах

РОЗДІЛ 3. ПРОТОТИП СИСТЕМИ КІБЕР ЗАХИСТУ ДЕРЖАВНОЇ УСТАНОВИ НА БАЗІ УСТАТКУВАННЯ CISCO

3.1. Прототип системи кіберзахисту на базі устаткування Cisco

3.2. Аналіз можливостей устаткування Cisco для кіберзахисту

3.3. Моделювання прототипу кіберзахисту за допомогою емулятора Cisco Packet Tracer

3.4. Інтеграція системи кіберзахисту на основі Cisco в державну установу

3.5. Моніторинг та підтримка системи кіберзахисту

7. Календарний план виконання роботи

№ п/п	Назва етапів випускної кваліфікаційної (дипломної) роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури ДР	До 27.12.2022 р.	« <u>27</u> » <u>12</u> 2022 р.
2	I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	26. 06. 2023 р.	« <u>26</u> » <u>06</u> 2023 р.
3	II розділ (аналіз експериментальної частини про і методики досліджень)	23. 10.2023 р.	« <u>23</u> » <u>10</u> 2023 р.
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проектні рішення)	30. 11.2023 р.	« <u>30</u> » <u>11</u> 2023 р.
5	Висновки	10. 12.2023 р.	« <u>10</u> » <u>12</u> 2023 р.
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	20.01.2024 р.	« <u>20</u> » <u>01</u> 2024 р.
7	Отримання відгуку керівника	29.01.2024 р.	« <u>29</u> » <u>01</u> 2024 р.
8	Отримання зовнішньої рецензії	01.02.2024р.	« <u>01</u> » <u>02</u> 2024 р.

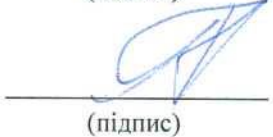
Дата видачі завдання «04» 04 2023 р.

Керівник дипломної роботи


(підпис)

О.В. Редич

Керівник освітньо-професійної програми


(підпис)

А.Ю. Горбовий

Завдання до виконання отримав
здобувач вищої освіти


(підпис)

О.Л. Ляхович

АНОТАЦІЯ

Короткий зміст роботи: У роботі проведено дослідження принципів та підходів організації системи захисту комп'ютерних мереж, розроблено прототип кіберзахисту комп'ютерної мережі державної установи. Проаналізовано використання програмного забезпечення Cisco Packet Tracer. Проведено дослідження технології та активного устаткування Cisco для організації захисту комп'ютерної мережі.

Ляхович О.Л. Розробка прототипу системи кіберзахисту комп'ютерної мережі державної установи. Національний університет Державної податкової служби України, Ірпінь, 2024 рік. У даному дипломному проекті наведено огляд підходів до побудови прототипу системи кіберзахисту та проведено аналіз існуючого обладнання та обґрунтований вибір для реалізації проекту. У якості демонстраційної частини побудовано модель мережі державної установи на базі системи кіберзахисту Cisco, виконані потрібні налаштування та перевірена її працездатність.

Автором було розроблено прототип у середовищі комп'ютерної мережі державної установи із використанням устаткування Cisco Packet Tracer.

Практична значимість прототипу полягає у можливості використання його для розгортання реальної захищеної мережі на устаткуванні Cisco. Це відкриває широкі перспективи для вдосконалення інфраструктури компаній та організацій, забезпечуючи надійний захист від кіберзагроз та забезпечуючи безперебійне функціонування мережевих систем. Реалізація цього прототипу дозволить ефективно впроваджувати передові технології безпеки, підвищуючи стійкість мережі до атак і забезпечуючи конфіденційність, цілісність та доступність даних.

Кваліфікаційна робота містить 59 с. тексту, 14 рисунків, 43 літературне джерело.

Ключові слова: мережа, обладнання, устаткування, Cisco, Cisco Packet Tracer.

ABSTRACT

Summary of the work: In the work, a study of the principles and approaches of the organization of the computer network protection system was carried out, a prototype of cyber protection of a computer network of a state institution was developed. The use of Cisco Packet Tracer software was analyzed. A study of Cisco technology and active equipment for the organization of computer network protection was conducted.

Lyakhovych O.L. Development of a prototype system of cyber protection of a computer network of a state institution. National University of the State Tax Service of Ukraine, Irpin, 2024. This diploma project provides an overview of approaches to the construction of a prototype of a cyber defense system, an analysis of existing equipment and a justified choice for the implementation of the project. As a demonstration part, a model of the network of a state institution based on the Cisco cyber protection system was built, the necessary settings were made and its functionality was checked.

The author developed a prototype in the environment of a computer network of a state institution using Cisco Packet Tracer equipment.

The practical significance of the prototype lies in the possibility of using it to deploy a real secure network on Cisco equipment. This opens up wide prospects for improving the infrastructure of companies and organizations, providing reliable protection against cyber threats and ensuring the smooth functioning of network systems. The implementation of this prototype will allow effective implementation of advanced security technologies, increasing the resistance of the network to attacks and ensuring confidentiality, integrity and availability of data.

The qualification work contains 59 pages. text, 14 figures, 43 literary sources.

Keywords: network, equipment, equipment, Cisco, Cisco Packet Tracer.

Зміст

ВСТУП	3
РОЗДІЛ 1.ІСТОРІЯ ДЕРЖАВНОГО КІБЕРЗАХИСТУ В УКРАЇНІ	5
1.1. Історія та зародження державного кіберзахисту в Україні	5
1.2. Розвиток кіберзахисту в світі та його вплив на Україну	9
1.3. Стан державного кіберзахисту в Україні	10
РОЗДІЛ 2.ТЕОРЕТИЧНІ АСПЕКТИ КІБЕР ЗАХИСТУ В ДЕРЖАВНИХ УСТАНОВАХ.....	12
2.1. Розробка політик безпеки інформації	12
2.2 Основні принципи та підходи до кіберзахисту.....	14
2.3 Особливості застосування кіберзахисту в державних установах	16
РОЗДІЛ 3.ПРОТОТИП СИСТЕМИ КІБЕР ЗАХИСТУ ДЕРЖАВНОЇ УСТАНОВИ НА БАЗІ УСТАТКУВАННЯ CISCO.....	18
3.1. Прототип системи кіберзахисту на базі устаткування Cisco.....	18
3.2. Аналіз можливостей устаткування Cisco для кіберзахисту	21
3.3. Моделювання прототипу кіберзахисту за допомогою емулятора Cisco Packet Tracer.....	36
3.4. Інтеграція системи кіберзахисту на основі Cisco в державну установу. ..	48
3.5. Моніторинг та підтримка системи кіберзахисту	49
ВИСНОВКИ.....	51
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	53

ВСТУП

Актуальність теми: У сучасних умовах збройна боротьба ведеться із застосуванням високотехнологічного озброєння і військової техніки, високоефективних засобів розвідки, управління й ураження зі значним збільшенням розмаху і швидкоплинності операцій. Інформаційне забезпечення процесів управління та навантаження органів управління постійно зростають. Забезпечення ефективності управління своїми силами і засобами та порушення його у противника надає вагомі переваги над ним в умовах сучасного протистояння.

Мета роботи: Провести дослідження принципів та підходів організації системи захисту комп'ютерних мереж, розробити прототип кіберзахисту комп'ютерної мережі державної установи.

Об'єкт дослідження: Інформаційне середовище та комп'ютерна мережа державної установи.

Предмет дослідження: технології та активне устаткування Cisco для організації захисту комп'ютерної мережі.

Завдання дослідження: Аналіз можливостей устаткування Cisco для кіберзахисту, моделювання прототипу кіберзахисту за допомогою емулятора Cisco Packet Tracer, інтеграція системи кіберзахисту на основі Cisco в державну установу.

Автором було розроблено прототип у середовищі комп'ютерної мережі державної установи із використанням устаткування Cisco Packet Tracer.

Практична значимість прототипу полягає у можливості використання його для розгортання реальної захищеної мережі на устаткуванні Cisco. Це відкриває широкі перспективи для вдосконалення інфраструктури компаній та організацій, забезпечуючи надійний захист від кіберзагроз та забезпечуючи безперебійне функціонування мережевих систем. Реалізація цього прототипу дозволить ефективно впроваджувати передові технології безпеки, підвищуючи

стійкість мережі до атак і забезпечуючи конфіденційність, цілісність та доступність даних.

Кібервпливи все частіше стають ефективним інструментом для досягнення мети щодо несилового контролю та управління, як об'єктами з критичною інформаційною інфраструктурою держави, що може піддатися такому впливу, так і окремо взятими громадянами, їх об'єднаннями. Вони відкривають можливості досягнення політичних цілей, змін легітимних урядів, а також здійснення деструктивних змін в усіх сферах життєдіяльності суспільства і держави (економічній, енергетичній, духовній тощо), взяття під контроль і навіть поневолення цілих народів і країн практично без застосування військової сили в класичному її розумінні. Взагалі, на сьогодні, практично всі більш-менш розвинені держави вже зіткнулися з кіберзагрозами та необхідністю формувати системи кібербезпеки та кібероборони. Тенденція перенесення дій у воєнних конфліктах до нового бойового середовища – кіберпростору ще більше загостило ці проблеми. Це спонукало провідні країни світу до запровадження першочергових заходів зі створення спеціальних структур і підрозділів для дій у кіберпросторі. Спираючись на світовий досвід можна стверджувати, що процес забезпечення кібербезпеки, перш за все, передбачає протидію деструктивним впливам у цій сфері. Для цього потребує створення й організації потужна підсистема кіберзахисту. Не менш важливими складовими системи забезпечення кібербезпеки мають виступати і підсистеми кіберрозвідки та кібервпливу.

РОЗДІЛ 1. ІСТОРІЯ ДЕРЖАВНОГО КІБЕРЗАХИСТУ В УКРАЇНІ

1.1. Історія та зародження державного кіберзахисту в Україні

Історія та зародження державного кіберзахисту в Україні є складним процесом, який розвивався відповідно до зростаючих кіберзагроз та потреб держави у захисті критично важливих інформаційних ресурсів. Нижче наведено докладну історію та зародження державного кіберзахисту в Україні:

Початок незалежності (1991-2000): Після отримання незалежності, Україна стала стикатися з різноманітними викликами, включаючи потенційні кіберзагрози. Протягом перших років незалежності держава мала обмежені можливості в області кіберзахисту, але почала свідомо ставити це питання на порядок денний. Початок незалежності України в 1991 році означив початок нового етапу в історії країни, але і призначив ряд важливих викликів, включаючи й потенційні кіберзагрози. Після довгих років існування в складі Радянського Союзу, Україна отримала незалежність та почала будувати свою державність.

Проте, в період від 1991 до 2000 року, країна стикалася з численними проблемами, а кібербезпека стала однією з актуальних тем. На той час українська держава мала обмежені ресурси і можливості в області кіберзахисту. Важливим фактором було те, що технології та відомості про кіберзагрози були ще в ранніх стадіях розвитку, і велика частина суспільства не мала повного розуміння цих ризиків.

Однак уряд України виявив свідомість щодо необхідності звертати увагу на кіберзахист. Ініціативи з розвитку кібербезпеки були включені до порядку денного. Державні структури та спеціальні служби пристосовувалися до нових викликів і розробляли стратегії для захисту важливих інформаційних ресурсів. Важливою була не лише реакція на конкретні загрози, але і розвиток внутрішніх кіберзахисних здібностей.

Цей період в історії України поклав початок формуванню кібербезпечної інфраструктури, яка стала надзвичайно важливою в епоху інформаційних

технологій. Крок за кроком, країна розвивала свої технічні та правові засади для ефективного протистояння кіберзагрозам, що визначило подальший шлях у розвитку її кібербезпеки.

Створення відповідних органів (2000-2010): У цей період в Україні були створені перші органи, які займалися кіберзахистом на державному рівні. Зокрема, Міністерство внутрішніх справ та Служба безпеки України активно займалися боротьбою з кіберзлочинами та забезпеченням кіберзахисту важливих об'єктів. У період від 2000 до 2010 року в Україні були вжиті важливі заходи щодо створення спеціалізованих органів, які мали займатися кіберзахистом на державному рівні. Це був критичний етап у визнанні важливості кібербезпеки та створенні структур для ефективного протидії кіберзагрозам.

Міністерство внутрішніх справ (МВС) та Служба безпеки України (СБУ) стали ключовими гравцями у сфері кіберзахисту. Вони активно займалися виявленням, розслідуванням та запобіганням кіберзлочинам. Ці органи встановлювали тісні контакти з іншими правоохоронними агентствами та міжнародними партнерами для обміну інформацією та співпраці в області кібербезпеки.

Окрім того, протягом цього періоду в Україні створювалися спеціалізовані підрозділи, які фокусувались на кіберзахисті важливих об'єктів, інфраструктури та державних систем. Ці органи отримували завдання з забезпечення надійності та стійкості інформаційних систем, що були критичними для національної безпеки[3].

Важливим етапом став також розвиток правового базису, пов'язаного із кіберзахистом. Уряд України приймав закони та нормативні акти, які регулювали питання кібербезпеки та визначали відповідальність за кіберзлочини.

У цій десятирічній період Україна визнала необхідність системного підходу до кіберзахисту, і створення відповідних органів було ключовим

елементом стратегії країни для забезпечення інформаційної безпеки та захисту важливих інфраструктурних об'єктів.

Розвиток кіберзахистових структур (2010-2020): По мірі зростання обсягу кіберзагроз та розвитку інтернет-технологій, Україна активно розширювала свої зусилля в галузі кіберзахисту. У 2016 році була створена Національна служба кібербезпеки України (НСКБУ), яка стала важливим органом у цій сфері. З початку конфлікту на сході України та атаки на критичну інфраструктуру держави були ще більш актуальними. В період від 2010 до 2020 року Україна продовжувала активно розвивати свої кіберзахистові структури, ураховуючи зростання обсягу кіберзагроз та швидкий розвиток інтернет-технологій. Важливим кроком у цьому напрямку стало створення Національної служби кібербезпеки України (НСКБУ) у 2016 році.

Національна служба кібербезпеки України стала ключовим органом у сфері кіберзахисту. Її створення було відповіддю на зростання кількості та складності кіберзагроз, а також на необхідність координування заходів у сфері кібербезпеки на національному рівні. НСКБУ виконує завдання з розробки та реалізації стратегії кіберзахисту, сприяє співпраці між державними органами, приватним сектором та міжнародними партнерами.

З початком конфлікту на сході України та зростанням геополітичних напруг, атаки на критичну інфраструктуру країни стали ще більш актуальними. Кібератаки стали частиною гібридної війни, і Україна виявилася на передовій лінії цього боротьби. НСКБУ відігравала важливу роль у захисті державних інформаційних ресурсів, протидії кібершпигунам та злочинцям у кіберпросторі.

У цей період уряд України також продовжував вдосконалювати законодавство та нормативну базу в галузі кібербезпеки, щоб ефективно реагувати на сучасні кіберзагрози. Розвиток кіберзахистових структур став стратегічним напрямком для забезпечення національної безпеки України в умовах динамічного кіберсередовища.

Реакція на кібератаки (2014-нині): Зокрема після анексії Криму та подій на сході України було зафіксовано кілька значущих кібератак, включаючи

атаки на енергосистему та державні інституції. Ці події сприяли посиленню уваги до кіберзахисту і сприяли подальшому розвитку відповідних структур та стратегій. Починаючи з 2014 року та подій, пов'язаних із анексією Криму та конфліктом на сході України, країна стала свідком значущих кібератак, що внесли великий вклад у сприйняття кіберзахисту як ключової складової національної безпеки. Кібератаки стали елементом гібридної війни, в якій використовувалися технологічні засоби для досягнення політичних та стратегічних цілей.

Важливою точкою були атаки на енергосистему та державні інституції. Кіберзлочинці виявили інтерес до критично важливих об'єктів, спрямовуючи атаки на енергетичні мережі та інші інфраструктурні об'єкти. Це викликало серйозну загрозу для економіки та безпеки країни.

Реакція на ці кібератаки була важливою для забезпечення стійкості та безпеки України в кіберпросторі. Крім розгляду інцидентів та вжиття технічних заходів для ліквідації кіберзагроз, уряд активно звертав увагу до розвитку кіберзахистових стратегій та структур.

У 2014 році було створено Центр кіберзахисту, який став ключовим органом у сфері реагування на кіберзагрози та координації заходів з кіберзахисту. Діяльність цього центру включає в себе аналіз кіберзагроз, розробку превентивних заходів, а також координацію взаємодії між різними кіберзахисними організаціями та міжнародними партнерами.

Загальна свідомість про необхідність кіберзахисту значно зросла, а уряд України активно працював над удосконаленням законодавства та стратегій у цій області. Реакція на кібератаки стала каталізатором для подальшого розвитку кіберзахисту в Україні, а створені структури отримали додаткові повноваження та ресурси для ефективного протистояння сучасним кіберзагрозам.

Сучасні виклики і перспективи: На сьогоднішній день Україна активно працює над підвищенням свого кіберзахисту. Це включає в себе розвиток законодавства, співпрацю з міжнародними партнерами, підвищення

кваліфікації персоналу та впровадження сучасних технологій для виявлення та захисту від кіберзагроз.

Загалом, історія державного кіберзахисту в Україні відображає поступовий розвиток та вдосконалення заходів та інфраструктури для боротьби з кіберзагрозами та забезпечення безпеки в інтернеті[2].

1.2. Розвиток кіберзахисту в світі та його вплив на Україну

Розвиток кіберзахисту в світі в останні десятиліття вплинув на безпеку України в багатьох аспектах. Нижче наведено докладний огляд цього впливу.

Загальний рівень світового кіберзахисту: З ростом кількості кіберзагроз та кібератак в різних країнах світу, зростає і увага до кіберзахисту. Багато країн розвивають та посилюють свої зусилля в цій галузі, вдосконалюючи технології, законодавство та міжнародну співпрацю. Це створює позитивну обстановку для України, оскільки вона може взяти приклад з кращих практик та знань інших країн.

Міжнародна співпраця: У боротьбі з кіберзагрозами Україна активно співпрацює з іншими країнами та міжнародними організаціями. Це включає в себе обмін інформацією про загрози, спільні справи та розробку міжнародних стандартів безпеки. Світовий рівень кіберзахисту сприяє підвищенню спроможностей України у цьому напрямку.

Кібератаки та кібервійськові операції: Світовий розвиток кіберзахисту також відображається в рості кібератак та кібервійськових операцій, в тому числі тих, які впливають на Україну. Наприклад, Російська Федерація вже неодноразово вчиняла кібератаки на українські об'єкти, включаючи атаки на критичну інфраструктуру та державні установи. Це нагадує Україні про необхідність постійно підвищувати рівень кіберзахисту для захисту від таких загроз.

Розвиток кіберінфраструктури: Розвиток інтернет-технологій і кіберінфраструктури світу також впливає на Україну. З одного боку, це

створює нові можливості для розвитку галузей як інформаційних технологій, так і кіберзахисту. З іншого боку, це створює нові загрози від кібератак та кіберзлочинців.

Розвиток кібервійськових сил: Багато країн, включаючи Україну, активно розвивають кібервійськові сили для захисту національної безпеки в кіберпросторі. Ця тенденція спрямована на захист інформації та критичних інфраструктур від можливих кіберзагроз.

Загальносвітовий розвиток кіберзахисту має важливий вплив на безпеку України, яка вступає в нього активно, підвищуючи свої зусилля та здатності в цьому напрямку. Україна має свої власні виклики та загрози в галузі кіберзахисту, і міжнародний досвід та співпраця грають важливу роль в забезпеченні безпеки в кіберпросторі[4].

1.3. Стан державного кіберзахисту в Україні

Створення стратегій і політик:

У багатьох країнах, у тому числі і в Україні, держави визначають свої стратегії кіберзахисту та розробляють політику для ефективного управління цією сферою. Це може включати в себе утворення спеціальних організацій або підрозділів, які відповідають за кібербезпеку та реагування на інциденти.

Створення стратегій і політик у галузі кіберзахисту є ключовим елементом національної безпеки в умовах сучасного цифрового світу. Розглянемо, як у багатьох країнах, включаючи Україну, цей процес може виглядати:

Розробка стратегій кіберзахисту:

Уряди формують стратегії кіберзахисту, щоб визначити основні цілі, завдання та напрямки дій у галузі кібербезпеки. Ці стратегії можуть враховувати загальні виклики, такі як захист критично важливих інфраструктур, забезпечення кібербезпеки громадян та підприємств, і встановлення механізмів виявлення та реагування на кіберзагрози.

Утворення спеціальних організацій:

Багато країн створюють спеціальні органи або підрозділи, відповідальні за реалізацію стратегій кіберзахисту. Ці органи можуть включати державні агентства, служби, центри кіберзахисту та інші установи, які координують заходи з кібербезпеки.

Визначення відповідальності:

У стратегіях кіберзахисту чітко визначаються ролі та відповідальність різних суб'єктів, які взаємодіють у сфері кібербезпеки. Це може включати правоохоронні органи, військові структури, галузеві регулятори, а також приватний сектор.

Впровадження нормативно-правового регулювання:

Законодавство грає важливу роль у створенні ефективної системи кіберзахисту. Визначення норм та стандартів, а також встановлення відповідальності за порушення кібербезпеки, допомагає створити правовий фундамент для захисту інформації та кіберінфраструктури.

Співпраця з приватним сектором та іншими зацікавленими сторонами:

Ефективна стратегія кіберзахисту передбачає широку співпрацю з приватним сектором, громадськістю, академічними установами та міжнародними партнерами. Обмін інформацією та ресурсами з цими сторонами дозволяє виявляти та вирішувати загрози більш ефективно.

Оцінка та апгрейд стратегій:

Стратегії кіберзахисту повинні бути регулярно оцінюватися та апгрейджуватися, враховуючи зміни у кіберзагрозах, технологічному середовищі та інших факторах. Цей процес дозволяє стратегіям залишатися актуальними та ефективними[1],[5].

РОЗДІЛ 2. ТЕОРЕТИЧНІ АСПЕКТИ КІБЕР ЗАХИСТУ В ДЕРЖАВНИХ УСТАНОВАХ

2.1. Розробка політик безпеки інформації

Теоретичні аспекти кіберзахисту в державних установах охоплюють широкий спектр питань, що стосуються захисту інформації, мереж та інших кіберпросторових активів. Основні принципи та аспекти цієї галузі можна узагальнити наступним чином:

Інформаційна безпека: кіберзахист в державних установах починається з захисту конфіденційної, цінної інформації. Це включає в себе розробку та впровадження політик безпеки інформації, шифрування даних, контроль доступу і моніторинг подій.

Інформаційна безпека в державних установах є важливою складовою забезпечення захисту важливих даних та систем від кіберзагроз. Розглянемо більш детально кожен аспект цього заявлення.

Розробка та впровадження політик безпеки інформації:

- **Аудит безпеки:** Перший крок - це проведення аудиту безпеки, щоб зрозуміти поточний стан інформаційної безпеки. Це включає в себе оцінку ризиків, ідентифікацію слабких місць та аналіз заходів безпеки, що вже існують.
- **Розробка політик:** На основі результатів аудиту розробляються політики безпеки інформації, які визначають стандарти та процедури для захисту даних. Ці політики повинні враховувати вимоги законодавства, особливості організації та конфіденційність інформації.
- **Імплементация політик:** Розроблені політики впроваджуються в життя через тренінг персоналу, встановлення необхідних технічних засобів та створення процесів відповідно до них.

Розробка і впровадження цих елементів інформаційної безпеки створює надійний фундамент для ефективного кіберзахисту в державних установах, забезпечуючи захист конфіденційної інформації та зниження ризиків кібератак.

Кібергігієна це освіта та тренінг персоналу в сфері кібербезпеки є ключовим елементом. Працівники державних установ повинні бути осведомлені про потенційні кіберзагрози, знати профілактичні заходи та вміти реагувати на інциденти. Кібергігієна в державних установах виступає як важлива складова для забезпечення високого рівня кібербезпеки, і її успішність залежить від свідомості та готовності персоналу до дій в кіберпросторі. Розглянемо кожен аспект цього елементу більш детально:

1.Освіта та тренінг персоналу:

- **Свідомість про кіберзагрози:** Працівники державних установ повинні бути освічені про різновиди кіберзагроз, їхні характеристики та потенційні наслідки для інформаційної безпеки. Це включає у себе навчання про типові шахраїства, фішингові атаки, віруси та інші загрози.

- **Знання профілактичних заходів:** Персонал повинен мати чітке розуміння профілактичних заходів і можливостей запобігання кіберзагрозам. Це може включати в себе правила безпеки паролів, оновлення програмного забезпечення, використання безпечних мереж і т. д.

2.Готовність реагування на інциденти:

- **Тренування на симуляторах:** Проведення тренувань та симуляцій кібератак для підготовки персоналу до реальних ситуацій. Це дозволяє працівникам навчитися визначати та ефективно реагувати на інциденти.

- **Плани евакуації та відновлення:** Розробка планів дій у випадку кіберінциденту, включаючи процедури евакуації, відновлення роботи та співпрацю зі спеціалізованими службами.

3.Системи своєчасного сповіщення:

- **Сповіщення та інформування персоналу:** Забезпечення систем сповіщення та інформування персоналу про поточні кіберзагрози та надання конкретних рекомендацій щодо захисту.

- **Співпраця із службами безпеки:** Забезпечення ефективної взаємодії з внутрішніми та зовнішніми службами безпеки для обміну інформацією та координації заходів в разі інциденту.

Глибока освіта та систематичні тренування персоналу створюють обізнаності та підготовку до дій в обличчя кіберзагроз. Важливо, щоб працівники державних установ були не лише свідомі про потенційні ризики, але й готові ефективно реагувати, максимально зменшуючи можливі наслідки для інформаційної безпеки.

Технічні заходи: Використання технічних засобів для захисту мереж, систем і даних. Це включає в себе встановлення і оновлення антивірусного програмного забезпечення, мережевих брандмауерів, систем виявлення вторгнень та інших засобів кіберзахисту.

Технічні заходи в області кіберзахисту грають важливу роль у створенні ефективної системи захисту мереж, систем та даних у державних установах. Ці технічні заходи об'єднуються для створення надійної системи кіберзахисту, яка забезпечує виявлення, запобігання та реагування на потенційні кіберзагрози в державних установах.

Стратегії реагування на інциденти: Державні установи повинні розробляти та впроваджувати стратегії для реагування на кіберінциденти. Це включає в себе плани відновлення роботи, ізоляцію інфікованих систем і розслідування інцидентів. Стратегії реагування на кіберінциденти в державних установах включають комплекс заходів, спрямованих на ефективне виявлення, обмеження та відновлення внаслідок кібератак[6],[8],[22].

2.2 Основні принципи та підходи до кіберзахисту

Кіберзахист є важливою складовою сучасного управління інформаційною безпекою. Основні принципи та підходи до кіберзахисту включають:

1.Принцип обов'язковості:

Кіберзахист має бути обов'язковим елементом для всіх систем та організацій, що використовують інформаційні технології. Реалізація стандартів безпеки, викладених у внутрішніх та міжнародних політиках безпеки.

2.Принцип стратегічності:

Кіберзахист повинен бути вбудованим у стратегічні цілі та плани розвитку організації. Розробка стратегічних документів, що враховують аспекти кібербезпеки, і взаємодія з бізнес-процесами.

3.Принцип комплексності:

Кіберзахист повинен охоплювати всі аспекти інформаційної інфраструктури, включаючи апаратне забезпечення, програмне забезпечення, персонал та процеси. Регулярне аудиторське оцінювання всіх аспектів системи для виявлення потенційних слабких місць.

4.Принцип доступності та продуктивності:

Кіберзахист має не тільки забезпечувати безпеку, але і не заважати нормальному функціонуванню систем та організацій. Впровадження заходів безпеки, які не ускладнюють роботу користувачів та процесів.

5.Принцип постійності:

Кіберзахист повинен бути неперервним процесом, а не винятковою подією. Регулярне оновлення та адаптація заходів кіберзахисту до змін у загрозах та технологіях.

6.Принцип захисту від внутрішніх та зовнішніх загроз:

Кіберзахист повинен враховувати як зовнішні, так і внутрішні загрози, включаючи навмисний та ненавмисний внутрішній доступ. Встановлення механізмів виявлення та запобігання інсайдерським загрозам.

7.Принцип найменшого привілею (Principle of Least Privilege - POLP):

Користувачам та системам має надаватися тільки та мінімальна кількість привілеїв, необхідних для виконання їхніх обов'язків. Суворе управління правами доступу та обмеження привілеїв.

8.Принцип безпеки за умовчанням (Security by Default):

Системи та програми повинні бути налаштовані для максимальної безпеки за замовчуванням. Встановлення стандартних налаштувань безпеки та вимог для нових систем.

Ці принципи становлять основу ефективної стратегії кіберзахисту, дозволяючи забезпечити безпеку інформаційних ресурсів та мінімізувати ризики для організацій та користувачів[11].

2.3 Особливості застосування кіберзахисту в державних установах

Застосування кіберзахисту в державних установах має свої власні особливості, які обумовлені специфікою їхньої діяльності та відповідальністю перед громадянами. Розглянемо ці особливості більш детально:

1.Чутлива інформація та конфіденційність:

Державні установи часто мають доступ до великої кількості чутливої інформації, такої як персональні дані громадян, державні секрети, фінансові дані тощо. Використання механізмів шифрування, строгий контроль доступу та моніторинг для забезпечення конфіденційності.

2.Обмежений бюджет та фінансові обмеження:

Державні установи часто опірні до обмежень бюджету, що може впливати на можливість впровадження дорогих заходів кіберзахисту. Ефективне управління ресурсами, визначення пріоритетів та використання вартісних та ефективних рішень.

3.Специфіка Кіберзагроз та Шпигунства:

Державні установи можуть бути об'єктами спроб кібершпигунства, кібертероризму та інших розроблених атак. Розробка та впровадження заходів кіберзахисту, що враховують специфіку державної інформації та взаємодію з агентствами національної безпеки.

4.Важливість інфраструктури та публічних послуг:

Багато державних установ відповідають за ключові функції та інфраструктуру, яка є важливою для функціонування країни. Впровадження високодоступних та відмовостійких систем, регулярні бекапи та відновлення, а також системи моніторингу для своєчасного виявлення аномалій.

5.Політичні та Правові Обмеження:

Державні установи повинні дотримуватися політичних та правових обмежень, що може впливати на вибір та впровадження кіберзахисних заходів. Розробка стратегій кіберзахисту, які враховують політичні та правові вимоги, та регулярне оновлення політик відповідно до змін.

6.Внутрішня інфраструктура та користувачі:

Велика кількість користувачів та різноманітні об'єкти державних установ потребують ефективного управління доступом та захисту. Використання систем управління ідентифікацією та аутентифікацією, централізованого управління доступом та ефективної архітектури безпеки.

7.Міжнародне співробітництво та стандартизація:

Державні установи можуть бути предметами міжнародних кіберзагроз, підкреслюючи необхідність співпраці з іншими країнами та міжнародними організаціями. Активна участь у міжнародних ініціативах та обмін інформацією для спільного реагування на кіберзагрози.

Забезпечення кібербезпеки в державних установах вимагає комплексного підходу, який враховує їхні особливості та гарантує надійний захист чутливої інформації та критичної інфраструктури[21],[33].

РОЗДІЛ 3. ПРОТОТИП СИСТЕМИ КІБЕР ЗАХИСТУ ДЕРЖАВНОЇ УСТАНОВИ НА БАЗІ УСТАТКУВАННЯ CISCO

3.1. Прототип системи кіберзахисту на базі устаткування Cisco

Прототип системи кіберзахисту на базі устаткування Cisco, як державної установи передбачає використання обладнання, програмного забезпечення та методологій, розроблених компанією Cisco, для побудови ефективної системи захисту комп'ютерної мережі. Cisco визнана світовим лідером у галузі мережевих технологій, і її продукти широко використовуються для створення надійних та безпечних мереж у різних сферах, включаючи державні установи.

(Рис.3.1) Використовується обладнання на прикладі Firewalls Cisco ASA 5516-X



Рис.3.1 Firewalls Cisco ASA 5516-X

(Рис.3.2) Має такі технічні характеристики:

Dimensions (H x W x D) 1.72 x 17.2 x 11.288 inches (4.369 x 43.688 x 28.672 cm)	Packets per second (64 byte) 750000
Serial ports 1 RJ-45 and Mini USB console	Maximum heat dissipation 123 BTU/hr
Power input (per power supply) AC current 0.25AC amps	Weight 8 lb (3 kg) with AC power supply
Integrated I/O 8 x 1 GE	VLANs 100
Memory 8 GB	Application control (AVC) or NGIPS sizing throughput (440-byte HTTP) 300 Mbps
Dual power supplies Not Available	Maximum new connections per second 20000
High-availability support Active/active and active/standby	Dedicated management port Yes (To be shared with with FirePOWER Services), 10/100/1000
Maximum AVC and NGIPS throughput 600 Mbps	Expansion I/O Not Available
Cisco Cloud Web Security users 2000	Weight (with AC power supply) 8 lb (3 kg)
Operating Acoustic Noise 41.6 A-weighted decibels (dBA) type, 67.2 dBA max	Stateful inspection throughput (max) 1.8 Gbps
Maximum application visibility and control (AVC) throughput 850 Mbps	Output Maximum Peak 12V @ 5.0A
Maximum 3DES/AES VPN throughput 250 Mbps	USB 2.0 Ports USB port type  , High Speed 2.0
Maximum site-to-site and IPsec IKEv1 client VPN user sessions 300	Minimum system flash 8 GB
Output steady state 12V @ 3.0A	Stateful inspection throughput (multiprotocol) 900 Mbps
Maximum Cisco AnyConnect IKEv2 remote access VPN or clientless VPN user sessions 300	Power AC Only
Solid-state drive 100 GB mSata	Maximum concurrent sessions 250000
Form factor 1 rack unit (RU), 19-in. rack-mountable	

(Рис.3.3) Щоб почати співпрацювати безпосередньо із Firewalls Cisco ASA 5516-X, будемо використовувати таке програмне забезпечення – Cisco ASDM Launcher



Рис.3.3 Основні елементи Cisco, які можуть бути використані в системі кіберзахисту державної установи:

1. Cisco ASA (Adaptive Security Appliance):

ASA є апаратним та програмним засобом, призначеним для захисту комп'ютерних мереж від різноманітних кіберзагроз. Вона надає функціонал

фірмового мережевого брандмауера, VPN, антивірусного захисту та системи виявлення вторгнень (IDS).

Приклад мережі:

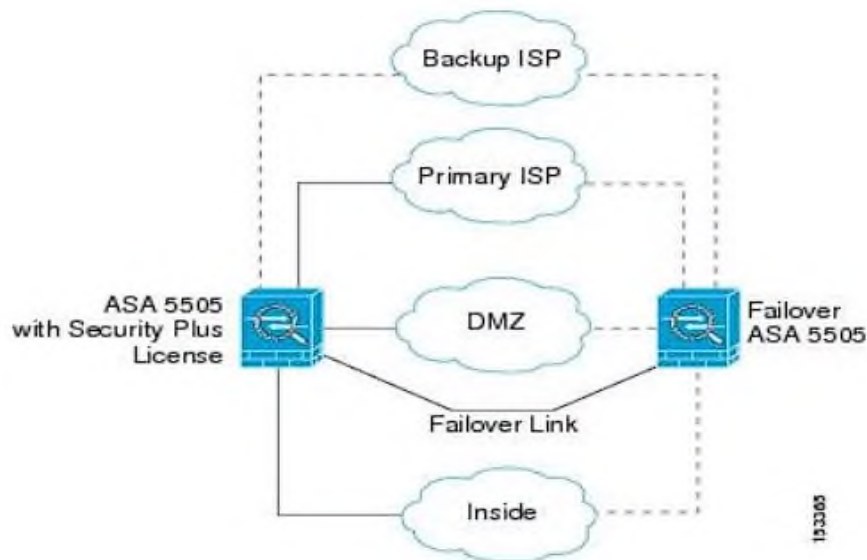
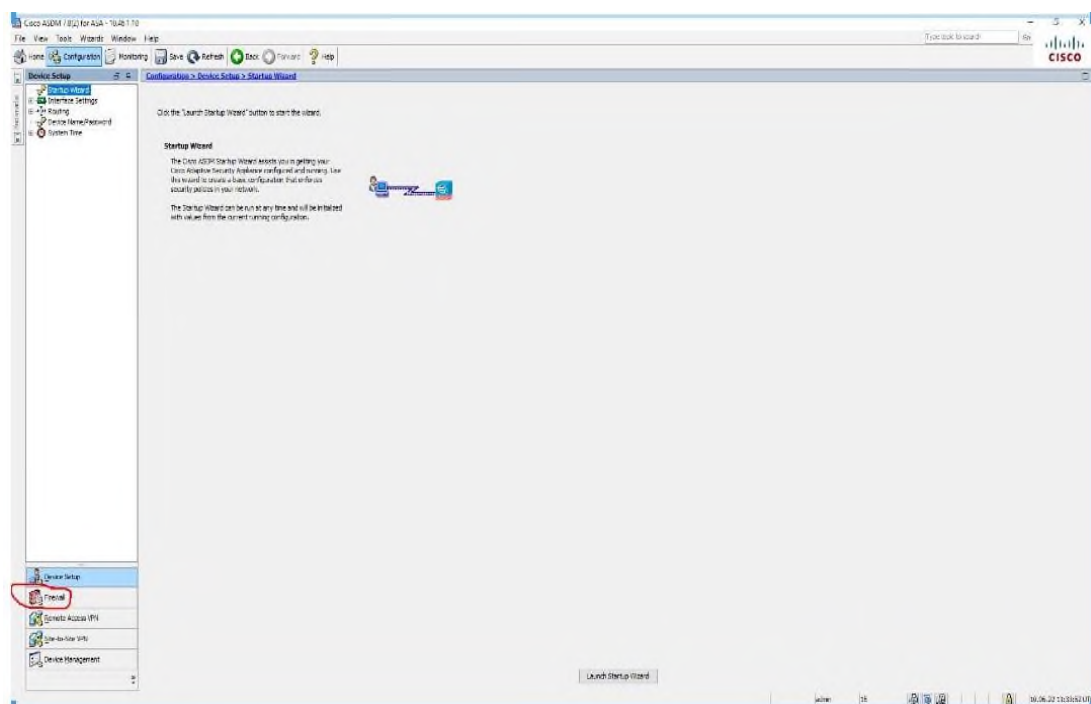


Рис. 3.4. Cisco Firepower:

Firepower - це інтегрована система безпеки, яка комбінує в собі брандмауер, IPS (інтрузійна система запобігання), антивірусний захист та інші функції. Вона надає високий рівень захисту від кіберзагроз та дозволяє ефективно виявляти та реагувати на інциденти.

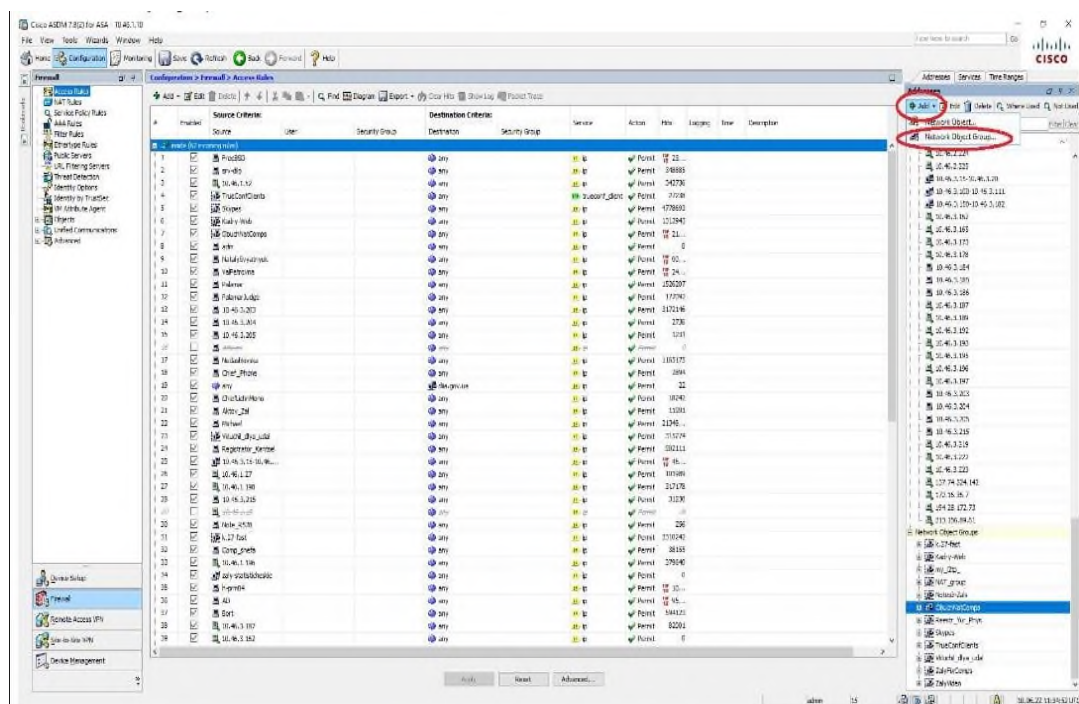


Cisco Umbrella:

Umbrella - це хмарний сервіс для захисту від вірусів та інших загроз в інтернеті. Він може блокувати шкідливий трафік ще до того, як він потрапить в корпоративну мережу.

4.Cisco Identity Services Engine (ISE):

ISE надає контроль доступу до мережі та автоматизоване управління ідентифікацією користувачів та пристроїв. Це дозволяє управляти правами доступу та підвищує безпеку мережі.



Cisco Stealthwatch:

Stealthwatch використовує технології аналізу мережевого трафіку для виявлення аномальної поведінки та потенційних загроз безпеки[36],[37].

3.2. Аналіз можливостей устаткування Cisco для кіберзахисту

Аналіз можливостей Cisco для кіберзахисту:

1.Брандмауер та VPN-захист:

Cisco ASA (Adaptive Security Appliance) є потужним брандмауером, який забезпечує контроль доступу до мережі та виявлення та запобігання загрозам.

Також, ASA інтегрує в себе VPN-технології для безпечного з'єднання та забезпечення конфіденційності даних у віртуальних приватних мережах.

Брандмауер та VPN-захист Cisco ASA (Adaptive Security Appliance). Cisco ASA, об'єднуючи в собі брандмауер та VPN-захист, є комплексним рішенням для забезпечення безпеки мережі та конфіденційності даних. Його розширені можливості, інтеграція функцій та підтримка сучасних технологій роблять його ефективним інструментом для державних установ та підприємств.

2. Інтрुзійна система запобігання (IPS):

Cisco пропонує рішення з інтрुзійної системи запобігання, такі як Cisco Firepower, які аналізують трафік на предмет підозрілих дій та автоматично реагують на потенційні загрози.

Інтрुзійна система запобігання (IPS) в сучасних мережах є важливим елементом для забезпечення безпеки. Cisco пропонує розширені рішення з інтрुзійного контролю, такі як Cisco Firepower, які включають в себе ряд функцій та технологій для виявлення та запобігання кіберзагрозам.

Основні аспекти Інтрुзійної Системи Запобігання Cisco:

1. Детектори та сигнатури:

Інтрुзійна система Cisco використовує обширну базу даних сигнатур для виявлення відомих загроз. Ці сигнатури представляють собою унікальні характеристики вже відомих типів атак, так що їх можна легко розпізнати та блокувати.

2. Аналіз трафіку:

IPS аналізує мережевий трафік в режимі реального часу, використовуючи глибокий пакетний аналіз. Це дозволяє виявляти непередбачувані або нові загрози, які можуть не бути відомими за допомогою звичайних сигнатур.

3. Технології протидії вторгненням:

Cisco Firepower використовує різні технології протидії вторгненням, такі як блокування піддоменів, аналіз глибоких пакетів, та інші, щоб заваджати атакам та взломам.

4.Аналіз поведінки:

Системи аналізу поведінки визначають аномальну активність або несподівані зміни у мережевому трафіку, що може вказувати на нові атаки або невідомі загрози.

5.Блокування загроз у реальному часі:

Коли система виявляє підозрілу активність або вторгнення, вона має можливість негайно реагувати та блокувати цільовий трафік для захисту мережі в реальному часі.

6.Інтеграція з іншими системами:

Cisco IPS може інтегруватися з іншими системами безпеки, такими як системи управління подіями та інцидентами (SIEM), щоб забезпечити централізоване керування та аналіз.

7.Захист від атак з використанням вразливостей:

IPS виявляє та блокує атаки, спрямовані на використання вразливостей програмного забезпечення, забезпечуючи захист від експлойтів та небезпечних програм.

8.Оновлення бази сигнатур:

Система регулярно отримує оновлення сигнатур для розпізнавання нових загроз та атак.

Значення Інтрुзійної Системи Запобігання:

1.Попередження вторгнень:

IPS дозволяє попереджати атаки та вторгнення до того, як вони можуть завдати шкоди мережі.

2.Швидка реакція:

Здатність реагувати в реальному часі дозволяє швидко блокувати атаки та нейтралізувати загрози.

3.Мінімізація ризиків:

IPS допомагає у мінімізації ризиків та втрат, пов'язаних з кіберзагрозами та атаками.

4.Захист від нових загроз:

Аналіз поведінки та глибокий пакетний аналіз дозволяють виявляти нові атаки та загрози, які можуть бути невідомими за допомогою традиційних сигнатур.

Інтрुзійна система запобігання Cisco є важливим елементом комплексної стратегії кіберзахисту, надаючи ефективний захист від різноманітних кіберзагроз.

3.Антивірусний захист:

У складі Cisco Firepower та інших рішень використовуються антивірусні та антimalware функції для виявлення та блокування шкідливого програмного забезпечення. Антивірусний захист в рамках Cisco Firepower є однією з важливих функцій, спрямованих на захист мережі та пристроїв від шкідливих програм і загроз. Cisco Firepower використовує інтегровані технології для виявлення та блокування вірусів, троянів, шпигунського ПЗ та інших форм шкідливого програмного забезпечення.

Основні характеристики антивірусного захисту у Cisco Firepower:

1.Система виявлення вірусів:

Cisco Firepower використовує сигнатури та патерни вірусів для виявлення відомих шкідливих програм. Сигнатури - це унікальні характеристики, які ідентифікують конкретні віруси або форми шкідливого коду.

2.Аналіз поведінки:

Антивірусний модуль Cisco Firepower може аналізувати поведінку програм для виявлення аномалій, які можуть вказувати на наявність вірусів або інших загроз.

3.Інтеграція з базою даних загроз:

Вірусні сигнатури та патерни регулярно оновлюються з централізованих баз даних загроз, що дозволяє системі ефективно виявляти нові та еволюційні віруси.

4.Глибокий пакетний аналіз:

Антивірусний двигун Cisco Firepower використовує глибокий пакетний аналіз для ретельного дослідження мережевого трафіку та виявлення прихованих загроз, що можуть бути присутні в різних рівнях комунікації.

5.Інтеграція з іншими функціями безпеки:

Антивірусний захист взаємодіє з іншими компонентами безпеки Cisco Firepower, такими як брандмауер, системи виявлення вторгнень (IDS/IPS), що робить його частиною комплексного підходу до кіберзахисту.

6.Блокування вірусів в реальному часі:

Як тільки антивірусний двигун виявляє вірус чи іншу шкідливу програму, він може негайно реагувати і заблокувати спробу інфікувати систему чи мережу.

7.Автоматичне вилікування та карантин:

Cisco Firepower може автоматично намагатися вилікувати заражені файли чи видалити їх у карантин для подальшого аналізу та блокування.

8.Моніторинг та звітність:

Пристрій надає можливості моніторингу та звітності щодо виявлених вірусів, що допомагає адміністраторам відстежувати та реагувати на потенційні загрози.

Значення антивірусного захисту в Cisco Firepower:

1.Захист від широкого спектру загроз:

Антивірусний захист в складі Cisco Firepower надає захист від різних форм шкідливого програмного забезпечення, забезпечуючи повноцінний захист.

2.Швидка відповідь на загрози:

Можливість блокування вірусів в реальному часі дозволяє швидко відреагувати на потенційні загрози та запобігти їхньому поширенню в мережі.

3.Оновлення та динамічна адаптація:

Система регулярно оновлюється, щоб враховувати нові форми вірусів та шкідливого ПЗ, забезпечуючи актуальний захист.

4.Синергія з іншими функціями безпеки:

Антивірусний захист інтегрований з іншими функціями Cisco Firepower для максимальної ефективності та обсяговості захисту.

5.Моніторинг та аналіз:

Можливості моніторингу дозволяють відслідковувати події та виявлені загрози, а аналітичні засоби надають детальний аналіз виявлених вірусів та їхніх впливів на мережу. Антивірусний захист у Cisco Firepower є ключовою складовою для забезпечення високого рівня безпеки та ефективного управління кіберзагрозами в сучасних мережах.

Захист від витоків даних:

Cisco представляє рішення, такі як Cisco Umbrella, які виявляють та запобігають витокам конфіденційної інформації, забезпечуючи захист від зловмисних атак та втрат даних.

Захист від витоків даних є важливим аспектом в сучасному кіберпросторі, особливо зростанням кількості загроз інформаційної безпеки. Cisco Umbrella - це інноваційний продукт, розроблений для забезпечення ефективного захисту від витоків даних.

Роль Cisco Umbrella в захисті від витоків даних:

Cisco Umbrella виступає як хмаровий сервіс безпеки, зосереджений на захисті від різних загроз, включаючи витoki даних. Основні функції і характеристики дозволяють системі ефективно виявляти та запобігати потенційним загрозам.

Основні функції та характеристики:

DNS-фільтрація:

Блокування шкідливих запитань: Umbrella використовує DNS-фільтрацію для аналізу DNS-запитів і блокує доступ до небезпечних доменів, запобігаючи витокам даних через інфіковані ресурси.

Захист від Malware та Phishing:

Виявлення шкідливих доменів: Umbrella використовує інтелектуальні алгоритми для виявлення malware та фішингових атак на рівні DNS, що дозволяє блокувати доступ до потенційно небезпечних ресурсів.

Захист від Ransomware:

Блокування веб-сайтів зі шкідливим змістом: Umbrella запобігає доступу до веб-сайтів, які можуть розповсюджувати ransomware та інші види шкідливих програм.

Захист на рівні кінцевих пристроїв:

Безпека на всіх рівнях: Umbrella не лише забезпечує захист на рівні DNS, але й доповнює це захистом на рівні кінцевих пристроїв, створюючи повноцінний захист мережі.

Переваги Cisco Umbrella:

1.Глобальна інтелігенція:

База даних загроз: Umbrella користується глобальною базою даних загроз, що дозволяє виявляти нові загрози та ефективно реагувати на них.

2.Миттєва реакція:

В реальному часі: Umbrella діє в реальному часі, блокуючи доступ до небезпечних ресурсів миттєво, щоб завчасно запобігти можливим витокам даних.

3.Зручність управління:

Централізоване управління: Адміністратори можуть централізовано керувати політиками безпеки та моніторити загрози через єдиний інтерфейс, що полегшує управління безпекою.

Захист від витоків даних, реалізований за допомогою Cisco Umbrella, визначається його широким функціоналом, глобальною інтелігенцією та зручністю управління, забезпечуючи комплексний захист від різних загроз та підвищуючи рівень безпеки в організаціях.

4.Ідентифікація та контроль доступу:

Cisco Identity Services Engine (ISE) використовується для централізованої ідентифікації та автоматизованого контролю доступу, забезпечуючи безпеку користувачів та пристроїв, які підключаються до мережі.

Cisco Identity Services Engine (ISE) - це рішення для ідентифікації та контролю доступу, яке дозволяє організаціям ефективно управляти доступом

користувачів до мережевих ресурсів. Нижче розглянуті ключові функції та характеристики Cisco ISE.

Основні Функції та Характеристики:

1.Ідентифікація та автентифікація:

- Централізована ідентифікація: ISE забезпечує централізовану ідентифікацію користувачів та пристроїв у мережі.
- Автентифікація користувачів: Підтримка різних методів автентифікації, таких як 802.1X, MAB (MAC Authentication Bypass), EAP (Extensible Authentication Protocol), що робить систему гнучкою.

2.Авторизація та політика доступу:

- Централізована авторизація: ISE надає можливість централізованої авторизації для визначення прав доступу користувачів.
- Визначення політик доступу: Можливість встановлення гнучких політик доступу, враховуючи атрибути користувача та пристрою.

3.Інтеграція з джерелами даних:

- LDAP, AD і інші системи: ISE може інтегруватися з різними джерелами даних, такими як Active Directory, LDAP, для одержання інформації про користувачів.

4.Гостьовий доступ:

- Гостьовий портал: Вбудований гостьовий портал для безпечного та зручного управління доступом гостей до мережі.

5.Моніторинг та звітність:

- Система моніторингу: Можливість моніторити активність користувачів та пристроїв у реальному часі.
- Звітність: Надає засоби для створення звітів про активність та події в мережі для аналізу та виявлення аномалій.

Переваги Cisco ISE:

Централізована управлінська панель:

- Управління з одного інтерфейсу: Забезпечення централізованого управління доступом через один інтерфейс для всієї мережі.

Безпека та відповідність:

- Система відповідності: Можливість визначати політики для відповідності з безпековими стандартами та регуляторами.

Гнучкість та розширюваність:

- Гнучкі політики: Можливість налаштовувати та змінювати політики в залежності від потреб організації.
- Розширюваність: Здатність масштабуватися для обслуговування великої кількості користувачів та пристроїв.

Cisco ISE є потужним інструментом для ідентифікації та контролю доступу, що надає організаціям засоби ефективного управління безпекою мережі, забезпечуючи гнучкість, розширюваність та централізований контроль.

6.Моніторинг мережі:

Cisco Stealthwatch використовує аналіз мережевого трафіку для виявлення непередбачуваної або аномальної активності, що допомагає у вчасному виявленні потенційних загроз. Cisco Stealthwatch - це рішення для моніторингу та аналізу мережевої активності, яке дозволяє виявляти аномальну поведінку, загрози та атаки в реальному часі. Давайте розглянемо деталі його функцій та характеристик:

1. Аналіз поведінки та виявлення загроз:

Аналіз трафіку: Stealthwatch аналізує мережевий трафік для виявлення нормальної та аномальної активності.

Моделювання поведінки: Використання алгоритмів для створення моделей поведінки пристроїв та користувачів.

2. Виявлення інцидентів та атак:

Система виявлення загроз: Stealthwatch використовує систему виявлення загроз для розпізнавання підозрілих або зловмисних дій.

Контекстуальний аналіз: Враховує контекст, такий як користувачі, пристрої та додатки для точного виявлення аномалій.

3. Аналіз трафіку та перформансу:

Моніторинг трафіку: Stealthwatch надає деталізовану інформацію про трафік на рівні користувачів, додатків та пристроїв.

Аналіз пропускної здатності: Вимірює пропускну здатність та виявляє можливі проблеми з мережевою ефективністю.

4. Інтеграція з джерелами даних:

Інтеграція з Cisco устаткуванням: Stealthwatch легко інтегрується з іншими продуктами Cisco, такими як Cisco Identity Services Engine (ISE) та Cisco Firepower, для отримання повноцінного захисту.

5. Розширена аналітика та звітність:

Аналітика на основі машинного навчання: Використання алгоритмів машинного навчання для розпізнавання змін у поведінці та нових загроз.

Гнучкі засоби звітності: Надання різноманітних звітів для аналізу активності та виявлення потенційних проблем.

6. Захист від витоків даних:

Розпізнавання витоків: Stealthwatch виявляє надто активних користувачів чи пристрої, що може свідчити про можливий витік даних.

Контроль інформаційних потоків: Можливість встановлювати політики для контролю за потоками даних та їх обмеженням.

7. Захист критичної інфраструктури:

Виявлення атак на KI: Stealthwatch допомагає виявляти атаки на критичну інфраструктуру, запобігаючи можливим серйозним наслідкам.

8. Переваги Cisco Stealthwatch:

Глибока візуалізація: Stealthwatch надає глибоку візуалізацію мережевої активності для швидкого виявлення проблем та загроз.

Розширена інтеграція: Інтеграція з Cisco Threat Response та іншими інструментами для автоматизації реакції на загрози.

Cisco Stealthwatch дозволяє підприємствам ефективно виявляти та вирішувати проблеми безпеки та аномальної активності в мережі, забезпечуючи високий рівень захисту від загроз.

Хмарні рішення:

Cisco Umbrella є хмарним сервісом, який забезпечує безпеку при використанні хмарових послуг та дозволяє ефективно блокувати шкідливий трафік з хмари.

Аналіз та виявлення загроз:

Рішення Cisco включають інтелектуальні системи аналізу, які виявляють та аналізують потенційні загрози, що дозволяє оперативно реагувати на нові та еволюючі кіберзагрози. Cisco пропонує різноманітні рішення для аналізу та виявлення загроз, спрямовані на забезпечення безпеки інфраструктури та даних підприємства. Давайте розглянемо деталі деяких з цих рішень:

1. Cisco Threat Response:

Опис: Cisco Threat Response - це інтегрована система, яка об'єднує дані з різних джерел для виявлення та реагування на кіберзагрози.

Функції та характеристики:

Централізований огляд: Подання всебічного огляду загроз та їхніх характеристик.

Автоматизована відповідь: Можливість автоматизованої відповіді на ідентифіковані загрози.

Інтеграція з різними джерелами: Об'єднання інформації з Cisco Security, а також з інших джерел, для повного розуміння загроз.

Пошук та розслідування: Зручний пошук та розслідування подій та загроз для подальшого аналізу.

2. Cisco Firepower Threat Defense (FTD):

Опис: Cisco FTD - це інтегрована платформа, яка комбінує функціональність брандмауера та системи виявлення і запобігання вторгненням (IDS/IPS).

Функції та характеристики:

Брандмауер: Керування трафіком та застосуванням політик безпеки на рівні мережі.

IDS/IPS: Виявлення та блокування атак на рівні інтрузійної системи запобігання (IPS).

Система виявлення загроз: Здатність виявляти важкі для виявлення загрози та небезпечні патерни поведінки.

3. Cisco Stealthwatch:

Опис: Cisco Stealthwatch - це рішення для аналізу та моніторингу мережі для виявлення аномальної активності та загроз.

Функції та характеристики:

Мережевий аналіз: Виявлення змін у поведінці мережі та ідентифікація потенційно небезпечних дій.

Система виявлення загроз: Використання машинного навчання для виявлення нових та розширених загроз.

Інтеграція з Cisco ISE: Оптимізована інтеграція з Cisco Identity Services Engine для контролю доступу та ідентифікації користувачів.

4. Cisco Umbrella:

Опис: Cisco Umbrella - хмаровий сервіс безпеки, який забезпечує захист від загроз відразу на рівні DNS.

Функції та характеристики:

DNS-фільтрація: Виявлення та блокування шкідливих DNS-запитань.

Захист від Malware та Phishing: Боротьба із вірусами, рансомварами та фішинговими атаками.

Гнучкі політики: Можливість налаштовувати політики безпеки в залежності від потреб.

Ці рішення взаємодіють між собою та інтегруються для надання комплексного захисту від сучасних кіберзагроз.

Підтримка масштабування:

Продукти Cisco розроблені з урахуванням можливостей масштабування, що робить їх ідеальними для використання в різних розмірах мереж, включаючи великі державні установи. Cisco надає широкий спектр продуктів та рішень, які розроблені з урахуванням можливості масштабування, тобто здатності системи рости зі збільшенням обсягу завдань, користувачів чи даних.

Розглянемо основні аспекти підтримки масштабування в екосистемі

Cisco:

1. Мережеві рішення:

- Cisco Nexus: Cisco Nexus - це портфель комутаторів та маршрутизаторів, спроектованих для високопродуктивних мережевих середовищ, які можуть легко масштабуватися для вирішення вимог інтенсивних застосунків.

- Cisco Catalyst: Комутатори Cisco Catalyst розроблені для надійності та ефективності мережі, а їхня архітектура дозволяє легко розширювати мережеві можливості.

2. Системи зберігання даних:

- Cisco MDS: Для області зберігання даних, Cisco MDS (Multilayer Director Switches) надає високопродуктивні та масштабовані рішення для Fibre Channel.

- Cisco UCS: В області обчислювальних систем Cisco UCS (Unified Computing System) забезпечує масштабовану архітектуру серверів для оптимізації обчислень у великих дата-центрах.

3. Системи безпеки:

- Cisco ASA: Апаратно-програмне забезпечення Cisco ASA (Adaptive Security Appliance) надає захист від кіберзагроз і має можливості масштабування для різних обсягів мережевого трафіку.

- Cisco Firepower: Рішення Cisco Firepower, яке об'єднує в собі систему виявлення і запобігання інтрузіям (IDS/IPS) та брандмауер, розроблено з урахуванням масштабованості для захисту великих і складних мереж.

4. Cisco SD-WAN:

- Cisco Viptela SD-WAN: Для оптимізації роботи корпоративних мереж, Cisco пропонує SD-WAN рішення, таке як Cisco Viptela SD-WAN, яке дозволяє легко масштабувати мережу і управляти її ресурсами.

5. Хмарові рішення:

- Cisco Cloud Services: Cisco також пропонує різноманітні хмарові послуги та рішення, такі як Cisco Webex та Cisco Meraki, які легко масштабуються для забезпечення обсягів користувачів та пристроїв.

6. Cisco ACI (Application Centric Infrastructure):

- ACI: Cisco ACI - це рішення для управління дата-центром, яке дозволяє автоматизовано керувати інфраструктурою і масштабувати її залежно від потреб застосунків.

7. Cisco DNA (Digital Network Architecture):

- Cisco DNA Center: Центр управління мережею Cisco DNA є централізованим місцем для конфігурації, визначення політик та моніторингу мережі, забезпечуючи масштабованість для різних мережевих середовищ.

Масштабування в продуктах та рішеннях Cisco враховує потреби сучасних бізнесів, де важливо забезпечити стабільну та ефективну роботу в умовах постійно зростаючих обсягів даних та користувачів.

Система управління подіями та інцидентами (SIEM):

Cisco може інтегруватися з SIEM-системами, що дозволяє ефективно виявляти, реєструвати та реагувати на інциденти в області кібербезпеки. Система управління подіями та інцидентами (SIEM) представляє собою комплексне програмне забезпечення, яке дозволяє збирати, аналізувати та реагувати на події в інформаційній системі. Основна мета SIEM - забезпечити централізований механізм моніторингу та реагування на події, які можуть свідчити про кіберзагрози або вказувати на проблеми безпеки.

Основні складові SIEM-системи та їх функції:

1.Збір та нормалізація даних:

Збір Логів: SIEM збирає лог-файли з різних джерел в мережі, таких як сервери, мережеві пристрої, програмне забезпечення безпеки і т. д.

Нормалізація даних: Дані стандартизуються та нормалізуються для спрощення їхнього аналізу та порівняння.

2.Кореляція подій:

Пошук Зв'язків: SIEM використовує правила та алгоритми для виявлення зв'язків між різними подіями, що може свідчити про складні атаки або інші безпекові проблеми.

3. Аналіз та виявлення загроз:

Машинне навчання: Сучасні SIEM-системи можуть використовувати методи машинного навчання для виявлення аномалій та нестандартної поведінки.

Пошук аномалій: SIEM виявляє аномалії та високоризикові події, що може свідчити про потенційні загрози.

4. Відповідь на інциденти:

Попередження та сповіщення: SIEM може надсилати сповіщення адміністраторам про небезпечні події або можливі атаки.

Автоматизована відповідь: Деякі системи можуть автоматично виконувати певні дії для реагування на інциденти.

5. Зберігання та архівування даних:

Локальне зберігання: SIEM зберігає дані для подальшого аналізу та аудиту.

Архівування: Можливість зберігати дані для відповідності нормативним вимогам щодо зберігання інформації.

6. Інтеграція з іншими системами безпеки:

Синхронізація з Antivirus та IPS: SIEM може інтегруватися з антивірусами, системами виявлення і запобігання інтрузіям (IPS) та іншими системами безпеки.

Реагування на загрози: Інтеграція дозволяє автоматизовано реагувати на виявлені загрози.

7. Аудит та звітність:

Створення звітів: SIEM надає можливості створення звітів про безпеку та аудит подій для подальшого аналізу та відповідності.

SIEM-системи грають важливу роль у забезпеченні безпеки інформаційних систем, допомагаючи організаціям вчасно виявляти та реагувати на потенційні кіберзагрози та інші безпекові інциденти.

Загальний висновок:

Cisco пропонує комплексний набір рішень для кіберзахисту, який охоплює всі аспекти безпеки мережі, від контролю доступу до ідентифікації, виявлення загроз та захист в хмарі. Їхні технології базуються на передових стандартах та інноваційних підходах, що робить Cisco значущим прототипом для систем кіберзахисту державних установ[36],[42].

3.3. Моделювання прототипу кіберзахисту за допомогою емулятора Cisco Packet Tracer

Cisco Packet Tracer — це потужний симулятор мережі, який дозволяє системним адміністраторам експериментувати взаємодіяти з поведінкою мережі та проводити оцінку можливих сценаріїв. Packet Tracer дозволяє імітувати роботу різних мережевих пристроїв: маршрутизатори, комутатори, бездротові точки доступу, ПК, мережеві принтери, IP-телефони тощо. Використання інтерактивного симулятора дає дуже правдоподібне відчуття роботи з мережею, створюючи мережі на десятки або сотні пристроїв. Ці налаштування, в свою чергу, залежать від характеру пристрою: деякі можна налаштувати за допомогою команд Cisco IOS, графічного веб-інтерфейсу або командного рядка операційної системи або графічні меню.

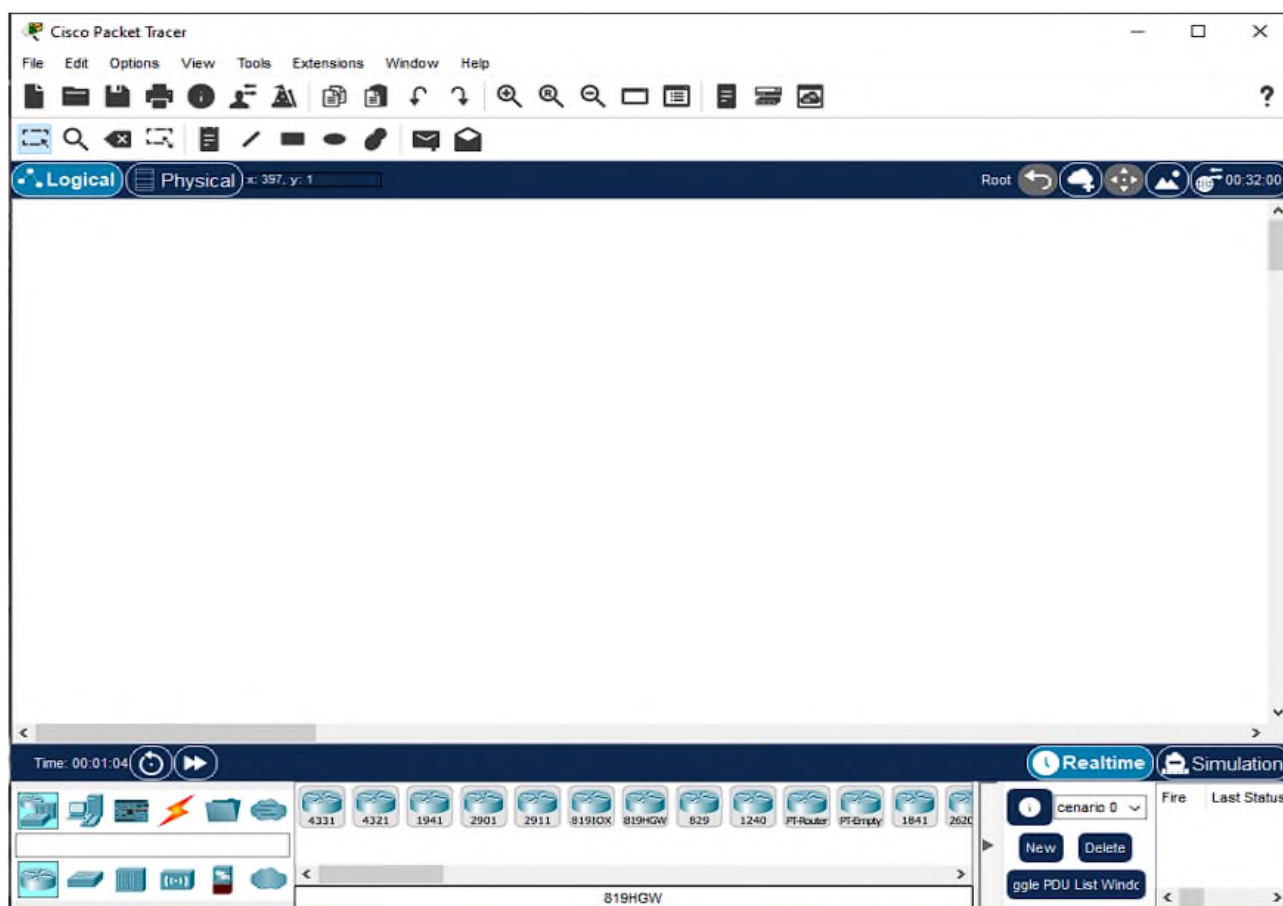


Рис.3.5 – Інтерфейс Cisco Packet tracer.

Cisco Packet Tracer можливо використовувати не тільки як емулятор, а й як мережевий додаток, що моделює віртуальні мережі в реальних мережах, у тому числі в Інтернеті. Користувачі різних комп'ютерів, незалежно від їхнього розташування, можуть працювати, налаштовувати та усувати неполадки в одній топології мережі. Ця функція багатокористувацького режиму Cisco Packet Tracer широко використовується для командної роботи. Крім того, за допомогою Cisco Packet Tracer користувачі можуть отримати навички проектування, моделюючи побудову логічних і фізичних моделей мережі. Схема мережі може бути накладена на креслення реального будинку або навіть міста, а всі його кабелі спроектовані, розташовуючи обладнання в будівлях і приміщеннях, враховуючи такі фізичні обмеження, як довжина і тип кабелів або радіус прокладки, зона покриття бездротової мережі. Симуляція, візуалізація, багатокористувацький дизайн і можливості проектування роблять

Cisco Packet Tracer унікальним інструментом для вивчення мережевих технологій. Вище зазначений загальний інтерфейс Cisco Packet Tracer(рис.3.5)

Створення нової мережі на основі емулятора Packet Tracer

Першим кроком для реалізації автоматичної генерації списків є створення мережі в якій користувачі мають різні посади такі як бухгалтер, адміністратор, айті-спеціаліст, спеціаліст технічної підтримки та інші, кожен з них повинен мати певний рівень доступу, в цьому допоможуть списки контролю доступу. Було виконано конфігурацію наступного сценарію (рис. 3.6). Дана модель складається з 6 мереж: розробка, підтримка, тестування, адміністрування, DNSсервер і серверна частина. Така конфігурація допоможе пояснити взаємозв'язок між різними компонентами системи та налаштувати поведінку мережі, надавши приклади з реального світу.

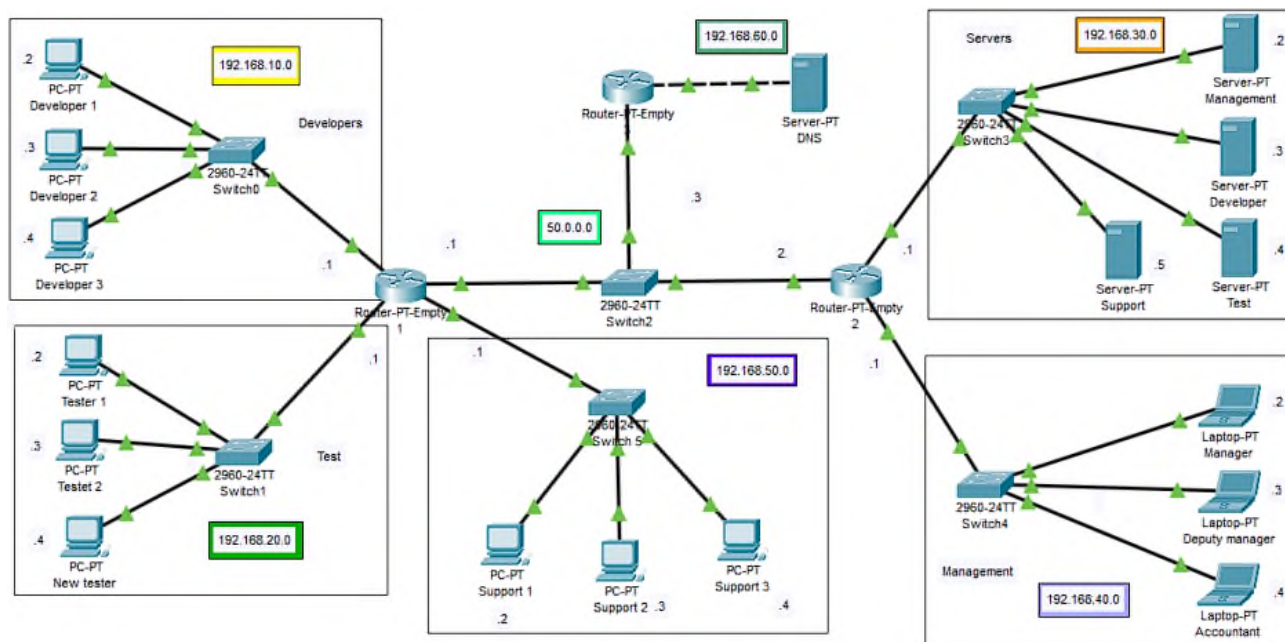


Рис. 3.6 – Змодельована мережа.

Система складається з шести мереж. Відділ розробки, відділ тестування та відділ підтримки використовують по три комп'ютера, а відділ менеджменту

складається з трьох ноутбуків, якими користуються відповідно керівник компанії, системний адміністратор і бухгалтер. . У розділі серверів є 4 сервери, відповідальні за кожен відділ. Доступ до серверів організований за технологією DNS, сервер якого знаходиться в мережі. Кожен користувач і сервер налаштовуються за допомогою IP-адреси. Мережа з'єднана між собою шістьма комутаторами і трьома маршрутизаторами, кожен з яких має статичні маршрути.

Конфігурація ACL в емуляторі Cisco Packet Tracer

Щоб краще бачити які процеси відбуваються в мережі було прийняте рішення налаштувати розширені ACL, змодельювавши те як буде відбуватися автоматична генерація списків контролю доступу. Було вирішено налаштувати найпоширеніші списки розширеного контролю доступу, які можуть стати вирішенням певних задач. Першим з найпоширеніших налаштувань розширених списків доступу є заборона трафіку від одного вузла до іншої мережі. Цей тип блокування часто використовується, коли приймається на роботу новий співробітник і давати доступ до даних компанії ще зарано. На даний момент відділ тестування є новим відділом і має доступ до відділу розробки, це може викликати порушення безпеки, так як кожен новий співробітник може влізти в іншу мережу і нашкодити усій компанії.

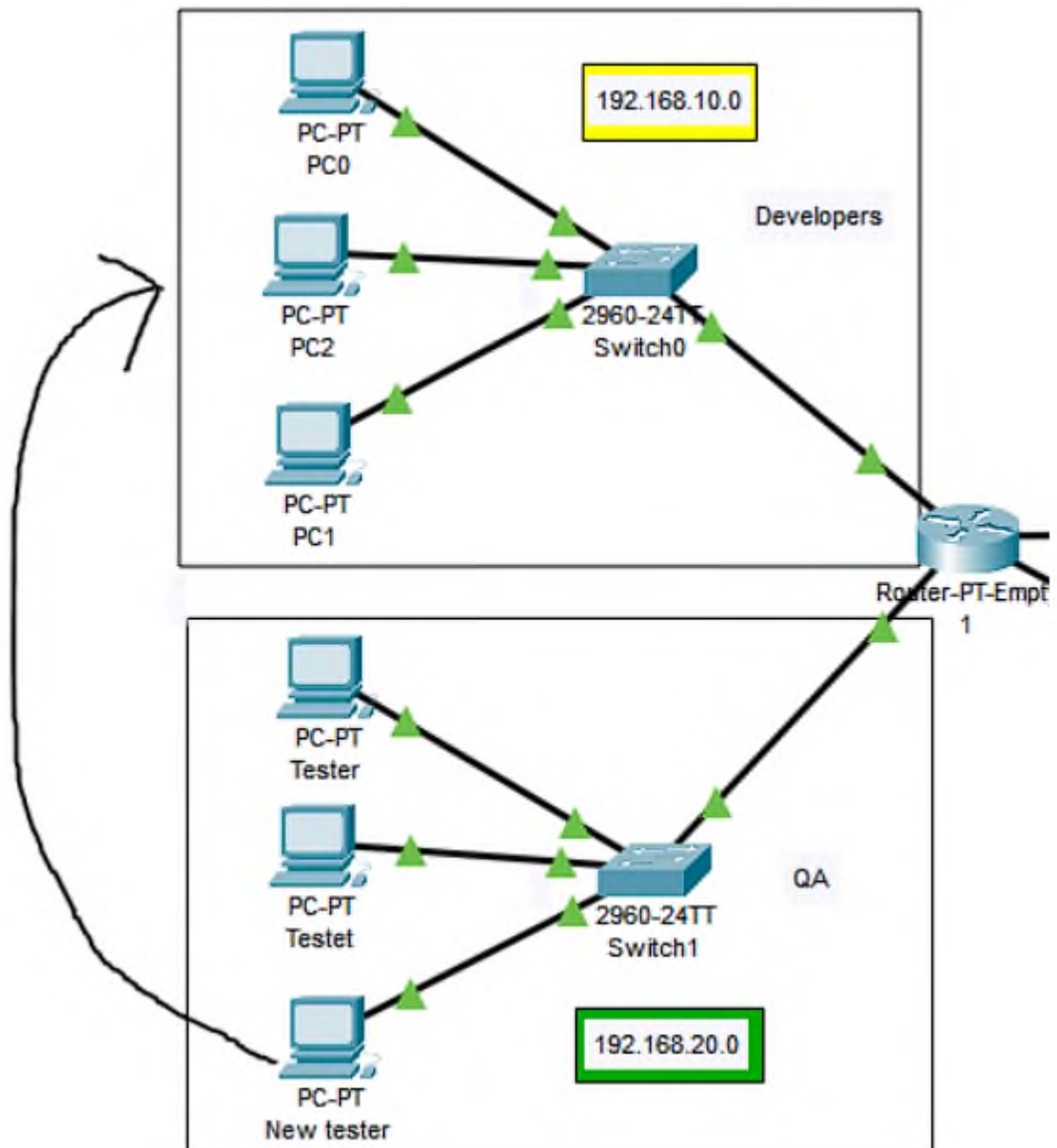


Рис.3.7 – Схема взаємодії між New tester і мережею Developers.

Тому першим чином потрібно обмежити доступ новим співробітникам відділу тестування до відділу розробників. Щоб обмежити доступ потрібно виконати наступний код на маршрутизаторі 1.

```
enable
configure terminal
access-list 134 deny icmp host 192.168.20.4 192.168.10.0 0.0.0.255
int fa1/0
ip access-group 134 in
```

ex

Тепер список контролю доступу під номером 134 забороняє вузлу 192.168.20.4 спрямовувати свій трафік до мережі 192.168.10.0. Щоб продемонструвати це використовуємо команду ping і бачимо, що трафік заблоковано (Рис. 3.8).

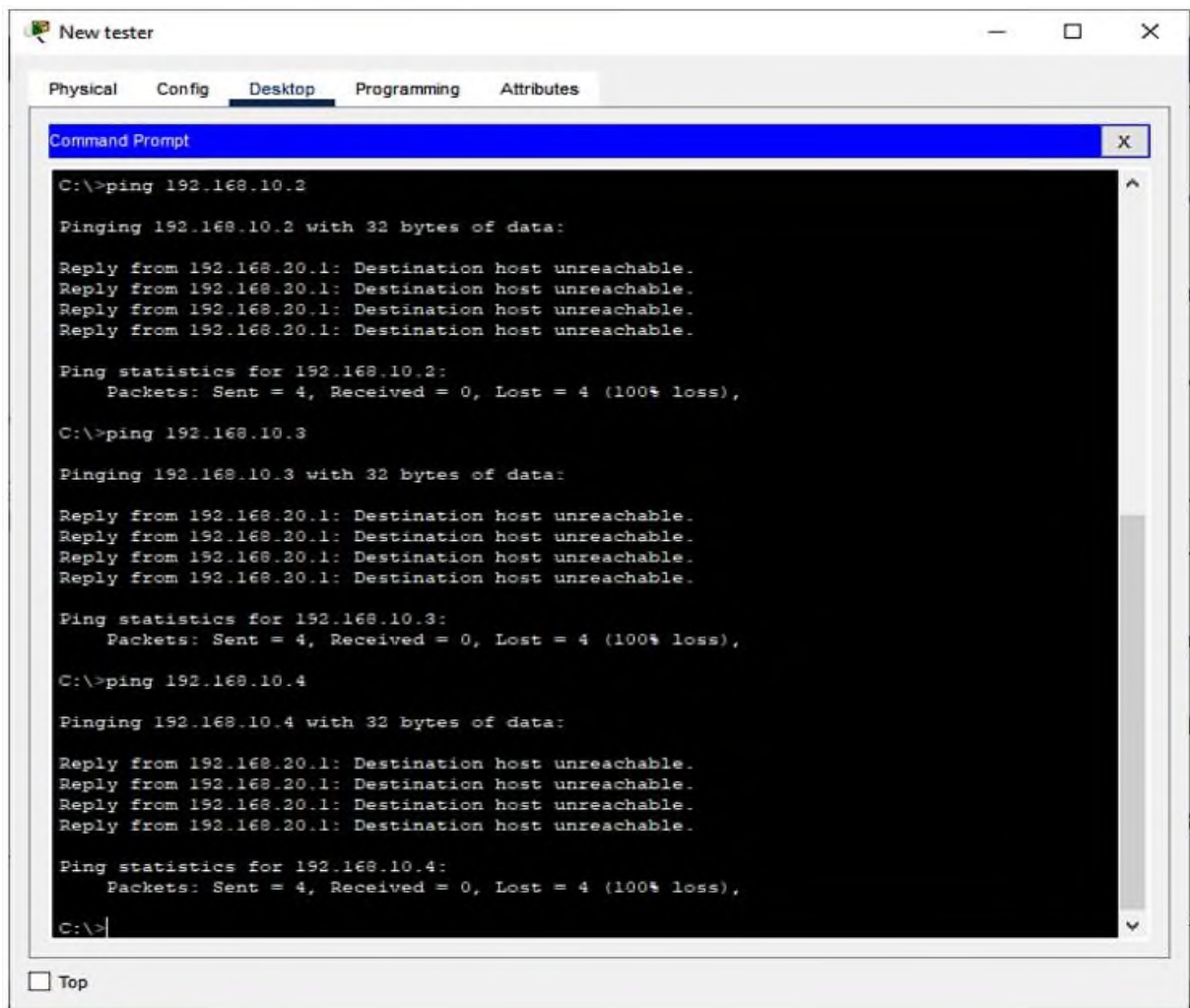


Рис.3.8 – Пінг з вузла New tester у мережі тестувальників та розробників.

Наступним кроком буде обмеження трафіку від мережі до вузла. Мережа тестувальників не повинна мати доступ до серверів розробки, менеджменту та технічної підтримки.

enable

configure terminal

access-list 127 deny icmp 192.168.20.0 0.0.0.255 192.168.30.2

```

access-list 127 deny icmp 192.168.20.0 0.0.0.255 192.168.30.3
access-list 127 deny icmp 192.168.20.0 0.0.0.255 192.168.30.5
int fa2/0
ip access-group 127 in
no sh
ex

```

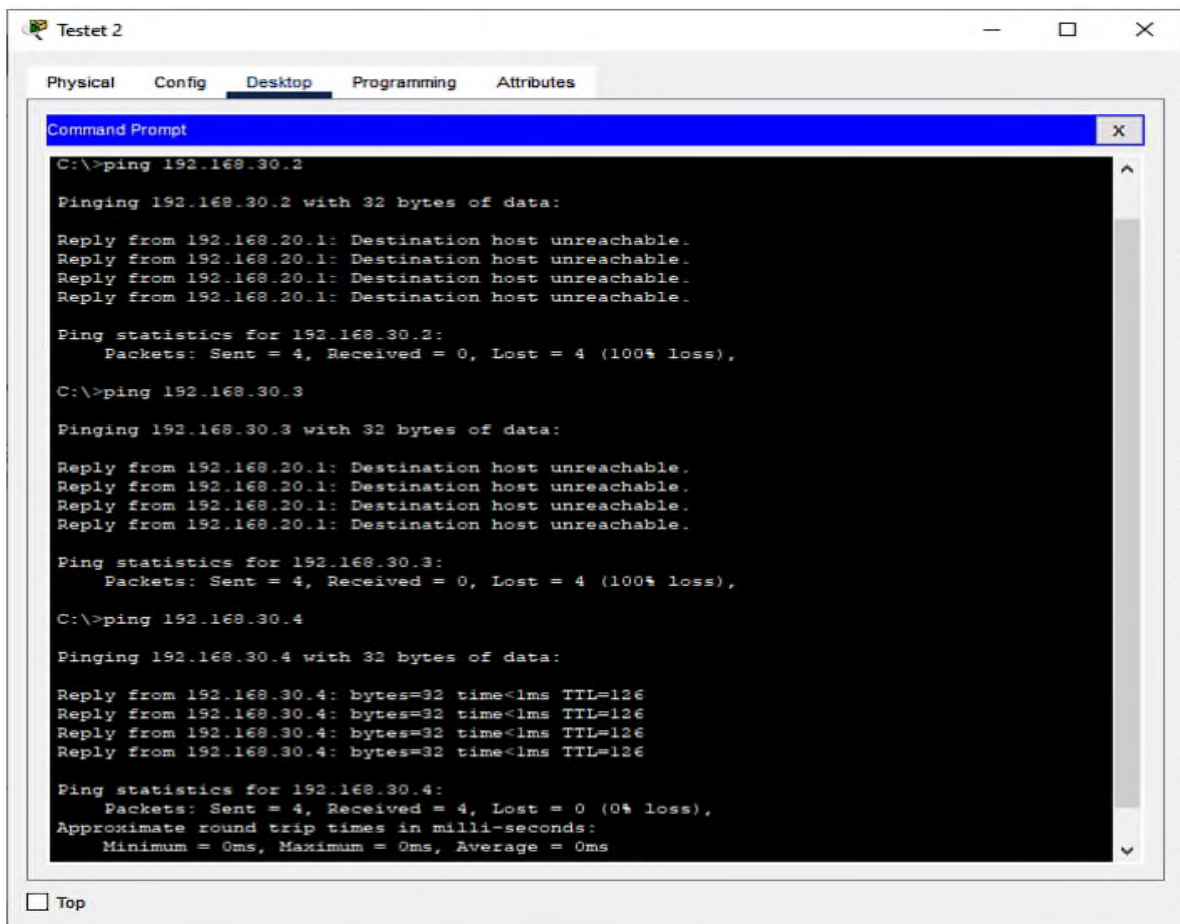


Рис.3.9 – Пінг з вузла New tester у мережу тестувальників і серверів.

Після налаштування списків контролю доступу для серверів потрібно також виконати налаштування між мережевого захисту. Такий тип захисту є представником блокування від мережі до мережі. Так як в будь якій компанії штат працівників постійно змінюється і щоб запобігти порушення безпеки треба обмежити доступ працівникам із відділів тестування і підтримки.

```

enable
configure terminal

```

```

access-list 156 deny icmp 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
int fa2/0
ip access-group 156 in
no sh

```

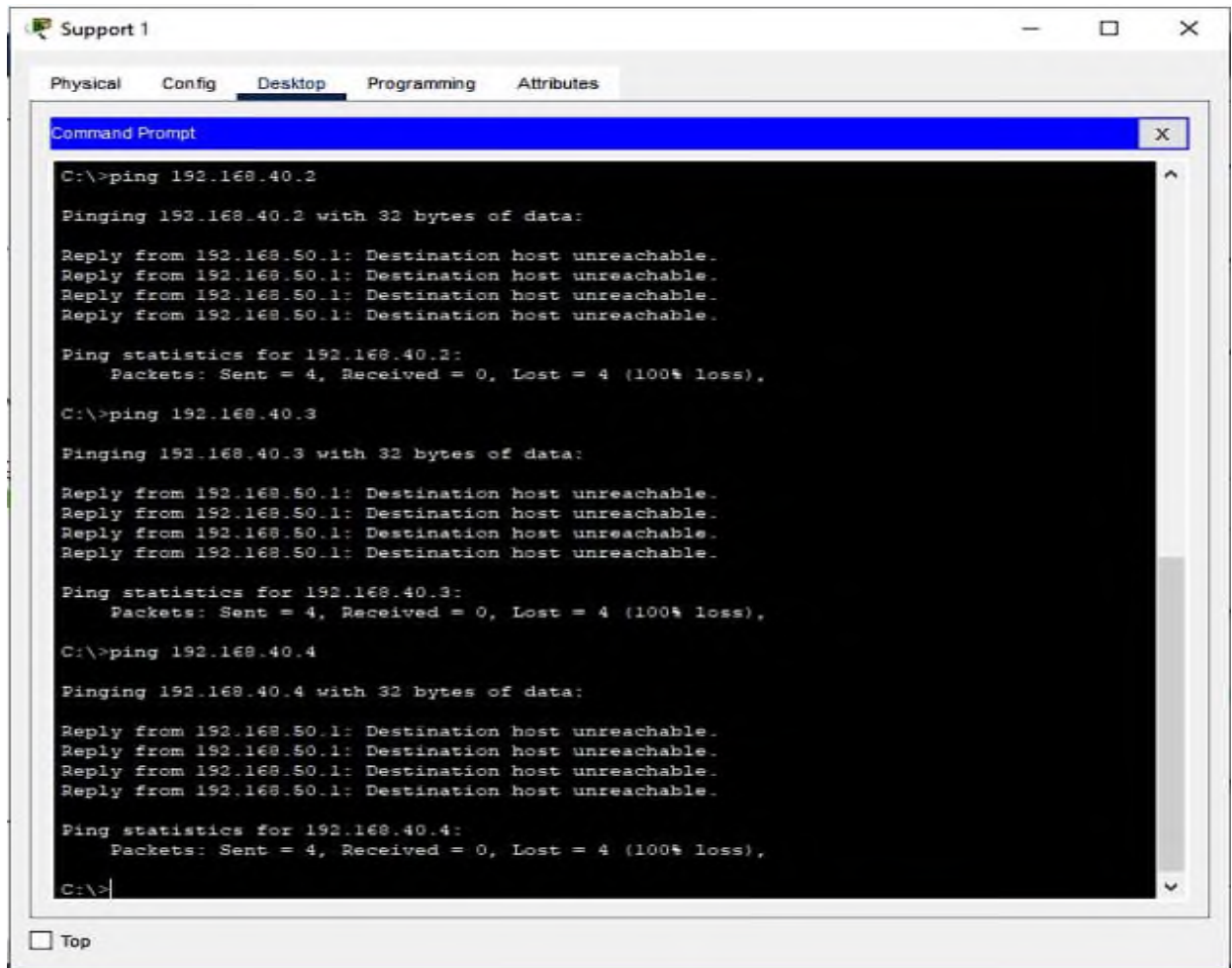


Рис.3.10 – Пінг з мережі Support до мережі менеджменту неможливий.

```

enable
configure terminal
access-list 148 deny icmp 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
int fa3/0
ip access-group 148 in
no sh

```

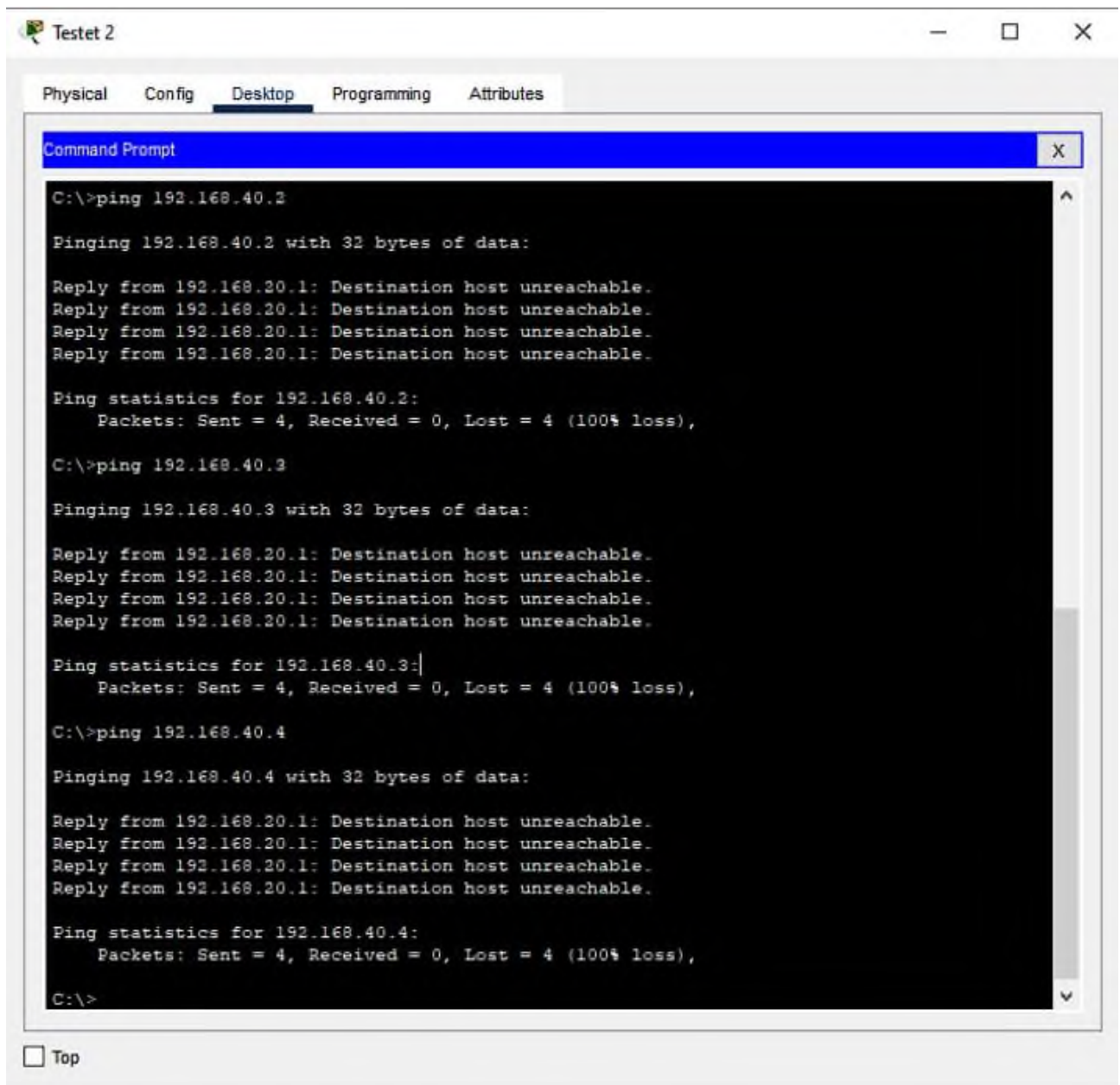


Рис.3.11 – Пінг з мережі Test до мережі менеджменту неможливий.

Щоб захисти сервери від перевантаження, необхідно відключити можливість надсилання запитів ping на них, але потрібно залишити доступ співробітникам. Даний тип захисту допоможе захистити сервери від різних помилок в системі які можуть нашкодити роботі мережі, наприклад, перевантажити сервер великою кількістю запитів. Щоб захистити сервери, потрібно налаштувавши наступний список контролю доступу на маршрутизаторі 2.

```
access-list 193 deny icmp any any echo
int fa1/0
ip access-group 193 out
no sh
ex
```

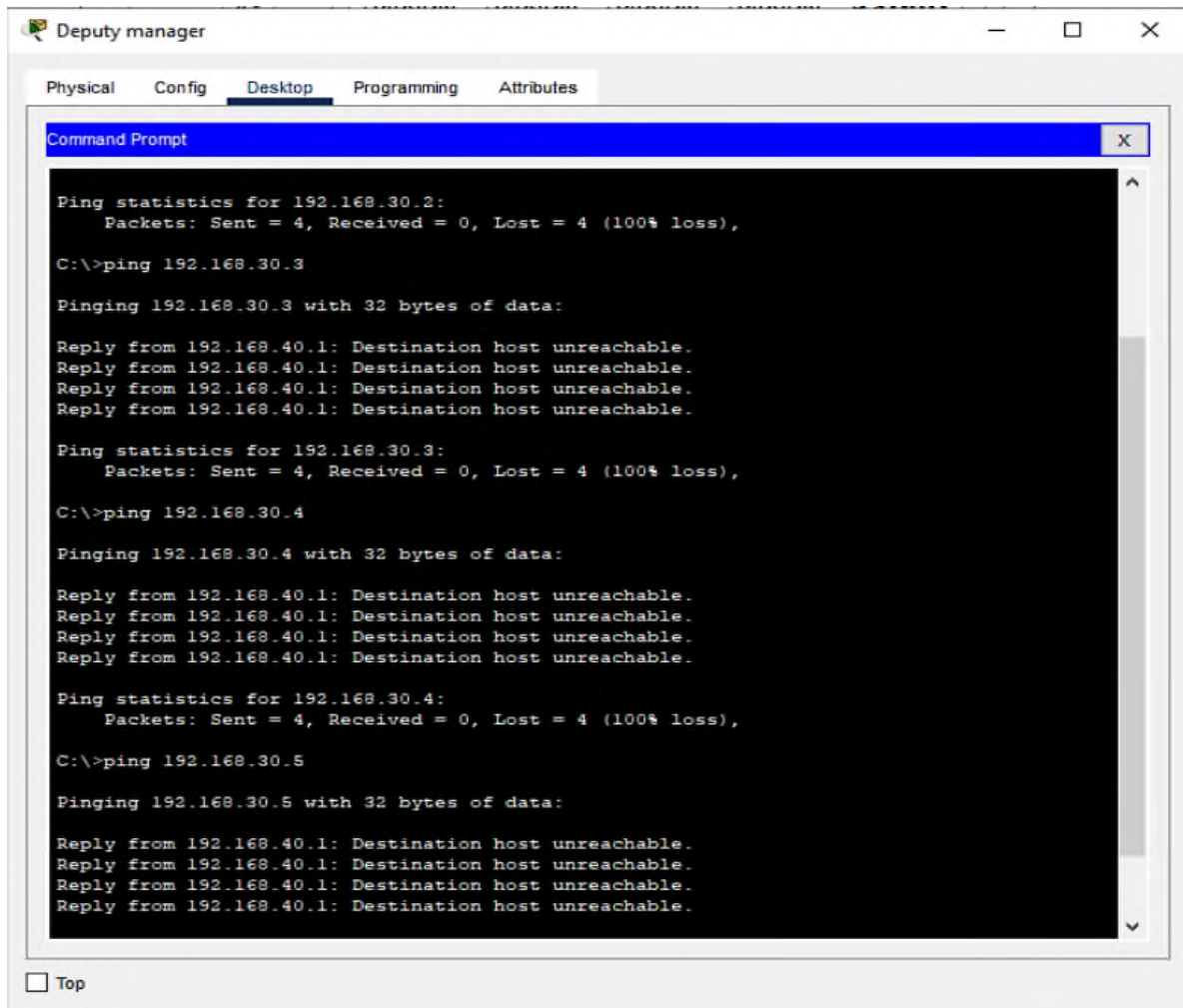


Рис.3.12 – Пінг з вузла Deputy manager до мережі Seprvers.

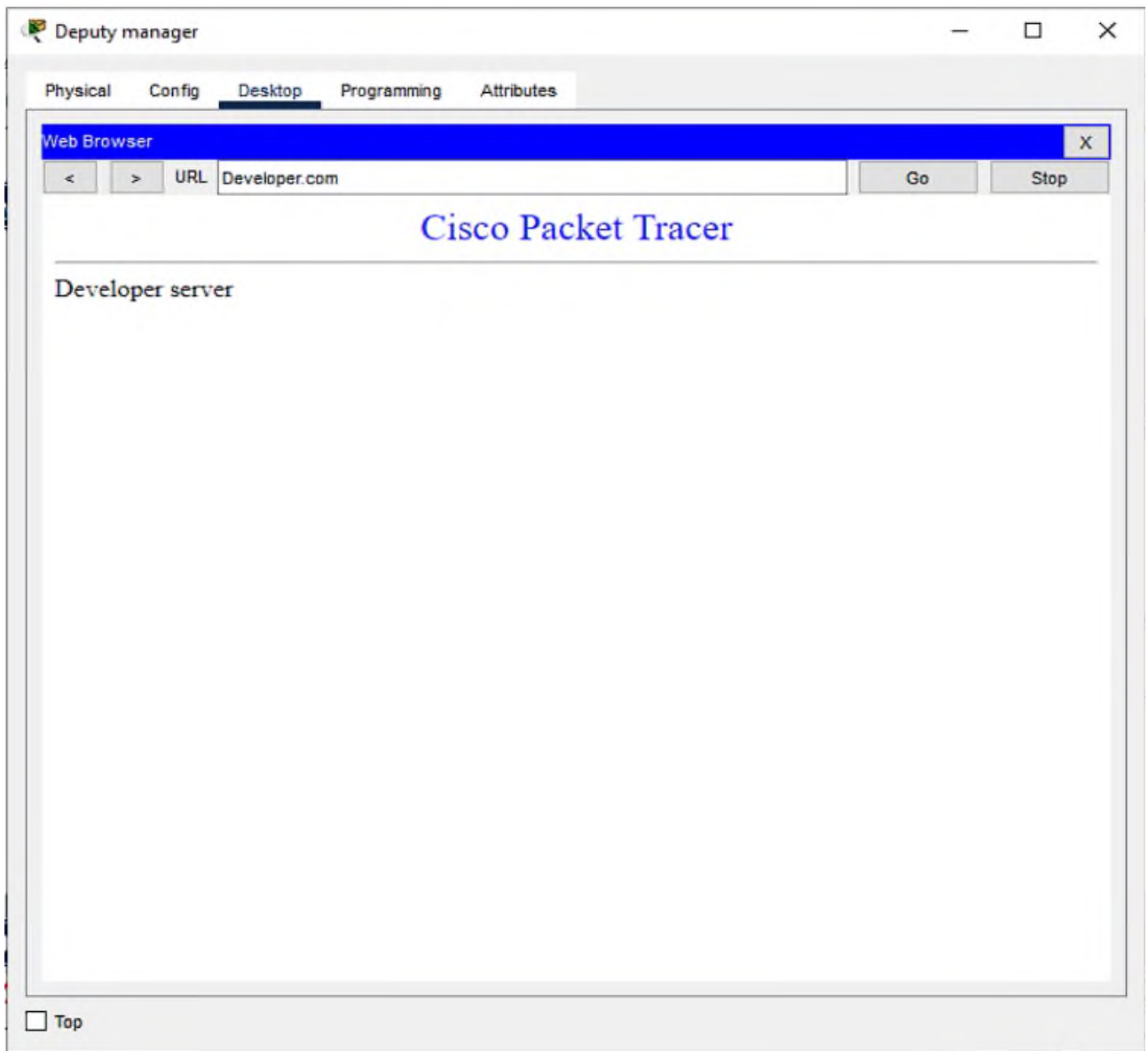


Рис.3.13 – перевірка доступу до сервера Developer з вузла Deputy manager.

Тепер потрібно заборонити трафік від вузла один до вузла два. Такий спосіб захисту потрібен для нових працівників, так як не кваліфікований спеціаліст може дуже нашкодити системі. Тому робітнику New tester буде дозволено мати трафік з робітником Developer 1. Потрібно відредагувати список контролю доступу під номером 134.

```
enable
configure terminal
ip access-list
```

```

ip access-list e 134
(config-ext-nacl)#no 10
(config-ext-nacl)#no 20
access-list 134 deny icmp host 192.168.20.4 192.168.10.3 0.0.0.0
access-list 134 deny icmp host 192.168.20.4 192.168.10.4 0.0.0.0
int fa2/0
ip access-group 134 in
no sh
ex

```

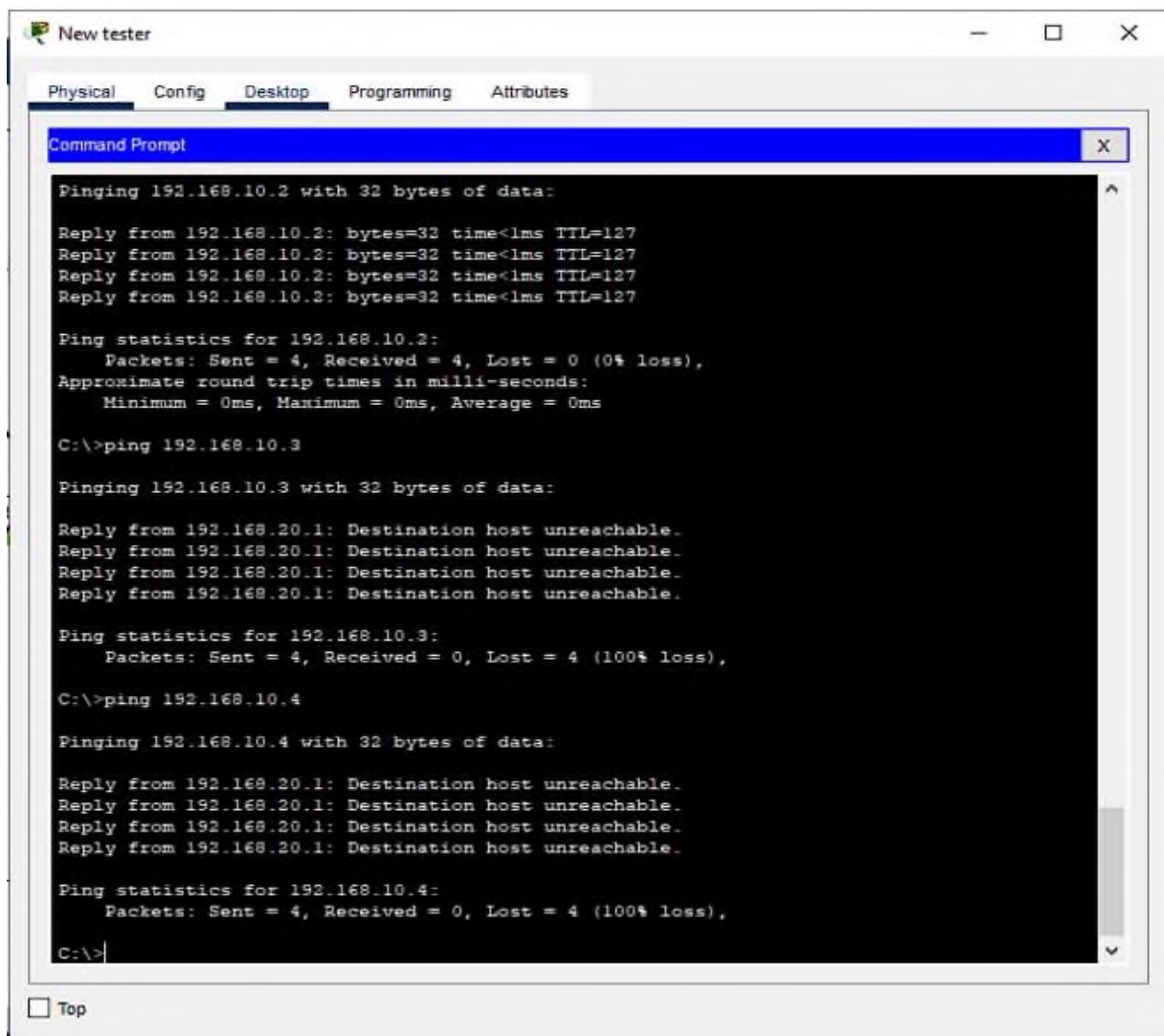


Рис.3.14 – Перевірка доступу вузла New tester до вузлів Developer [40],[41].

3.4. Інтеграція системи кіберзахисту на основі Cisco в державну установу.

Інтеграція системи кіберзахисту, заснованої на рішеннях Cisco, в державну установу є важливим етапом у забезпеченні безпеки інформаційної інфраструктури та виконанні завдань у сфері кібербезпеки. Розглянемо ряд ключових етапів та аспектів цієї інтеграції.

1. Аналіз потреб та загроз:

Оцінка інфраструктури: Проведення аналізу існуючої інфраструктури та ідентифікація вразливостей.

Аналіз загроз: Визначення типів потенційних кіберзагроз, які можуть виникнути для державної установи. Аналіз потреб та загроз на основі Cisco є важливим етапом у визначенні стратегії кіберзахисту та виборі оптимальних рішень для забезпечення безпеки інформаційних систем. Аналіз потреб та загроз на основі Cisco дозволяє детально визначити специфічні вимоги та шляхи для покращення кіберзахисту в державній установі. Цей процес є ключовим етапом для вибору оптимальних рішень та планування стратегії безпеки.

2. Вибір та Розгортання Рішень Cisco:

Вибір відповідних продуктів: Враховуючи потреби та особливості державної установи, вибір рішень Cisco, таких як брандмауери, системи виявлення і запобігання інтрузіям, SIEM-системи тощо.

Розгортання: Планування та розгортання вибраних рішень відповідно до потреб та архітектури мережі державної установи.

1. Інтеграція з існуючими системами:

Спільна робота з іншими засобами безпеки: Забезпечення взаємодії систем Cisco з іншими системами безпеки, які вже використовуються в установі.

Локальна інтеграція: Підтримка локальної інтеграції з іншими важливими системами та джерелами даних.

2. Налаштування та достосування:

Налаштування правил та політик: Встановлення правил та політик безпеки відповідно до вимог та стандартів безпеки.

Достосування до потреб: Забезпечення того, що рішення Cisco адаптовані до конкретних потреб та вимог державної установи.

3. Навчання та сертифікація:

Навчання персоналу: Забезпечення проходження персоналом державної установи необхідних курсів та сертифікацій від Cisco для ефективного використання систем безпеки.

Підтримка та обслуговування: Навчання та створення здатностей для внутрішньої підтримки та обслуговування систем Cisco.

4. Моніторинг та аналіз:

Централізований моніторинг: Створення централізованої точки моніторингу для подій та інцидентів за допомогою SIEM-системи Cisco.

Аналіз журналів: Використання засобів аналізу журналів для виявлення аномалій та виняткових ситуацій.

5. Реагування та підтримка інцидентів:

Створення процедур реагування: Розробка та впровадження процедур реагування на інциденти для швидкого та ефективного відгуку на кіберзагрози.

Підтримка інцидентів: Створення команди та механізмів підтримки для вирішення інцидентів у випадку кібератак чи інших подій безпеки.

Інтеграція системи кіберзахисту Cisco в державну установу є стратегічно важливим кроком для забезпечення високого рівня безпеки інформаційної інфраструктури та надійного захисту від сучасних кіберзагроз. Цей процес вимагає уважного аналізу, планування та співпраці між різними відділами та фахівцями з безпеки[43].

3.5. Моніторинг та підтримка системи кіберзахисту

Сучасний кіберпростір вимагає надійного та ефективного захисту інформаційних систем від різноманітних кіберзагроз. У цьому контексті,

моніторинг та підтримка системи кіберзахисту відіграють важливу роль у забезпеченні безпеки та стійкості інформаційних технологій. Особливе значення в цьому контексті має використання продуктів та рішень від Cisco, які є лідерами у сфері кібербезпеки. Моніторинг та підтримка системи кіберзахисту на основі Cisco є критичними елементами для забезпечення ефективності та надійності захисту інформаційної інфраструктури. Детально розглянемо ці процеси:

Системи моніторингу подій (SIEM): Використання SIEM, таких як Cisco Stealthwatch, для централізованого збору, аналізу та відстеження подій в інформаційній системі. Це дозволяє швидко виявляти аномалії та потенційні загрози. Моніторинг та підтримка системи кіберзахисту Cisco є динамічним та постійно розвиваючимся процесом, який вимагає від організації не лише реакції на існуючі загрози, але і передбачення майбутніх та адаптації до них. Моніторинг та підтримка системи кіберзахисту на основі Cisco є важливим елементом стратегії кібербезпеки, який дозволяє не лише виявляти потенційні загрози, але й ефективно реагувати на них. Використання продуктів Cisco в цьому контексті є кроком у напрямку створення надійного та стійкого захисту інформаційних ресурсів.

ВИСНОВКИ

В результаті проведеного дослідження було розглянуто та проаналізовано теоретичні аспекти системи кіберзахисту комп'ютерної мережі державної установи на основі активного устаткування Cisco та програмного забезпечення Cisco Packet Tracer.

Автором було розроблено прототип у середовищі комп'ютерної мережі державної установи із використанням устаткування Cisco Packet Tracer.

Практична значимість прототипу полягає у можливості використання його для розгортання реальної захищеної мережі на устаткуванні Cisco. Це відкриває широкі перспективи для вдосконалення інфраструктури компаній та організацій, забезпечуючи надійний захист від кіберзагроз та забезпечуючи безперебійне функціонування мережевих систем. Реалізація цього прототипу дозволить ефективно впроваджувати передові технології безпеки, підвищуючи стійкість мережі до атак і забезпечуючи конфіденційність, цілісність та доступність даних.

Компанії, які сьогодні хочуть захиститися в кіберпросторі, борються з нестачею кваліфікованих робітників. Не вистачає людей з належним рівнем знань, щоб забезпечити високий рівень здатності виявлення загроз.

Якщо ці компанії хочуть підвищити безпеку всієї інформаційної системи їм потрібно знайти «найслабшу ланку» .

Організаціям необхідно підтримувати і постійного поліпшувати потенціал корпоративної безпеки шляхом оцінки та підвищення потенціалу безпеки своїх співробітників. Низький рейтинг здібностей до будь-яких знань або навичок потенційно порушує безпеку підприємства. Таким чином, можливості безпеки персоналу повинні бути пріоритетом для організації, оскільки, коли можливості технічної безпеки неефективні, виходять з ладу або недоступні, можливості персоналу можуть забезпечити останню лінію захисту.

Рекомендації щодо подальшого розвитку та впровадження системи кіберзахисту в державній установі можуть включати різні аспекти, оскільки кібербезпека вимагає комплексного підходу. Забезпечити ефективну взаємодію

та обмін інформацією з іншими державними установами, локальними та міжнародними організаціями, а також приватним сектором для виявлення та вирішення загроз. Ці рекомендації можна адаптувати відповідно до конкретних потреб та умов державної установи. Важливо враховувати постійну зміну кіберзагроз та адаптувати заходи безпеки для ефективного захисту інформації та інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Проектування інформаційних систем: навчальний посібник / В. С. Авраменко, А. С. Авраменко. Черкаси: Черкаський національний університет ім. Б.Хмельницького, 2017. 434 с.
2. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 251 -253 с.
3. Безпека соціально-економічних процесів в кіберпросторі : матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). – Київ : Київ. нац. торг.-екон. ун-т, 2019. – 244 с.
4. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа інформаційна та кібербезпека: соціотехнічний аспект. Підручник за загальною редакцією доктора технічних наук. 37 с.
5. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко, Л. В. Бурячок, П. М. Складанний, Н. В. Лукова-Чуйко. – Київ: ДУТ – КНУ, 2016. – 178 с.
6. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
7. Бурячок В. Л. Модель формування дерева атак для одержання інформації в інформаційно-телекомунікаційних системах і мережах при вилученому доступі / В. Л. Бурячок // Науковий журнал «Інформатика та математичні методи в моделюванні»
8. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.

9. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. CS&CS, 2019. Issue 1(13). С.17-29
10. Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 01–02 грудня 2022 р. – Житомир: Житомирська політехніка, 2022. – 409 с.
11. М. В. Грайворонський, О. М. Новіков. “Безпека інформаційнокомунікаційних систем”. Київ: Видавнича група BVH, 2009, 608 с.
12. Грищук Р.В., Даник Ю. Г. Синергія інформаційних та кібернетичних дій // Труди університету. К.: НУОУ. 2014. № 6 (127). С. 132–143.
13. Гулак Г. М. Основи криптографічного захисту інформації: підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук. – Вінниця: ВНТУ, 2011. – 199 с.
14. Даник Ю.Г., Корнейко О.В. Основи методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони України // Information Technology and Security. 2018. Том 6. № 2(11). С. 105-123
15. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. – 320 с.
16. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
17. Закон України «Про захист персональних даних». URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 20.01.2024)
18. Закон України «Про інформацію». URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення 20.01.2024)
19. Закон України «Про основні засади забезпечення кібербезпеки України». URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

20. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: ХНЕУ, 2008. – 196 с.
22. Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. – Одеса : ОДУВС, 2018. – 156 с.
23. Комп'ютерна інженерія і кібербезпека : досягнення та інновації : матеріали II Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених, м. Кропивницький, 25–27 листоп. 2020 р. / М–во освіти і науки України, Держ. наук. установа “Інститут модернізації змісту освіти”, Центральноукр. нац. техн. ун–т ; [відп. за вип. О. П. Доренський]. — Кропивницький: ЦНТУ, 2020. — 147 с.
24. Ковів І.Б. Основи побудови комплексної системи захисту інформації для інформаційно-телекомунікаційної системи. Навчальний посібник. Київ: Вид-во ІСЗЗІ НТУУ “КПІ імені Ігоря Сікорського”, 2016. 88с.
25. Кузьменко Б. В. Захист інформації / Б. В. Кузьменко, О. А. Чайковська. — Київ: Видавничий відділ КНУКіМ, 2009. – 69 с.
26. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. — К.: Видавничий дім «Кондор», 2019. — 272 с.
27. Мельник С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Ленков // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. – Київ. ВІКНУ, 2011. – Вип. 30. – с. 159-165.
28. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Харків: ХНЕУ, 2013. – 476 с.
29. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

30. Організація комп'ютерних мереж: підручник: для студ. спеціальності 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.
31. Табунщик Г.В. Інженерія якості програмного забезпечення: навчальний посібник / Г. В. Табунщик, Р. К. Кудерметов, Т. І. Каплієнко. 2-ге видання. Запоріжжя: Дике Поле, 2016. 176 с.
32. Тихомиров О. О. Класифікації забезпечення кібербезпеки // Вісник Запорізького національного університету : зб. наук. праць. Юридичні науки. Запоріж
33. Харченко Л.С. Кібербезпека України : Глосарій / Л. С. Харченко, В. А. Ліпкан, О. В. Логінов; за заг. ред. Р. А. Калюжного. — К. : Текст, 2004. — 136 с.].
34. Цимбалюк В.С. Сутність кібербезпеки в умовах входження України до глобальної кіберцивілізації / В. Цимбалюк // Науковий вісник академії ДПС України. — 2007. — № 4. — С. 174–178.
35. Яковів І.Б. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. Збірник наукових праць “Інформаційні технології і безпека”. Том 5, № 2. К.: ІССЗІ, 2017. Одеського національного політехнічного університету. – № 2, 2013, с. 123 – 131
36. Офіційне видання Cisco CCNA ICND2 200-101 Маршрутизація та комутація 2015
37. Повний довідник по Cisco.: пер. с англ. М. : Вільямс. 2004. - 1078 с.
38. Penetration Testing / K. Cardwell – Birmingham: Packt Publishing Ltd, 2014. – 412
40. Cisco Packet Tracer: чого нам варте налаштувати мережу? URL: https://www.cisco.com/c/dam/global/ru_ua/assets/pdf/cisco_packet_tracer.pdf (дата звернення 20.01.2024)

41. Cisco. URL: <https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20190513-secureboot.html> (дата звернення 20.01.2024)
42. Cisco – мережеві коммутатори Cisco [Електронний ресурс] - URL: [www.cisco.com c/ru ru/products/switches/ index.html](http://www.cisco.com/c/ru/ru/products/switches/index.html)
43. GNS3 vs Packet Tracer – Know difference between GNS3 & Packet Tracer - URL: <https://ipwithease.com/gns3-vs-packet-tracer/> (дата звернення 20.01.2024)