МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЦЕНТР ЗАОЧНОЇ, ДИСТАНЦІЙНОЇ ТА ВЕЧІРНЬОЇ ФОРМ НАВЧАННЯ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Модель кіберзахисту розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства»

Завідувач
випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Кальченко В.В.**

Студента групи ІНз – 61С **Ситнік М.О.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Центр заочної, дистанційної і вечірньої форм навчання

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____" _____2020 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи ІНз-61с спеціальності "Інформатика" заочної форми навчання Ситнік Максима Олександровича.

Тема: "**Модель кіберзахисту розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства**"

Затверджена наказом по СумДУ

№_____ від _____2020 р.

Зміст пояснювальної записки: 1) аналіз предметної області; 2) постановка задачі; 3) аналіз захищеності діючої розподіленої інформаційно-телекомунікаційної системи об'єкта дослідження; 5) розробка моделі кіберзахисту розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства.

Дата видачі завдання "_____"_____2020 р.

Керівник випускної роботи _____ Кальченко В.В.

Завдання прийняв до виконання _____ Ситнік М.О.

РЕФЕРАТ

Записка: 43 стор., 15 рис., 2 табл., 28 джерел.

Мета роботи — розробка моделі кіберзахисту розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства.

Об'єкт дослідження — інформаційно-телекомунікаційна система торгівельного підприємства на прикладі ТОВ «Весела торбинка».

Предмет дослідження — сукупність засобів програмно-технічного характеру, які можуть бути спрямовані на забезпечення кібербезпеки інформаційно-телекомунікаційної системи об'єкта дослідження.

Методи дослідження — методи теоретичного узагальнення – при описі предметної області дослідження; аналізу та синтезу – при дослідженні захищеності діючої розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства; формалізації – при створенні проектів розподіленої комп'ютерної мережі в симуляторі Cisco Packet Tracer; системного аналізу та експерименту – при розробці моделі кіберзахисту розподіленої інформаційно-телекомунікаційної системи та налаштуванні пристроїв забезпечення безпеки.

Результати — розроблено модель кіберзахисту розподіленої інформаційно-телекомунікаційної системи ТОВ «Весела торбинка». При проектуванні мережі було запропоновано використовувати багатофункціональний пристрій забезпечення безпеки Cisco ASA 5506-X для головного офісу підприємства. Розроблено модель мережі за допомогою програмного забезпечення Cisco Packet Tracer та здійснено налаштування міжмережевого екрану Cisco ASA 5506-X та маршрутизаторів для забезпечення захисту мережі.

РОЗПОДІЛЕНА СИСТЕМА, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, МАРШРУТИЗАТОР, МІЖМЕРЕЖЕВИЙ ЕКРАН, КІБЕРЗАХИСТ, CISCO PACKET TRACER, CISCO ASA, ТОРГІВЕЛЬНЕ ПІДПРИЄМСТВО.

ЗМІСТ

ВСТУП

Проблема забезпечення кіберзахисту виникла у зв’язку з поширенням комп’ютерних технологій та бурхливим розвитком Інтернет. Зростаючі об’єми інформації формують інформаційне середовище, яка вимагає більш жорстких вимог до методів і засобів обробки і передачі даних.

Використання засобів обчислювальної техніки в системах управління бізнес структурами вимагає наявності якісних і потужних систем обробки, зберігання і передачі даних. Виконання цих вимог призвело до створення єдиної електронної інфраструктури, яка дозволяє кінцевим користувачам з робочих місць підключися до різних видів баз даних та знань, а також, незалежно від географічного положення, передавати та отримувати необхідну інформацію. Створення таких систем призвело до ряду проблем, однією з яких є безпека обробки і передачі конфіденційної інформації.

Сьогодні питання кіберзахисту є актуальним не лише для спеціалістів з кібербезпеки. Прецеденти в області кібербезпеки можуть впливати на всіх користувачів інформаційних технологій. Достатньо згадати такі вірусні атаки як WannaCry та Petya.A чи кібератаки, які спрямовуються на певні об’єкти інфраструктури, наприклад, BlackEnergy [1, 2].

Сучасні потреби інформатизації суспільства вимагають від інформаційно-телекомунікаційних систем бізнес структур високої стійкості до зовнішніх і внутрішніх загроз, доступності, цілісності та конфіденційності інформації (яка зберігається, обробляється, передається каналами зв’язку) [3]. У світі бізнесу і торгівлі комп’ютерна мережа – це не лише сукупність з’єднаних між собою пристроїв. Так для торгівельного підприємства інформаційно-телекомунікаційна система – це виробничий ресурс, використання якого забезпечує збір, аналіз та розповсюдження інформації, яка є основним інструментом їхнього бізнесу і джерелом доходів. З огляду на це, метою дипломної роботи є розробка моделі

кіберзахисту розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства.

Об’єкт дослідження – інформаційно-телекомунікаційна система торгівельного підприємства на прикладі ТОВ «Весела торбинка».

Предмет дослідження – сукупність засобів програмно-технічного характеру, які можуть бути спрямовані на забезпечення кібербезпеки інформаційно-телекомунікаційної системи об’єкта дослідження.

Поставлена мета обумовила необхідність вирішення наступних завдань:

– розглянути поняття розподіленої інформаційно-телекомунікаційної системи та її захищеності;

– систематизувати основні причини виникнення проблем захисту інформаційно-телекомунікаційних систем;

– розглянути основні типи загроз розподілених інформаційно-телекомунікаційних систем;

– проаналізувати захищеність розподіленої інформаційно-телекомунікаційної системи об’єкта дослідження;

– розробити проект розподіленої інформаційно-телекомунікаційної системи об’єкта дослідження з урахуванням вимоги кіберзахисту;

– здійснити основні налаштування пристроїв забезпечення безпеки в запропонованій моделі кіберзахисту інформаційно-телекомунікаційної системи.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Поняття розподіленої інформаційно-телекомунікаційної системи та її захищеності

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [4].

При цьому під інформаційною системою розуміється організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [4]. А під телекомунікаційною системою — сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [4].

Також під інформаційно-телекомунікаційною системою розуміють сукупність каналів, об’єктів і засобів зв’язку, а також інформаційні ресурси у вигляді інформації і апаратно-програмних засобів, призначених для прийому, передачі, накопичення, обробки і зберігання даних.

Розподілена інформаційно-телекомунікаційна система – це набір незалежних комп’ютерів, які користувач сприймає як єдину об’єднану систему. Всі робочі станції автономні, а в якості програмного забезпечення користувачами використовується єдина система [5].

Наявність у торгівельного підприємства телекомунікаційної системи, її подальша модернізація та розвиток створюють нові можливості інтеграційного характеру:

– єдину інформаційно-мережеву взаємодію всіх учасників торгівельного процесу;

– використання загальносистемних сервісів, до яких відносяться мережевий друк, використання спеціальних додатків для колективної роботи фахівців торгівельного підприємства;

– рішення задач торгівлі за рахунок спеціалізованих прикладних програмних продуктів;

– можливість створення дієвих механізмів інформаційної безпеки в процесі комунікації фахівців підприємства.

Якщо порівнювати розподілені інформаційно-телекомунікаційні системи з корпоративними мережами з доступом до Інтернет, то до перших вищі вимоги з точки зору кібербезпеки. Для корпоративних мереж стандартні засоби безпеки зазвичай добре показують себе при вирішенні питання захисту внутрішньої мережі від зловмисників.

Зазвичай в розподілених інформаційних системах використовуються відкриті канали передачі даних, тому для них типовими і найпоширенішими є віддалені атаки. При цьому зловмисник має змогу здійснювати не лише пасивний збір інформації, яка циркулює в системі, але й змінювати, підміняти чи якимось іншим чином впливати на неї [3].

Захищеність інформаційно-телекомунікаційних систем як правило розуміють як [6, 7]:

– набір технологічних прийомів та засобів, які використовуються для забезпечення захисту компонентів інформаційної системи;

– зведення до мінімуму ризику для складових інформаційно-телекомунікаційної системи;

– сукупність логічних і фізичних заходів, які направлені на захист від загроз інформації та складових інформаційно-телекомунікаційної системи.

Вимоги до кібербезпеки розподілених інформаційних систем необхідно формально визначати. Дотримання вимог гарантує, що у разі появи загроз різної природи, які були передбачені в вимогах до кібербезпеки, система збереже свою функціональність в повному обсязі. Якщо технічні умови функціонування системи були правильно визначені, то безпека системи має бути оцінена та забезпечена під

час проектування шляхом детальної розробки архітектури системи, використанні спеціальних засобів та не може порушуватися у разі появи передбачених обставин.

Практичне виконання механізмів забезпечення захищеності розподіленої інформаційно-телекомунікаційної системи є залежним від множини факторів: розміру бізнесу, напрямку діяльності компанії, типу інформаційної системи, міри її складності та розподіленості, топологічної схеми мереж, програмного забезпечення, що використовується і т. д [8].

Управління інформаційною безпекою та визначення засобів захисту інформаційно-телекомунікаційної системи є нелегким динамічним процесом. З огляду на те, що розподілена інформаційно-телекомунікаційна система – це складна система з багаторівневою архітектурою, то при прийнятті рішення про методи та засоби забезпечення її захисту необхідно ділити її та складові частини. Правила, процеси і процедури, які використовуються для ефективного управління мають бути формалізовані для кожного сегмента цієї системи. Це дає змогу прийняти оптимальне рішення щодо найбільш прийнятного компонента захисту певної складової частини системи [9].

1.2. Основні причини виникнення проблем захисту

Згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» захист інформації — діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [4].

Доступ до внутрішньої мережі, віддалений доступ і доступ в Інтернет сьогодні використовуються достатньо широко, що породжує певний ризик і ставить цілий ряд питань безпеки. Мережа і апаратні засоби, що використовуються для доступу в мережу, можуть містити дефекти захисту, можуть бути неправильно встановлені чи налаштовані, а також можуть неправильно використовуватись [10].

Проведений аналіз літературних джерел дозволяє систематизувати основні причини виникнення загроз захисту мережі. До основних з них відносять:

– технологічні недоліки – кожна мережа і кожна комп’ютерна технологія мають свої проблеми захисту (недоліки, притаманні TCP/IP, операційним системам і мережевому обладнанню) [10];

– недоліки конфігурування – навіть сама надійна технологія захисту може бути неправильно реалізована чи використана, в результаті чого може виявитися проблема захисту (недостатній захист, який забезпечується налаштуванням за замовчуванням, неправильна конфігурація мережевого обладнання, незахищені облікові записи користувачів, облікові записи користувачів з простими паролями, неправильне налаштування служб Інтернет) [10];

– недоліки політики захисту мережі – неправильно реалізована політика захисту може зробити вразливою навіть найкращу технологію мережевого захисту (відсутність документованої політики захисту, внутрішні протиріччя політик, відсутність логічного контролю доступу до мережевого обладнання, невідповідність програмного забезпечення і апаратних засобів прийнятої політики, необізнаність про можливі атаки) [10];

– нестабільна робота обладнання – будь-які збої в роботі кабельної системи, серверів, персональних комп’ютерів, а також перебої в електроживленні негативно впливають на рівень захищеності системи від загроз) [11, 12];

– дефекти програмного забезпечення – при наявності вразливостей програмного забезпечення, а також при несвоєчасному встановлені оновлень безпеки інформація в системі може бути втрачена чи пошкоджена через помилки програмного забезпечення чи зараження вірусами [11, 12];

– несанкціоновані дії сторонніх осіб – порушення конфіденційності інформації шляхом її викрадення, підміни, пошкодження чи знищення, порушення роботи інформаційної системи чи вивід з ладу обладнання [11, 12];

– помилки користувачів – випадкові її, які можуть призвести до знищення чи зміни даних, порушення роботи системи внаслідок некоректного використання програмного та апаратного забезпечення [11, 12];

– навмисні дії користувачів – поєднує в собі все, що описано в попередніх двох пунктах, та включає поширення конфіденційної інформації [12].

Якщо при втручанні в роботу системи втрати чи викрадення інформації не відбулося, то це також класифікується як порушення безпеки інформаційної системи [12].

Кіберзахист має бути головним елементом організації мережі. Правильне рішення проблем захисту дозволить:

– мінімізувати витрати впровадження і експлуатації засобів мережевого захисту;

– відкрити можливість використання нових мережевих додатків і послуг;

– зробити Інтернет недорогим і безпечним засобом глобальних комунікацій [10].

У положеннях чинного законодавства, а саме в Законі України «Про основні засади забезпечення кібербезпеки України» визначається, що кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [14].

1.3. Основні типи загроз розподілених інформаційно-телекомунікаційних систем

Розподілена інформаційно-телекомунікаційна система є принадливою для багатьох загроз як ненавмисних, так і зловмисних дій, і в певних випадках ці загрози можуть бути реалізованими успішно. Це пов’язано як із можливою високою професійністю порушників, так і з вразливістю всіх комп’ютеризованих систем [22].

Дослідження й аналіз інформаційної безпеки різних розподілених обчислювальних систем підтверджують той факт, що, незалежно від використовуваних мережних протоколів, топології, інфраструктури розподілених обчислювальних систем, механізми реалізації загроз у розподілених інформаційно-

телекомунікаційних системах є інваріантними стосовно особливостей конкретної системи. Це пояснюється тим, що розподілені інформаційно-телекомунікаційні системи проектуються на основі однакових принципів, отже мають практично однакові проблеми безпеки [22].

Розглянемо найпоширеніші типи загроз і способи захисту від них докладніше.

Аналіз мережевого трафіку.

Аналіз мережевого трафіку («Sniffing») – метод пасивного спостереження за мережевим трафіком за допомогою деякого пристрою чи утиліти. Інформація зібрана шляхом перехоплення може використовуватися для підготовки других типів мережевих атак чи викрадення інформації [10].

Мета атаки: виявлення структури потоку даних, а також збір інформації для подальшого викрадення, наприклад, паспортні дані, ідентифікаційні номери, дані про функціонування мережі, фінансові дані тощо [10, 22].

Об’єкт атаки: мережевий трафік.

Опис атаки: Зловмисник може використовувати різні програми для вивчення або захоплення пакетів даних, залежно від його місяця знаходження. Для взлому можуть бути використані сучасні сніфери, які розроблені для діагностики мереж. За допомогою програм сніферів можна проаналізувати захоплені пакети та перетворити інформацію в статичну для збереження чи детального вивчення [23].

Наслідки атаки: доступ до даних сторонніми особами.

Методи захисту:

– проектування системи безпеки на етапі розробки архітектури мережі;

– відключення promiscous-режиму для мережевих інтерфейсів;

– використання протоколу IPSec для захисту пакетів, що передаються шифруванням. Технологія IPSec використовується для інкапсуляції та захисту даних шифруванням, підтримується більшістю сучасних маршрутизаторів, міжмережевих екранів та іншим мережевим обладнанням [23].

DoS- і DDoS-атаки.

Відмова в обслуговуванні (Denial Of Service) – злочинна атака на сервер або персональний комп’ютер користувача, щоб довести його до відмови, створити всі можливі умови при яких власники або користувачі обладнання чи системи втрачають можливість доступу до файлів та серверів, або мають складнощі з підключенням.

Мета атаки: порушення стабільної роботи мережі або сервера.

Об’єкт атаки: хости мережі.

Опис атаки: подібні атаки спрямовані перевантаження мережевого каналу трафіком з метою ускладнити чи заблокувати проходження по ньому корисної інформації.

Наслідки атаки: відмова пристрою.

Методи захисту:

– проектування системи безпеки на етапі розробки архітектури мережі;

– для мінімізації ризику від пристроїв, що підключені до інтернету, необхідно відключити невикористовувані мережеві функції та задіяти SSH;

– використання спеціального програмного забезпечення;

– фільтрація і блокіровка трафіку.

Підміна довіреного об'єкта мережі (Spoofing).

Під довіреним об'єктом розуміється елемент мережі (комп'ютер, міжмережевий екран, маршрутизатор і т.п.), що має легальне підключення, і яким присвоєні права для доступу до мережевих ресурсів інформаційної системи.

Мета атаки: порушення конфіденційності та цілісності інформації.

Об’єкт атаки: DNS-сервер, хости.

Опис атаки: процес здійснення атаки полягає в присвоєнні прав довіреного користувача, що дозволяє зловмисникові вести сеанс роботи з об'єктами системи від імені довіреного користувача. Для формування помилкового TCP-пакету атакуючому досить підібрати відповідні поточні значення ідентифікаторів TCP-пакета для даного TCP-з’єднання. Також атака даного типу може полягати в передачі службових повідомлень від імені мережевих керуючих пристроїв

(наприклад, від імені маршрутизаторів) про неправдиву зміну маршрутно-адресних даних. Ідентифікація переданих повідомлень здійснюється тільки за мережевою адресою відправника, яку легко підробити [24].

Наслідки атаки: порушення конфіденційності даних, зараження програмного забезпечення.

Методи захисту:

– контроль доступу – найефективніший метод захисту, а точніше, мінімізації IP-спуфінга. Його суть полягає в управлінні доступом. Будь-який трафік, який надходить із зовнішньої мережі має бути заблоковано. Це знизить ефективність IP-спуфінга.

– фільтрація RFC 2827 – застосовується до вихідного трафіку та блокує спуфінг чужих мереж користувачами нашої мережі. Полягає в фільтрації вихідного трафіку, який не містить вихідної адреси, очікуваної на даному інтерфейсі.

– аутентифікація – для зменшення ефективності спуфінгу необхідно впроваджувати методи аутентифікації, відмінні від аутентифікації на базі IP-адрес [25].

Соціальна інженерія.

Соціальна інженерія (Social Engineering) – використання некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації [24].

Мета атаки: зловмисник намагається отримати цікаві для її відомості через прямий контакт з людиною, що володіє необхідною інформацією, тим чи іншим способом (при веденні телефонної розмови, поштового листування, довірчої бесіди в кафе і т.д.) [24].

Об’єкт атаки: користувачі комп’ютерної техніки.

Опис атаки: джерелом загрози можуть бути електронні листи, текстові повідомлення в будь-яких месенджерах, SMS-повідомлення та телефонні дзвінки. Шахраї можуть видавати себе за співробітників банків і інших фінансових організацій, державних службовців, співробітників силових відомств, інтернет-провайдерів, представників поштових сервісів і великих веб-ресурсів і т.п. [26].

Наслідки атаки: порушення конфіденційності даних, зараження програмного забезпечення.

Методи захисту:

– навчання співробітників – всі працівники компанії мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації компанії, а також про способи запобігання витоку даних;

– актуальне антивірусне забезпечення на комп’ютерах співробітників;

– використання спеціалізованого програмного забезпечення для виявлення і попередження атак;

– обмеження прав користувачів в системі.

В результаті проведеного аналізу підсумуємо деякі варіанти кіберзахисту від мережевих атак:

– навчання співробітників поведінки, що ускладнює мережеву атаку;

– обмеження на користуванням мережею Інтернет співробітниками;

– підтримка актуальності антивірусного програмного забезпечення;

– проектування системи безпеки на етапі розробки архітектури мережі;

– використання сучасних маршрутизаторів під час проектування і розробки моделі кіберзахисту мережі;

– відключення promiscous-режиму для мережевих інтерфейсів;

– використання шифрування IPSec для захисту пакетів, що передаються.

РОЗДІЛ 2
ПОСТАНОВКА ЗАДАЧІ

2.1. Мета та задачі

Метою дипломної роботи є розробка моделі кіберзахисту розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства.

Об’єкт дослідження – інформаційно-телекомунікаційна система торгівельного підприємства на прикладі ТОВ «Весела торбинка».

Предмет дослідження – сукупність засобів програмно-технічного характеру, які можуть бути спрямовані на забезпечення кібербезпеки інформаційно-телекомунікаційної системи об’єкта дослідження.

Поставлена мета обумовила необхідність вирішення наступних завдань:

– розглянути поняття розподіленої інформаційно-телекомунікаційної системи та її захищеності;

– систематизувати основні причини виникнення проблем захисту інформаційно-телекомунікаційних систем;

– розглянути основні типи загроз розподілених інформаційно-телекомунікаційних систем;

– проаналізувати захищеність розподіленої інформаційно-телекомунікаційної системи об’єкта дослідження;

– розробити проект розподіленої інформаційно-телекомунікаційної системи об’єкта дослідження з урахуванням вимоги кіберзахисту;

здійснити основні налаштування пристроїв забезпечення безпеки в запропонованій моделі кіберзахисту інформаційно-телекомунікаційної системи.

2.2. Методи дослідження

Для досягнення поставленої мети використовувався комплекс загальнонаукових методів [16]:

– методи теоретичного узагальнення – при описі предметної області дослідження;

– аналізу та синтезу – при дослідженні захищеності діючої розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства;

– формалізації – при створенні проектів розподіленої комп'ютерної мережі в симуляторі Cisco Packet Tracer;

– системного аналізу та експерименту– при розробці моделі кіберзахисту розподіленої інформаційно-телекомунікаційної системи та налаштуванні пристроїв забезпечення безпеки.

2.3. Вибір засобів реалізації

Для розробки моделі інформаційно-телекомунікаційної системи торгівельного підприємства в дипломній роботі прийнято рішення використати симулятор Cisco Packet Tracer.

Cisco Packet Tracer – це програма, створена компанією Cisco для відтворення роботи власного обладнання: роутерів, комутаторів, бездротового обладнання, серверів, ПК і т.д. Даний симулятор дає можливість здобути досвід в налаштуванні реальної мережі, яка може містити необмежену кількість пристроїв. Налаштування обладнання здійснюється декількома способами: введення команд в операційну систему Cisco IOS, через графічний веб-інтерфейс, командами та графічним меню операційної системи. В Packet Tracer режим віртуалізації дає можливість користувачу відстежити переміщення пакетів даних та отримати повну інформацію про них на всіх пристроях мережі. За допомогою симулятора можна виявити слабкі місця, несправності та надійність мережі [17, 18].

Переваги:

– зрозумілий графічний інтерфейс;

– можливість моделювання фізичної і логічної топології;

– наявність режиму симуляції, в якому наглядно зображені всі процеси що проходять в мережі;

– можливість додавання/видалення коментарів [19, 20].

Недоліки:

– підтримуються не всі команди реального Cisco IOS;

– можливість створення імітаційної моделі лише для обладнання компанії Cisco Systems;

– Cisco Packet Tracer доступний для скачування лише для інструкторів, студентів, випускників та адміністраторів Мережевої академії Cisco [19, 20].

З урахуванням недоліків програмного забезпечення Cisco Packet Tracer, його можливостей достатньо для використання в якості засобу реалізації моделі розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства для досягнення поставленої мети дипломної роботи.

РОЗДІЛ 3
АНАЛІЗ ЗАХИЩЕНОСТІ ДІЮЧОЇ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ОБ’ЄКТА ДОСЛІДЖЕННЯ

3.1. Опис інформаційного простору об’єкта дослідження

Товариство з обмеженою відповідальністю «Весела торбинка» (ТОВ «Весела торбинка») засноване в 2012 році і на даний момент має мережу з 15 структурних підрозділів під торговою маркою «САМ Маркет». Структура підприємства складається з досить великої кількості підрозділів, розташованих на відстані один від одного. Це склади, торгові точки, розташовані не тільки в різних районах міста, а й в різних населених пунктах.

В кожному структурному підрозділі організовано незалежні локальні комп'ютерні мережі, об'єднані між собою в мережу більш високого рівня – корпоративну, що має центральний офіс, де концентрується вся інформація, яку збирають зі структурних підрозділів підприємства. В центральному офісі організовано автоматизоване сховище даних, інструментарій якого дозволяє виконувати аналіз інформації, що надходить, генерувати на основі аналітичних даних оптимальні управлінські рішення по підвищенню ефективності функціонування підприємства.

Для можливості доступу до сервісів виділено наступні групи користувачів:

- Системний адміністратор;
- Директор;
- Бухгалтерія;
- Відділ кадрів;
- Адміністратори магазину;
- Касири;
- Оператори.

Організація розподіленої інформаційної-телекомунікаційної системи, що об'єднує всі локальні комп'ютерні мережі структурних підрозділів торгівельного підприємства, дозволяє:

– об'єднати автономно розподілені процеси обробки інформації торгівельного підприємства;

– об'єднати інформаційні ресурси підприємства в загальну систему з організацією автоматизованого сховища інформації;

– зменшити фінансові витрати на обробку інформації при організації торгового процесу;

– оптимізувати функціонування прикладних програмних продуктів, що використовуються в торгівельному підприємстві;

– надати працівникам торгівлі сучасний комплекс програмно-апаратних засобів збору, зберігання і обробки необхідної інформації;

– забезпечити ефективність спільної роботи фахівців;

– раціонально використовувати електронне торгове обладнання, персональні комп'ютери, периферійні пристрої і т.д.;

– скоротити обсяг паперових технологій в адміністративній роботі і безпосередньо в процесі торговельної діяльності;

– і т.д.

3.2. Аналіз захищеності розподіленої інформаційно-телекомунікаційної системи ТОВ «Весела торбинка»

Для побудови схеми діючої розподіленої інформаційно-телекомунікаційної системи ТОВ «Весела торбинка» було використано симулятор Cisco Packet Tracer. Оскільки торгові точки підприємства мають аналогічну топологію було прийнято рішення зобразити на схемі головний офіс та п’ять магазинів.

Загальну схема мережі наведено на рисунку 3.1.

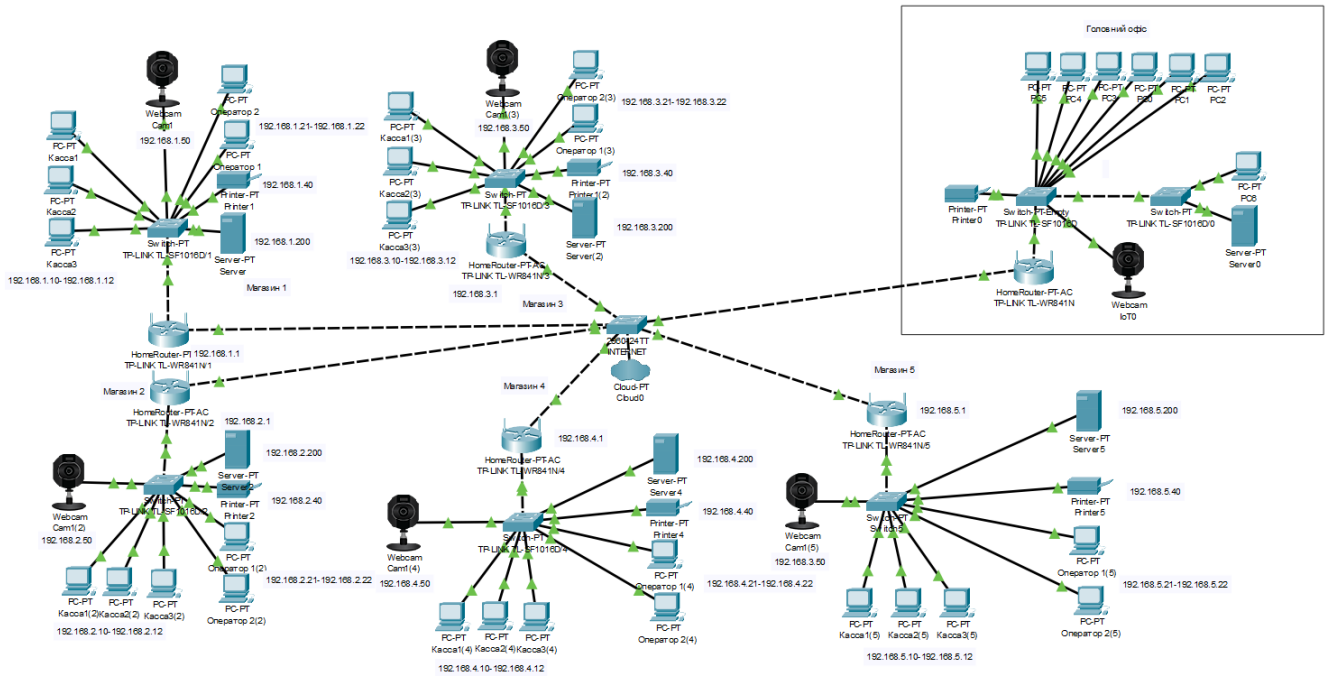

Рисунок 3.1 – Загальна схема розподіленої інформаційно-телекомунікаційної мережі ТОВ «Весела торбинка»

У кожному магазині налаштована своя локальна мережа топології «зірка». Кожен магазин має свій окремий сервер для збереження інформації. В кожній локальній мережі робочі станції з’єднуються з комутатором, а той в свою чергу з маршрутизатором (рис. 3.2).

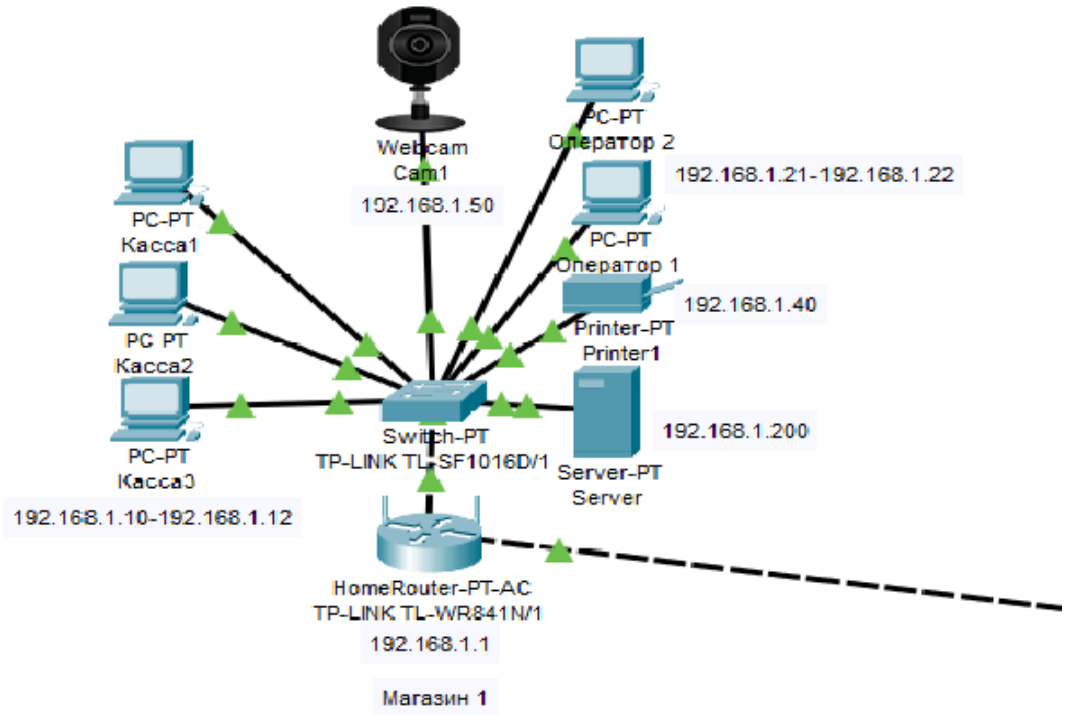

Рисунок 3.2 – Схема локальної мережі магазину

Розподіл IP-адрес для кожного з вузлів мережі – динамічний, маршрутизація – динамічна.

Мережа ТОВ «Весела торбинка» включає такі структурні елементи як: робочі станції PC-PT, сервери, комутатори, маршрутизатори, камери відеоспостереження та мережеві принтери.

Терміном «робоча станція» позначають стаціонарний комп'ютер в складі локальної обчислювальної мережі по відношенню до сервера [18]. Робочі станції використовуються співробітниками для вирішення прикладних задач. Частина робочих станцій магазинів доповнена допоміжними пристроями – принтерами чеків, сканерами штрих-кодів та ін.

Сервер – багатокористувацький комп'ютер, виділений для обробки запитів від всіх робочих станцій. Він надає робочим станціям доступ до системних ресурсів і розподіляє ці ресурси [18]. На сервери магазинів та головного офісу встановлено операційні системи сімейства Windows.

Мережевий комутатор – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента [18]. В комп’ютерній мережі ТОВ «Весела торбинка» використовуються некеровані комутатори TP-Link та D-Link. Некерований комутатор не вимагає налаштування, завдяки чому його встановлення не створить для користувача ніяких проблем. Некеровані комутатори мають меншу пропускну здатність, ніж керовані комутатори. Зазвичай некеровані комутатори використовуються в домашній мережі тому при розробці моделі кіберзахисту інформаційно-телекомунікаційної системи ТОВ «Весела торбинка» необхідно враховувати цей момент.

Маршрутизатор – мережевий пристрій, який поєднує різні комп’ютерні мережі та мережі побудовані за різними технологіями і управляє обміном даними між ними [18]. В комп’ютерній мережі ТОВ «Весела торбинка» використовуються маршрутизатори TP-Link.

Для торгівельних організацій зі зростаючою мережею магазинів доцільно встановлювати міжмережеві екрани, наприклад, Cisco ASA.

Якщо подивитися на функції і технології, які зазвичай використовують організації, то вони присутні як в міжмережевих екранах так і в маршрутизаторах. Однак міжмережевий екран варто обрати в тому випадку, коли в головному офісі потрібно організувати безпечний доступ в Інтернет, захищений віддалений доступ користувачів і підключення віддалених філій [27].

Головне призначення Cisco ASA це безпека. І такі функції безпеки як міжмережевий екран, IPS, VPN, підключення віддалених користувачів, з технічної точки зору реалізовані краще ніж на звичайному маршрутизаторі. У міжмережевих екранах за замовчуванням включені багато функцій безпеки, які на маршрутизаторі необхідно налаштовувати в ручну, або взагалі відсутні [27].

На сьогоднішній день в комп'ютерній мережі об'єкта дослідження використовується тип кабелю вита пара UTP5.

Вита пара (англ. Twisted pair) – мережевий кабель, який складається зі скручених в джгут декількох ізольованих провідників. Найпоширеніший кабель складається з двох або чотирьох пар. Скручування між собою пар дає кабелю захист від перешкод. Характеризується категоріями. Найчастіше зустрічається Cat 5e UTP.

Захист розподіленої інформаційно-телекомунікаційної системи в ТОВ «Весела торбинка» забезпечується наступними заходами:

1. Перевірка того, що користувач сервісів компоненту розподіленої системи є дійсно користувачем, якому дозволено мати доступ до сервісів та даних системи (аутентифікація).

2. Обмеження доступу до сервісів компонента залежно від результатів аутентифікації (авторизація). Для вирішення цього завдання реалізовано обмеження доступу, в основу якого покладено ролі.

3. Зміна стандартних портів маршрутизаторів для підключення по RDP.

З урахуванням проведеного аналізу можна зробити висновок, що розподілена інформаційно-телекомунікаційна система ТОВ «Весела торбинка» є недостатньо захищеною та потребує вдосконалення.

РОЗДІЛ 4
РОЗРОБКА МОДЕЛІ КІБЕРЗАХИСТУ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ТОРГІВЕЛЬНОГО ПІДПРИЄМСТВА

4.1. Проектування розподіленої комп'ютерної мережі торгівельного підприємства з використанням симулятора Cisco Packet Tracer

При проектуванні розподіленої комп'ютерної мережі ТОВ «Весела торбинка» необхідно враховувати, що вона має відповідати зростаючим вимогам торгівельного підприємства, а саме легко масштабуватися при необхідності збільшення робочих станцій; підтримувати механізми забезпечення якості сервісу, бути безпечною та продуктивною.

Оскільки для проектування мережі ТОВ «Весела торбинка» було прийнято рішення використовувати симулятор Cisco Packet Tracer, для формування інформаційно-телекомунікаційної системи обиралося обладнання Cisco Systems.

При виборі обладнання керувалися його характеристиками.

Виходячи із фінансової і практичної точки зору, а також необхідністю кіберзахисту мережі, організації безпечного доступу в Інтернет і підключення віддалених магазинів в головному офісі було прийнято рішення встановити міжмережевий екран Cisco ASA 5506-X.

Cisco ASA 5506-X забезпечує безпрецедентний рівень захисту від мережевих загроз завдяки таким можливостям: глибока перевірка мережі, аналіз окремих потоків, безпека підключень за рахунок оцінки захищеності кінцевих пристроїв, підтримка передачі голосових і відеоданих через VPN (табл. 4.1).

Міжмережевий екран Cisco ASA 5506-X: 8 портів 10/100/1000 BaseT Ethernet, 1 порт USB 2.0, серійні порти RJ-45 Console і Mini USB, блок живлення AC (рис. 4.1).

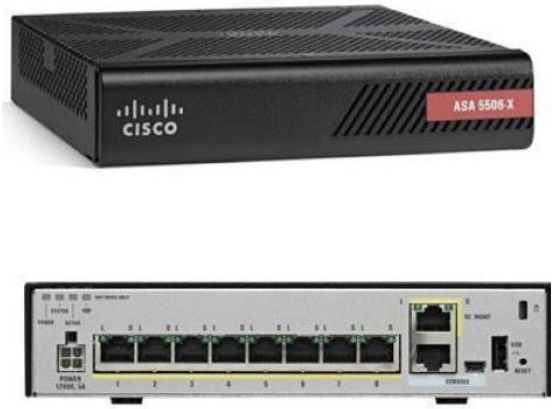

Рисунок 4.1 – Маршрутизатор Cisco ASA 5506-X

Таблиця 4.1 – Технічні характеристики Cisco ASA 5506-X [28]

Тип пристрою	Міжмережевий екран
Порти доступу Ethernet	8 x GE RJ-45
Число IPSec VPN	10
Продуктивність FIREWALL	750 Мбіт/с
VLAN 802.1q стандарт/макс	5/30
Габаритні розміри (ВхШхГ)	4,45x20,04x17,45
Пам’ять FLASH	16 Гб
Об’єм ОЗУ	4 Гб
Тип живлення	AC 100-240В
IPSec VPN 3DES/AES	100 Мбіт/с
Нових сесій в секунду, макс	5000
Тип встановлення	Настільне
Продуктивність IPS	125 Мбіт/с
Висока доступність	Ні
Кількість захищених вузлів	Не обмежено

Для мережі магазинів було обрано маршрутизатори Cisco 2811.

Маршрутизатори Cisco 2811 мають встановлене програмне забезпечення Cisco IOS та підтримують ідею самозахисту мережі – Cisco Self-Defending Network

маючи вдосконалені функції безпеки, підтримуючи IPSec VPN, систему попередження вторгнень (IPS), контроль доступу (NAC) та фільтрацію за URL-адресами (табл. 4.2).

Ключові особливості: висока продуктивність, модульна архітектура, апаратна підтримка засобів забезпечення безпеки, можливість використання технологій передачі електроенергії по мережам Ethernet (PoE).

Маршрутизатор Cisco 2811: 2 порти Fast Ethernet (10/100BASE-T), 2 порти USB 1.1, 4 слоти HWIC/WIC/VIC/VWIC, 1 слот NM/NME, 2 слота PVDM2, 2 слота AIM (рис. 4.2).

Рисунок 4.2 – Маршрутизатор Cisco 2811

Таблиця 4.2 – Технічні характеристики Cisco 2811

Тип пристрою	Маршрутизатор
Вбудовані порти LAN	2*10/100 TX
Пам’ять Flash, Мб (станд./макс)	64 / 128
Пам’ять DRAM, Мб (станд./макс)	256 / 768
Інтегровані PVDM (DSP) слоти	2
Підтримка інтерфейсних карт	4 слота (кожен слот підтримує любий HWIC, WIC, VIC и VWIC-модулі)
Наявність мережевих слотів	1
Порти USB 1.1	2
Консольний порт (до 115.2 Кбіт/с)	1

Продовження таблиці 4.2

Додатковий порт (AUX) (до 115.2Кбит/с)	1
Монтаж на стені	так
Апаратне прискорення VPN	DES, 3DES, AES 128, AES 192, та AES 256
AC-IP Maximum In-Line Power Distribution	160W

Проаналізувавши наявну вхідну інформацію, було створено логічну схему комп'ютерної мережі торгівельного підприємства ТОВ «Весела торбинка» (рис. 4.3).

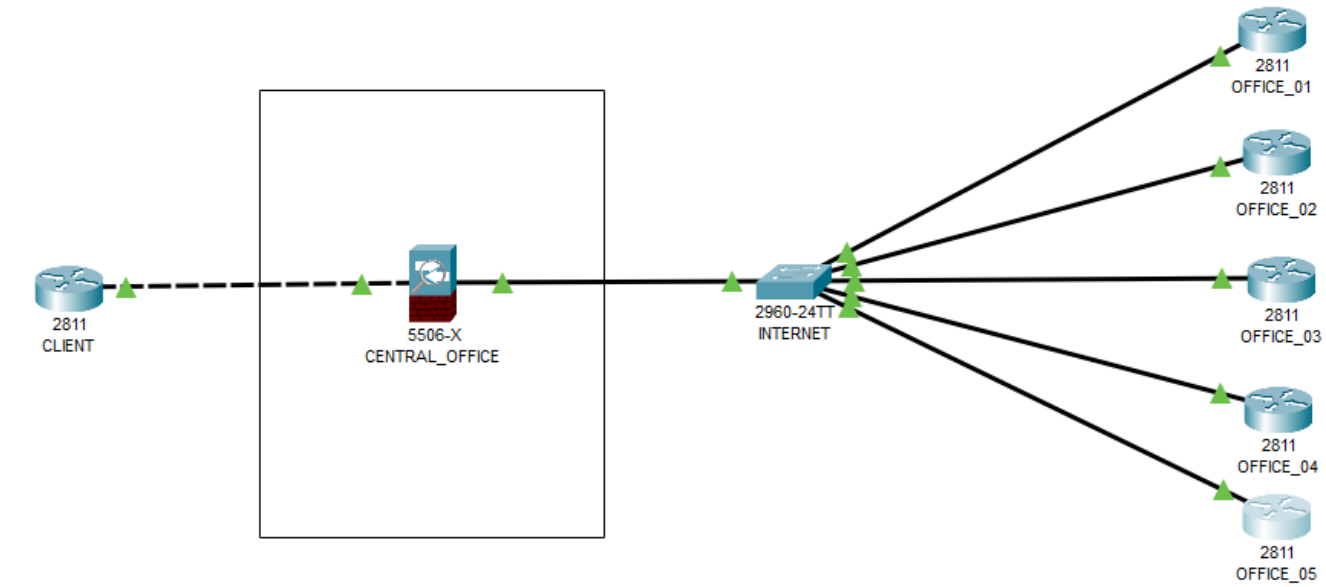

Рисунок 4.3 – Логічна схема комп'ютерної мережі торгівельного підприємства ТОВ «Весела торбинка» (основні комутаційні вузли)

На логічній схемі комп'ютерної мережі торгівельного підприємства ТОВ «Весела торбинка» представлені:

– фізичні пристрої мережі;

– типи пристроїв;

– імена пристроїв;

– лінії зв’язку.

4.2. Налаштування конфігурації багатофункціонального пристрою забезпечення безпеки Cisco ASA 5506-X

Налаштуємо пристрій Cisco ASA 5506-X на виконання функцій захисту мережі за допомогою наступного набору основних команд (interface, nameif, security-level, ip address, route). Розглянемо детальніше кожну з них:

– interface – використовується для ідентифікації типу апаратних засобів, що використовуються, встановлює параметри продуктивності та ініціалізує інтерфейси. Синтаксис: interface ідентифікатор.

– nameif – використовується для присвоєння імені інтерфейсам ASA. Синтаксис: nameif ідентифікатор імені.

– security-level – використовується для визначення рівня безпеки інтерфейсу. За замовчуванням зовнішній інтерфейс Ethernet0 має рівень безпеки 0, а внутрішній інтерфейс Ethernet1 має рівень безпеки 100. Синтаксис: security-level рівень.

– ip address – дозволяє кожному із інтерфейсів пристрою захисту присвоїти ip адресу. Синтаксис: ip address ім’я IP_адреса [маска].

– route – використовується для задання статичних маршрутів для інтерфейсів. Синтаксис: route имя IP_адрес маска шлюз [метрика].

Сконфігуруємо два інтерфейси INET та LAN, перший з який призначений для зовнішньої мережі, а другий відповідно для внутрішньої. Результати налаштування представлено на рисунку 4.4.

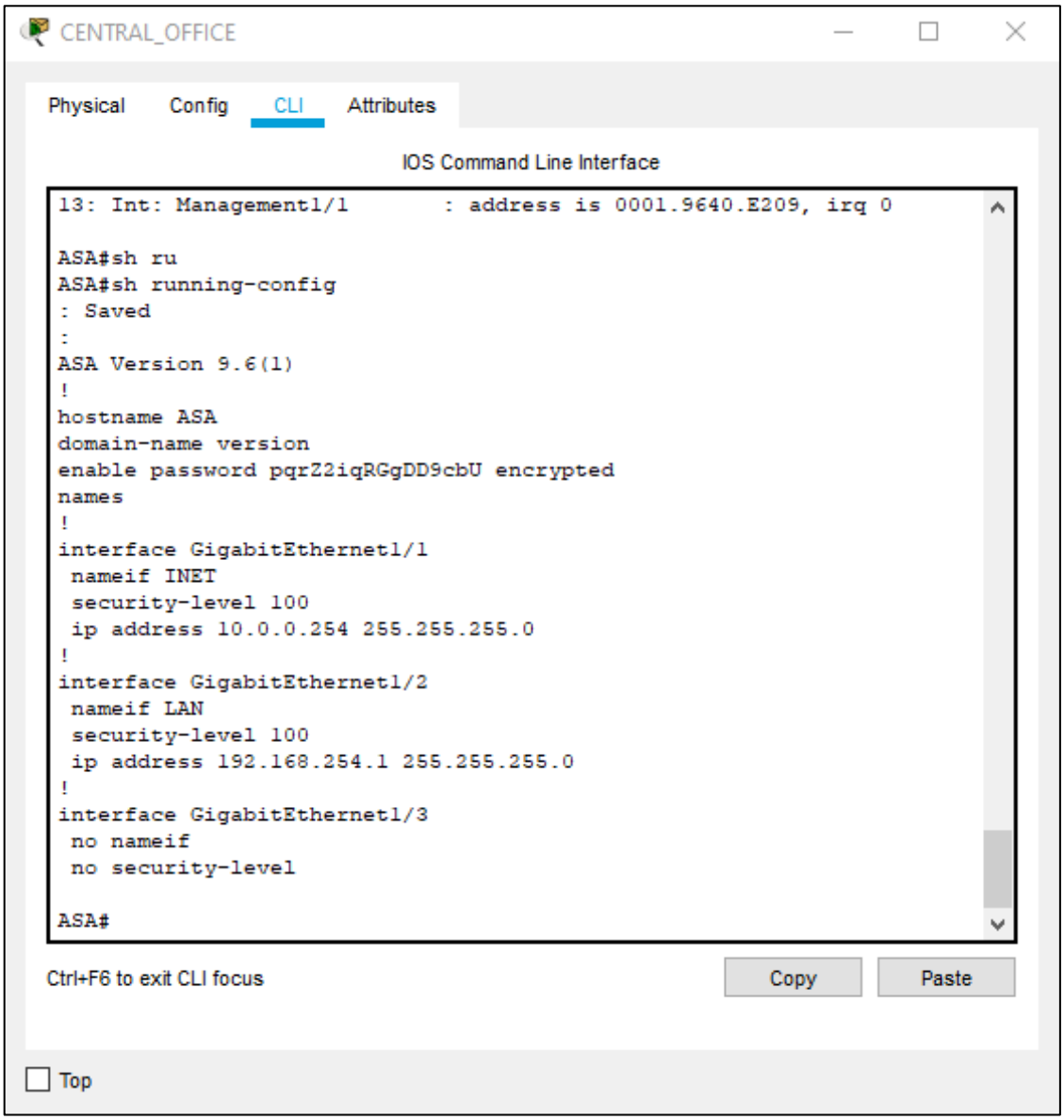

Рисунок 4.4 – Налаштування інтерфейсів

Далі здійснимо налаштування параметрів шифрування за допомогою набору протоколів IPSec. IPSec забезпечує захист дані, що передаються по міжмережевому протоколу IP. Результати налаштування представлено на рисунку 4.5.

Відповідність політик IKEv1 встановлюється, коли обидві політики від двох однорангових вузлів містять однакові значення параметрів аутентифікації, шифрування, хешу і Діффі-Хеллмана.

Для налаштування використовуємо команди, представлені в лістингу 4.1.

Лістинг 4.1 – Налаштування параметрів шифрування за допомогою набору протоколів IPSec

```
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ikev1 policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit
```

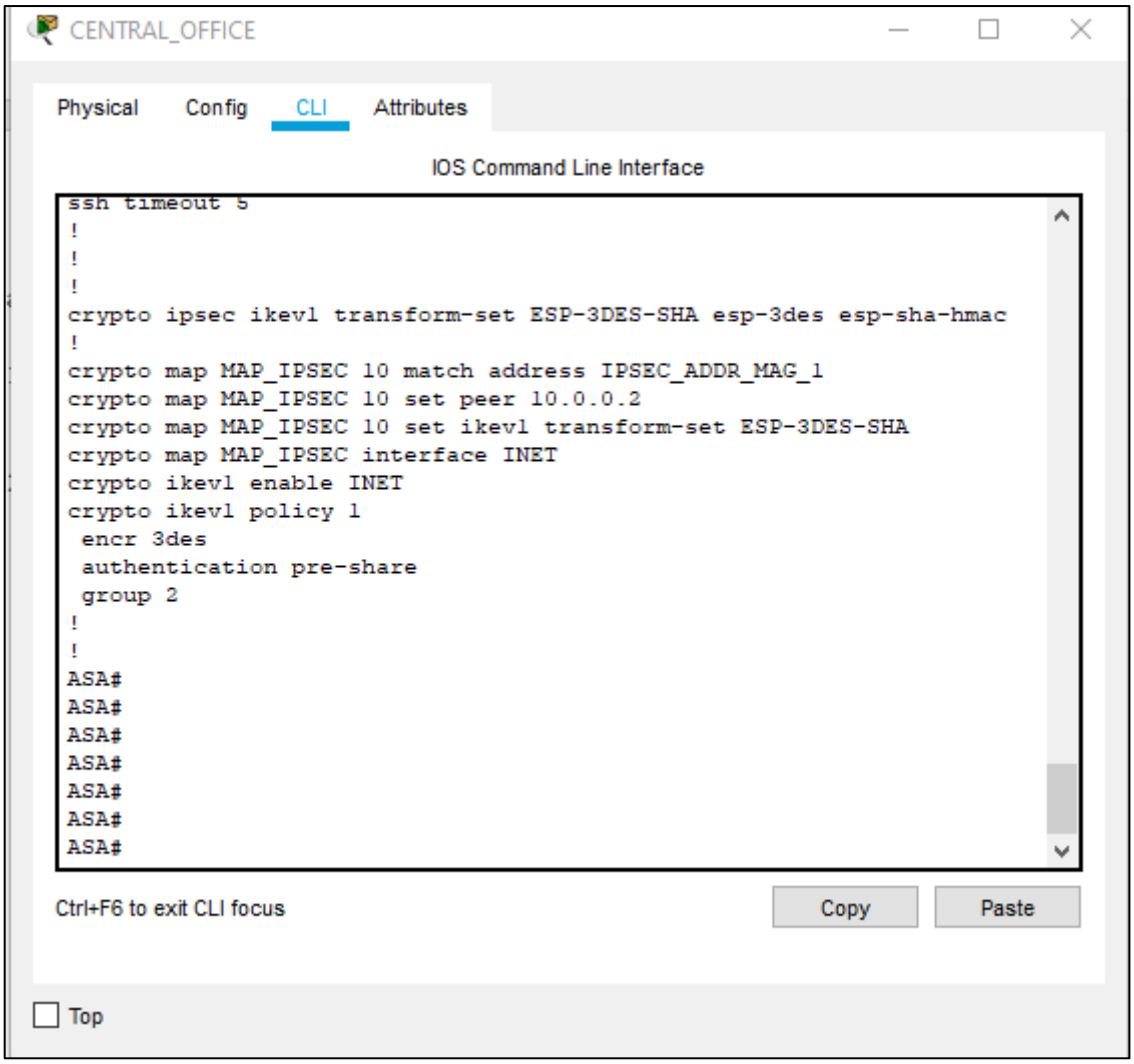

Рисунок 4.5 – Налаштування параметрів шифрування за допомогою набору протоколів IPSec

Для налаштування списку контролю доступу для потрібного трафіку VPN використовується розширений або іменований список контролю доступу для вказаного трафіку, який повинен бути захищений шифруванням (лістинг 4.2). Результати налаштування представлено на рисунку 4.6.

Лістинг 4.2 – Налаштування списку контролю доступу

```
access-list IPSEC_ADDR_MAG_1 extended permit ip 192.168.254.0 255.255.255.0 192.168.1.0 255.255.255.0
```

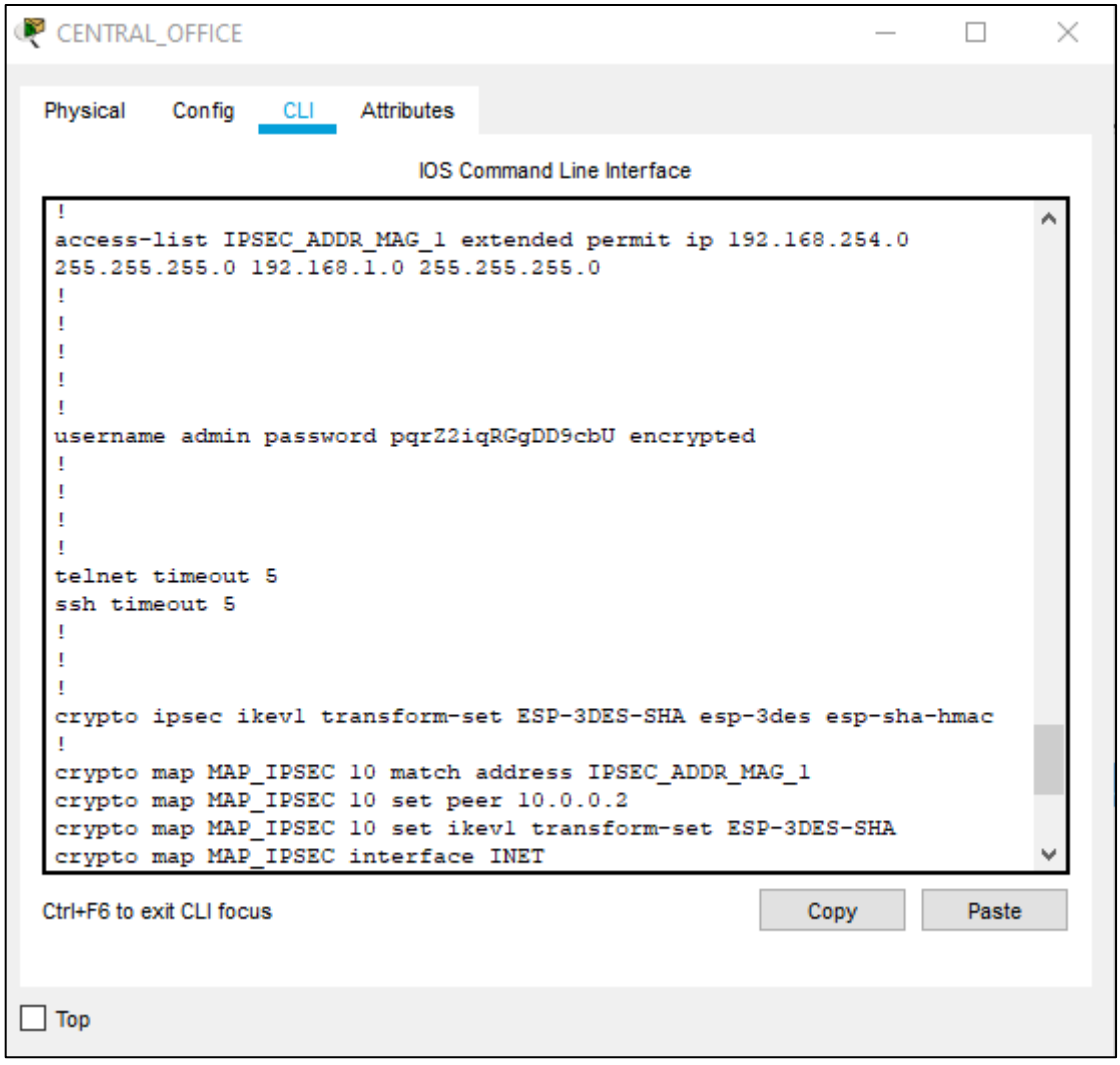

Рисунок 4.6 – Налаштування списку контролю доступу

Налаштуємо кріптосхему і застосуємо її до інтерфейсу INET (лістинг 4.3). Результати налаштування представлено на рисунку 4.7.

Кріптосхема визначає політику IPsec для узгодження в SA IPSEC і включає:

– список контролю доступу для визначення пакетів, які з'єднання IPSec дозволяє і захищає;

– ідентифікацію тимчасових вузлів;

– локальні адреси для трафіку IPSec;

– набори перетворень IKEv1.

Лістинг 4.3 – Налаштування кріптосхеми

```
crypto map MAP_IPSEC 10 match address IPSEC_ADDR_MAG_1
crypto map MAP_IPSEC 10 set peer 10.0.0.2
crypto map MAP_IPSEC 10 set ikev1 transform-set ESP-3DES-SHA
crypto map MAP_IPSEC interface INET
```

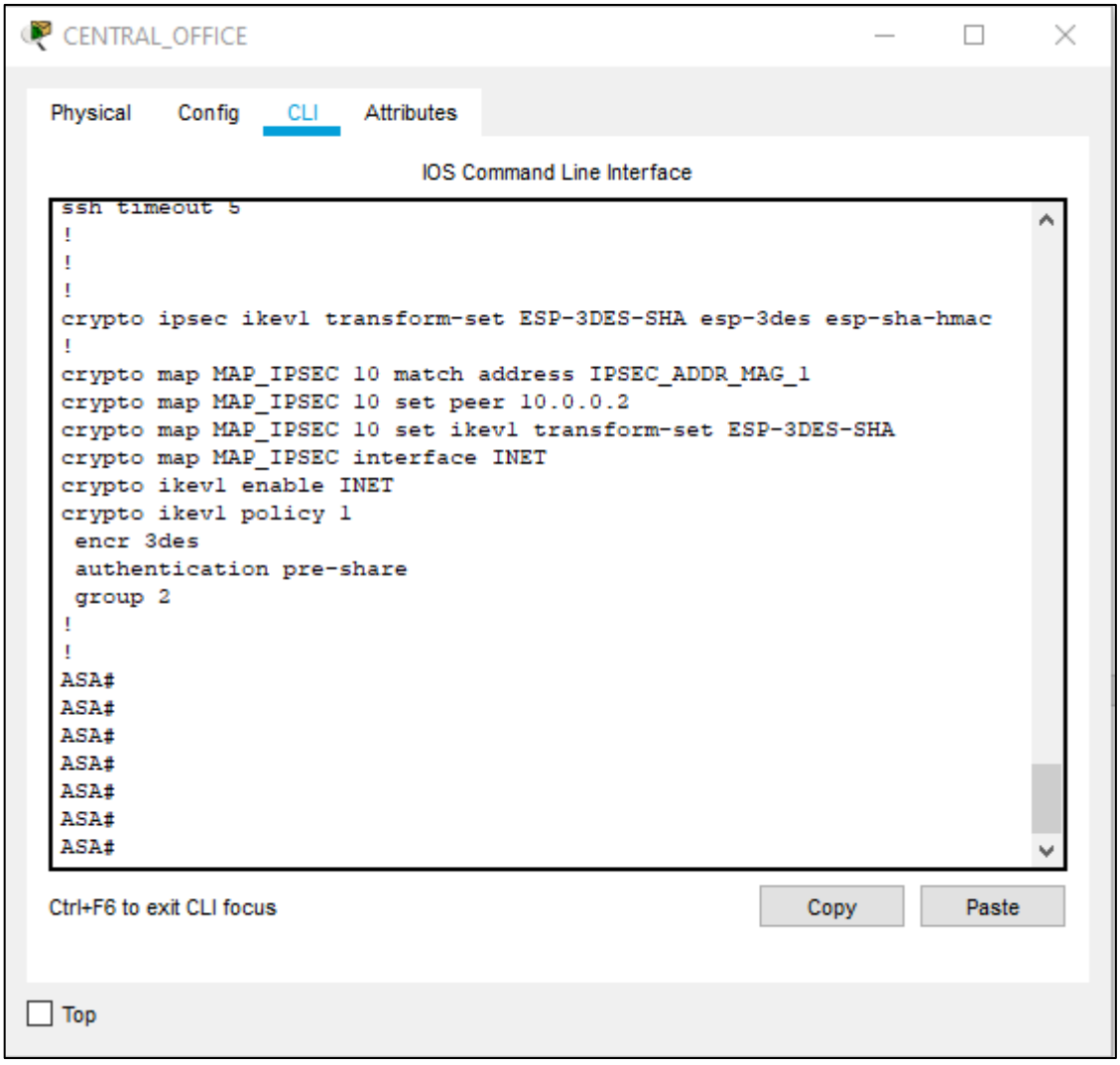

Рисунок 4.7 – Налаштування кріптосхеми

Виконаємо налаштування тунельної групи (профіль з'єднання локальних мереж).

Для тунелю між локальними мережами використовується тип профілю з'єднання ipsec-l2l. Для того щоб налаштувати зумовлений ключ IKEv1 необхідно виконати команди з лістингу 4.4.

Лістинг 4.4 – Налаштування тунельної групи

```
tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
pre-shared-key passw0rd
exit
```

Для налаштування маршрутизації між головним офісом та магазином необхідно виконати команду лістингу 4.5.

Лістинг 4.5 – Налаштування маршрутизації

```
route INET 192.168.1.0 255.255.255.0 10.0.0.2
```

Результати налаштування представлено на рисунку 4.8.

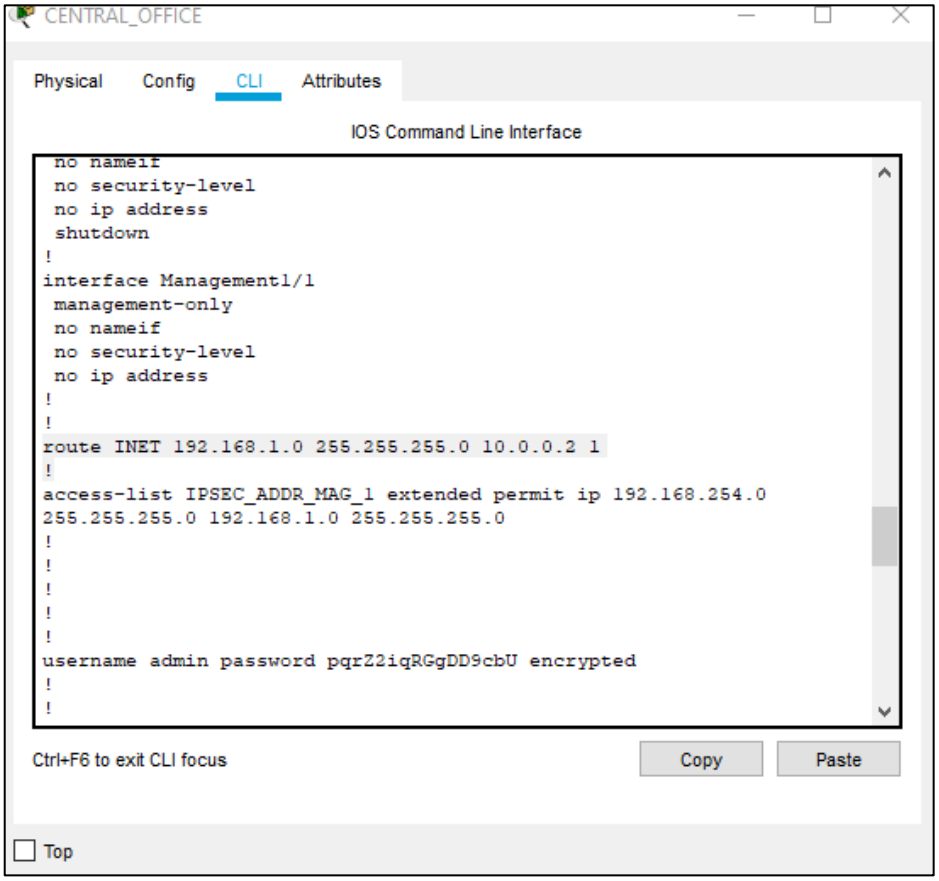

Рисунок 4.8 – Налаштування маршрутизації

4.3. Налаштування маршрутизаторів Cisco 2811

Запропонована схема мережі ТОВ «Весела торбинка» складається з головного офісу та п’яти типових магазинів. Для кожного магазину запропоновано використовувати маршрутизатор Cisco 2811, отже їх налаштування буде типовим. В рамках дипломної роботи розглянемо налаштування маршрутизатору Cisco 2811 на прикладі одного магазину.

В першу чергу виконаємо налаштування ISAKMP – інтернет проколу асоціації безпеки та керування ключами. ISAKMP забезпечує платформу обміну ключами і застосовується для незалежного обміну ключами. Зазвичай для обміну ключами використовує IKE – стандартний протокол набору протоколів IPSec, що використовуються для захисту взаємодії в VPN.

Створюємо політику ISAKMP для Фази 1. Тип тунелю L2L (лістинг 4.6)

Лістинг 4.6 – Створення політики ISAKMP для Фази 1

```
 crypto isakmp policy 10
 hash sha
 authentication pre-share
!
 crypto isakmp key vpnuser address 10.0.0.254
```

Команда crypto isakmp policy використовується для створення політик IKE, в яких вказані бажані алгоритми та параметри створюваного захищеного каналу. В наведеному лістингу створено політику IKE з пріоритетом 10.

Результат виконання команди наведено на рисунку 4.9.

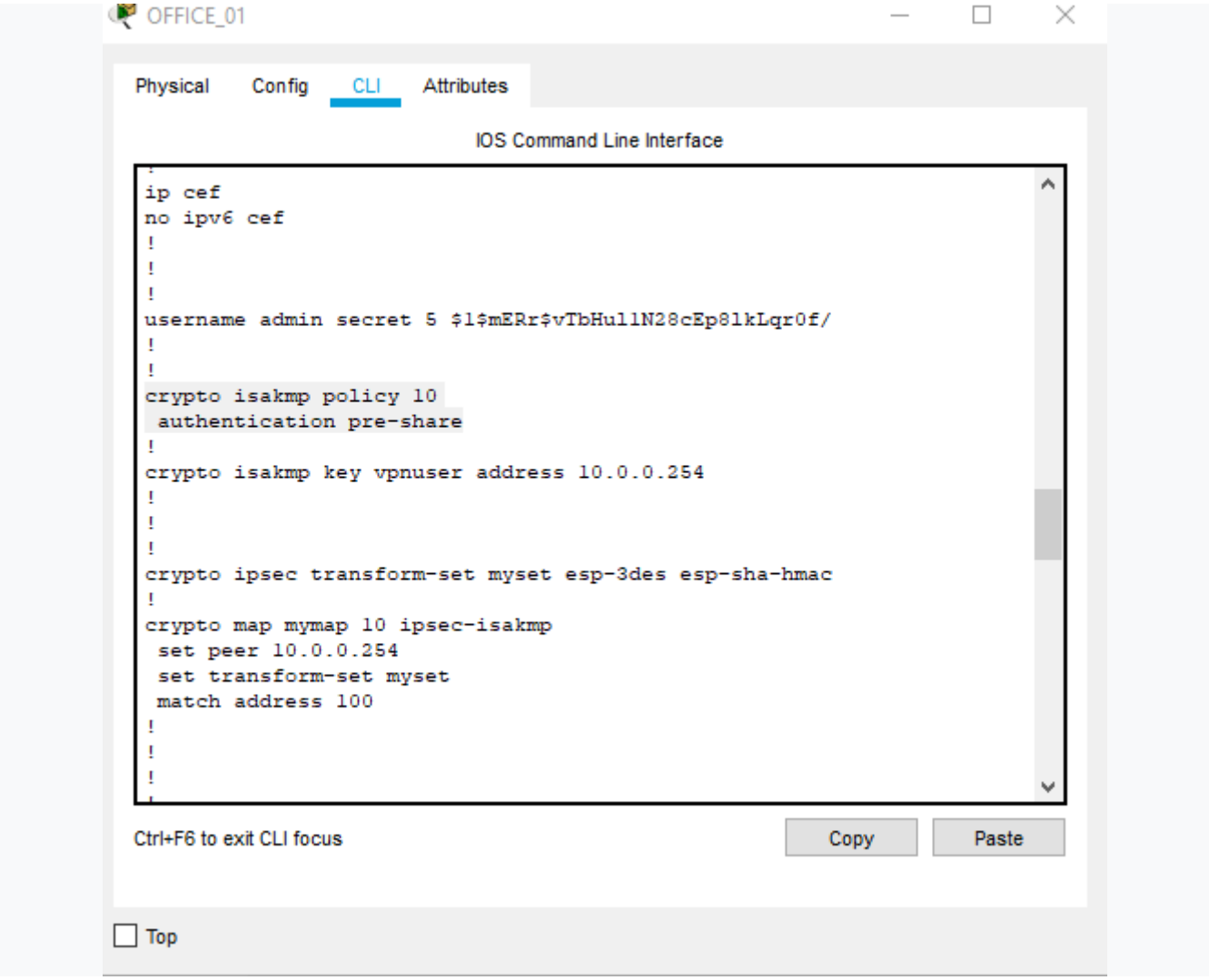

Рисунок 4.9 – Створення політики ISAKMP для Фази 1

Створюємо політику для Фази 2 для забезпечення фактичного шифрування даних (лістинг 4.7)

Лістинг 4.7 – Створення політики для Фази 2

```
crypto ipsec transform-set myset esp-3des esp-sha-hmac
```

Результат виконання команди наведено на рисунку 4.10.

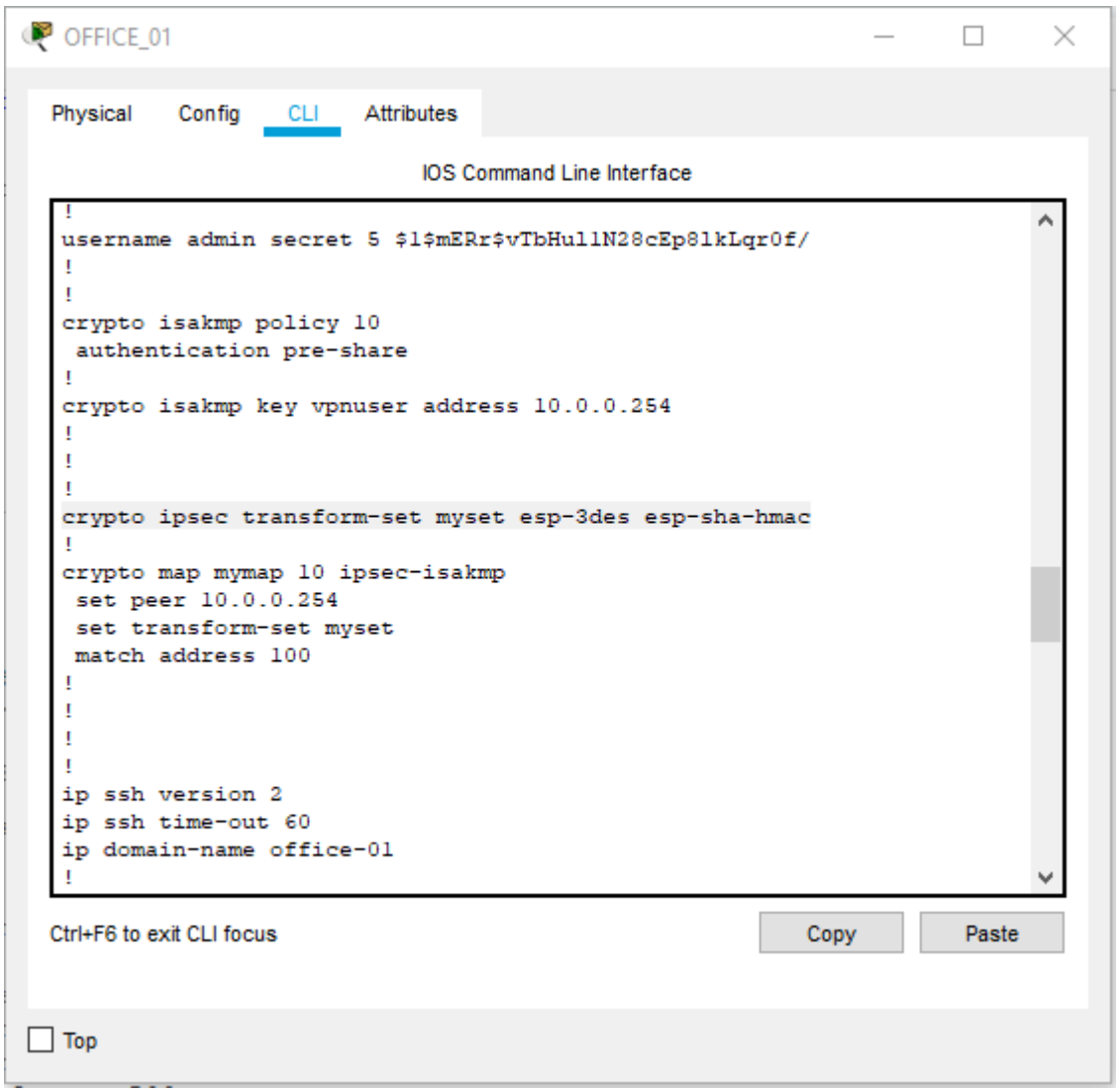

Рисунок 4.10 – Створення політики для Фази 2

Створюємо актуальну криптографічну карту (лістинг 4.8).

Лістинг 4.8 – Створення криптографічної карти

```
crypto map mymap 10 ipsec-isakmp
 set peer 10.0.0.254
 set transform-set myset
 match address 100
```

Результат виконання команди наведено на рисунку 4.11.

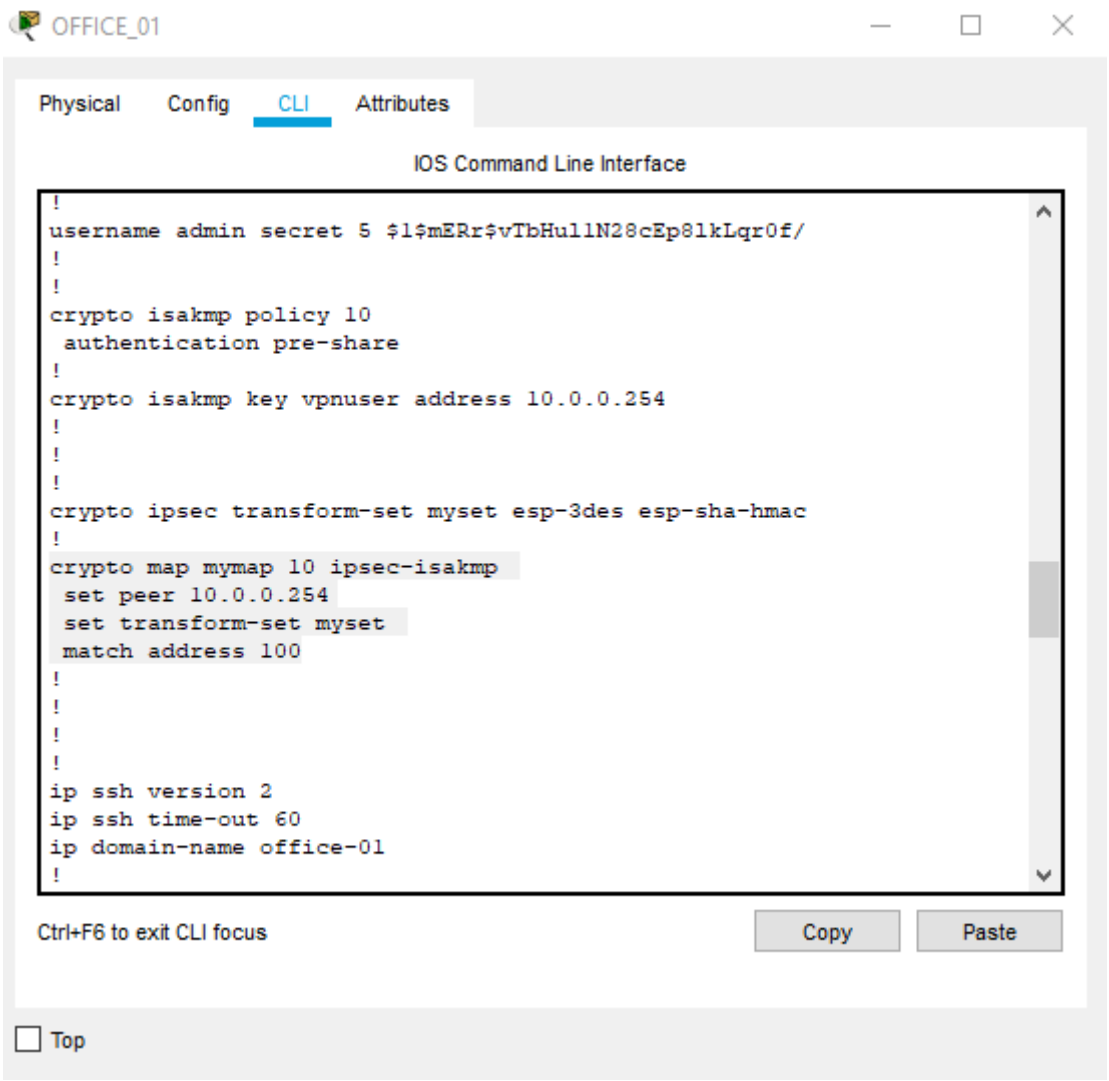

Рисунок 4.11 – Створення криптографічної карти

Застосуємо криптографічну карту на зовнішній інтерфейс (лістинг 4.9).

Лістинг 4.9 – Застосування криптографічної карти на зовнішній інтерфейс

```
interface fastethernet0/0
 ip address 10.0.0.2 255.255.255.0
 crypto map mymap
```

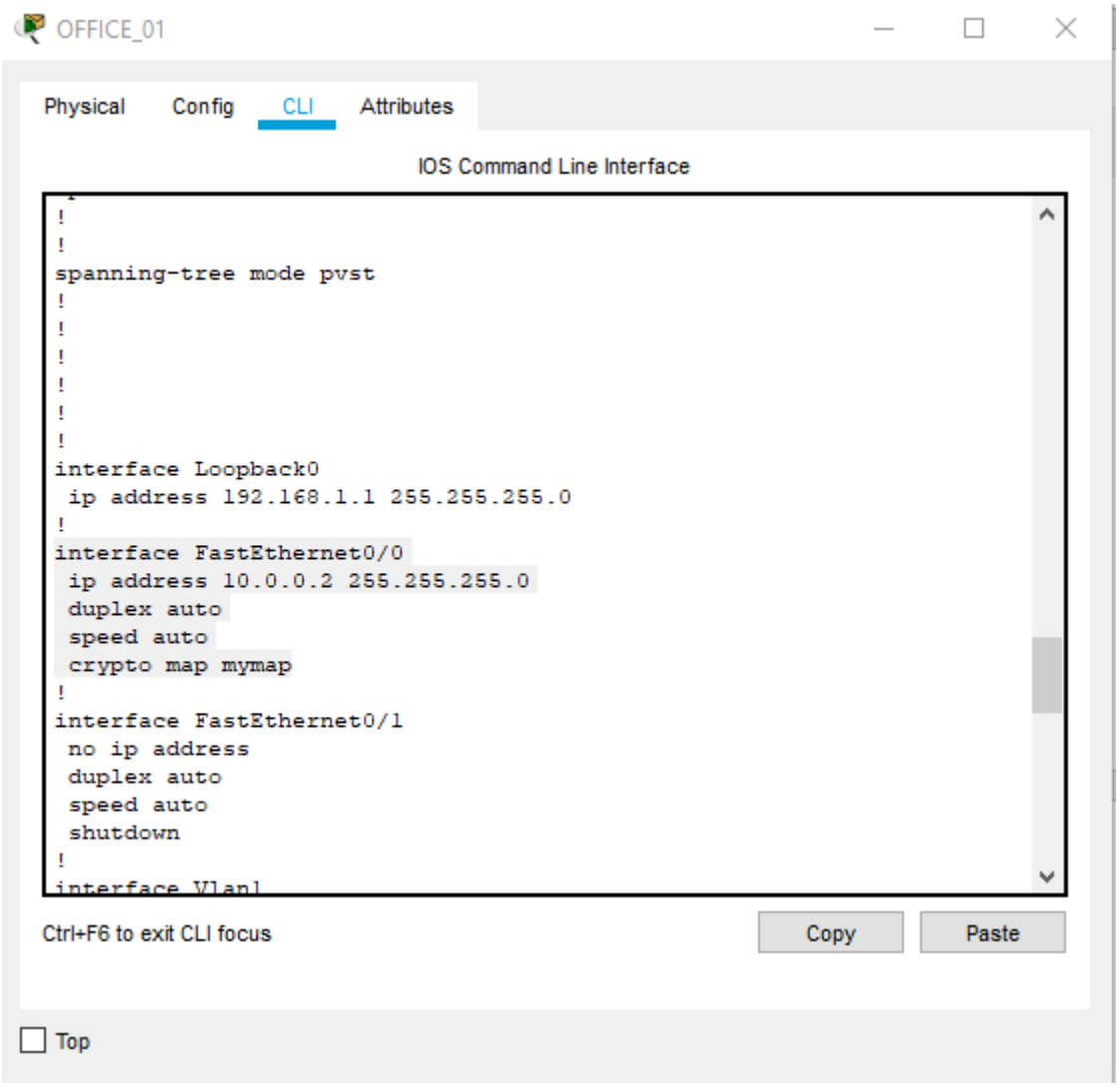

Рисунок 4.12 – Застосування криптографічної карти на зовнішній інтерфейс

Створимо ACL (Access Control List) для зашифрованого трафіку (рис. 4.13).

Лістинг 4.10 – Створення ACL (Access Control List) для зашифрованого трафіку

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.254.0 0.0.0.255
line con 0
line aux 0
line vty 0 4
```

Трафік з 192.168.1.0 до 192.168.254.0 зашифровано. Трафік, який не відповідає списку доступу, незашифрований для Інтернету.

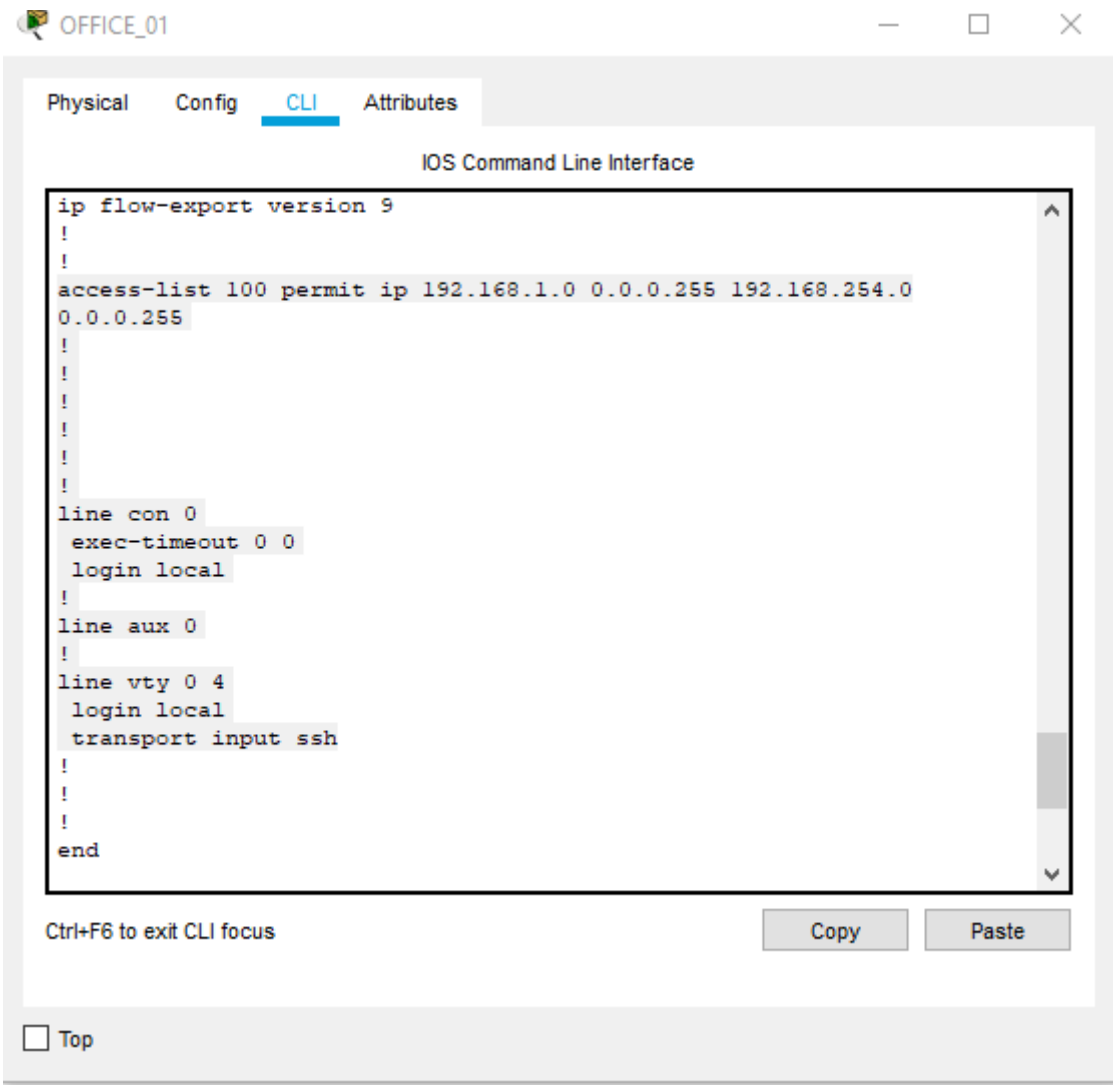

Рисунок 4.13 – Створення ACL для зашифрованого трафіку

ВИСНОВКИ

В результаті написання дипломної роботи було розглянуто та проаналізовано сутність поняття розподіленої інформаційно-телекомунікаційної системи та сформульовано її значення для торгівельних підприємств. Систематизовано основні причини виникнення проблем захисту інформаційно-телекомунікаційних систем та узагальнено існуючі методи їх попередження, в результаті чого можна зробити висновок, що кіберзахист має бути головним елементом організації мережі. Також було розглянуто основні типи загроз розподілених інформаційно-телекомунікаційних систем та узагальнено базові методи захисту від атак, а точніше методи зменшення ризику мережевих атак.

Крім того в ході виконання дипломної роботи було проаналізовано захищеність розподіленої інформаційно-телекомунікаційної системи ТОВ «Весела торбинка» та зроблено висновок про її незахищеність, що підтверджує актуальність теми дипломної роботи.

Для розробки моделі кіберзахисту розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства ТОВ «Весела торбинка» було використано симулятор Cisco Packet Tracer. При проектуванні мережі акцент зроблено на використанні багатофункціональних пристроїв забезпечення безпеки Cisco ASA.

При створенні проекту розподіленої інформаційно-телекомунікаційної системи було здійснено основні налаштування пристроїв забезпечення безпеки Cisco ASA, а саме налаштування множини інтерфейсів, параметрів шифрування, списків контролю доступів та криптосхем. Для забезпечення шифрування даних, які передаються по міжмережевому протоколу IP, було здійснено налаштування засобів IPSec.

Запропонована модель кіберзахисту розподіленої інформаційно-комунікаційної системи торгівельного підприємства може бути реалізована в ТОВ «Весела торбинка».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Center for Internet Security – Cybersecurity Threats [Електронний ресурс] / Center for Internet Security – Режим доступу: https://www.cisecurity.org/cybersecurity-threats/

2. Аксьончиков С.О., Ємельянова І.В., Маркова К.Д., Сватовський І.І. Регресійний аналіз тенденцій розвитку кібератак. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління»*. 2017. Випуск 36. С. 5-13. URL: http://nbuv.gov.ua/j-pdf/VKhIMAM_2017_36_3.pdf.

3. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. *Реєстрація, зберігання і обробка даних*. 2015. Т.17. №2. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131565/04-Korpan.pdf?sequence=1.

4. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 19.04.2014 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 28.02.2020 р.).

5. Глоба Л.С. Розробка інформаційних ресурсів та систем : підручник. Київ : Політехніка, 2013. 380 с.

6. Домарев В.В. Защита информации и безопасность компьютерных систем. К. : Изд-во «ДиаСофт», 1999. 480 с.

7. Домарев В.В. Безопасность информационных технологий Методология создания систем защиты. К. : ООО «ТИД «ДС»», 2001. 688 с.

8. Информационные системы и технологии в экономике и управлении. ИНТУИТ. *Национальный открытый университет*. URL: https://www.intuit.ru/studies/courses/3627/869/lecture/31761 (дата звернення: 29.02.2020 р.).

9. Кузнецова М.Г. Застосування механізмів підвищення живучості для забезпечення захищеності інформаційного ресурсу в розподілених системах. *Реєстрація, зберігання і обробка даних*. 2006. Т.8. №3. С. 40-47. URL: http://dspace.nbuv.gov.ua/handle/123456789/50851.

10. Выбор политики защиты. Часть 1. URL: http://www.williamspublishing.com/PDF/5-8459-0387-4/part.pdf.

11. Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Бутузов В.М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посіб. / за заг ред. проф. Я. Ю. Кондратьева. Київ, 2004. 144 с.

12. Технології захисту інформації. Лекція 4. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.

13. Бакін Д.С. Проблеми захисту інформації в комп'ютерних мережах: матеріали всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листопада 2016 р. Кропивницький, 2016. С. 79-80. URL: http://dspace.kntu.kr.ua/jspui/ bitstream/123456789/5101/1/AUConferenceCyberSecurity_November2016_p79.pdf

14. Про основні засади забезпечення кібербезпеки України: Закон України від 08.07.2018 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.06.2020 р.).

15. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України: дис. ... канд. юр. наук : 12.00.07 / Сумський державний університет. Суми, 2018. 221 с.

16. Важинський С.Е. Щербак Т.І. Методика та організація наукових досліджень : навч. посіб. Суми : СумДПУ імені А.С. Макаренка, 2016. 260 с.

17. Cisco Packet Tracer. URL : https://www.cisco.com/c/ru_ua/training-events/netacad/training-courses/ciscopacket-tracer.html.

18. Киричек Г.Г., Скрупський С.Ю. Методичні вказівки до виконання лабораторних робіт з дисципліни «Комп'ютерні мережі». Моделювання мереж в середовищі Packet Tracer. Для студентів напряму підготовки 6.050102

«Комп'ютерна інженерія», усіх форм навчання. Частина 1. Запоріжжя : ЗНТУ, 2013. 378 с. URL: http://eir.zntu.edu.ua/bitstream/123456789/50/1/M04173.pdf.

19. Рвачова Н.В., Павліченко В.А. Програмні засоби для моделювання NGN мереж. *Проблеми інформатизації*: тези доп. четв. міжнар. наук.-техн. конф., Черкаси – Баку – Бельсько-Бяла – Полтава, 3-4 лист. 2016 р. Харків, 2016. С. 58.

20. Jozef Janitor, Karol Kniewald. Visual Learning Tools for Teaching / Learning Computer Networks : Sixth International Conference on Networking and Services, 2010. P. 351-355.

21. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network. URL : http://index-of.es/EBooks/German/Hacking/maximum_security.pdf.

22. Матов О.Я., Василенко В.С. Модель загроз у розподілених мережах. *Реєстрація, зберігання і обробка даних*. 2008. Т.10. №1. С. 91-102.

23. Костромин В. А. Кибератаки в подробностях: атаки с применением снифферов. URL : http://rus-linux.net/MyLDP/sec/cyber-attacks-network-sniffing.html (дата звернення: 15.06.2020 р.).

24. Угрозы безопасности сетевых информационных систем. Удаленное взаимодействие на сетевые информационные системы, их классификация. *ИНТУИТ. Национальный открытый университет*. URL : https://www.intuit.ru/studies/professional_skill_improvements/17834/courses/1300/lecture/25504?page=3 (дата звернення: 16.06.2020 р.).

25. Болехівський Н. Полотай О. Класифікація мережевих атак та методи протидії і ззахисту. URL : https://sci.ldubgd.edu.ua/bitstream/handle/123456789/6737/1.pdf?sequence=1&isAllowed=y (дата звернення: 16.06.2020 р.).

26. Социальная инженерия – как не стать жертвой. URL : https://efsol.ru/articles/social-engineering.html (дата звернення: 16.06.2020 р.).

27. Отличие межсетевого екрана от маршрутизатора (Firewall vs Router). URL : http://blog.netskills.ru/2014/03/firewall-vs-router.html (дата звернення: 16.06.2020 р.).

28. Cisco. URL : https://www.cisco.com/c/en/us/index.html (дата звернення: 17.06.2020 р.).