Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: «Комплексна модель захисту мережевої інфраструктури для організації підприємств»

Виконавець: студент IV курсу, групи КБ-43
_____ **Валерій ЛОСЄВ**
(підпис) (ім’я, прізвище)

	Підпис	**Ім’я ПРІЗВИЩЕ**
Керівник		Сергій ДАКОВ
Нормоконтроль		Олександр ТОРОШАНКО

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-43** (група) **Лосєву Валерію Андрійовичу** (прізвище ім’я по батькові)

Тема кваліфікаційної роботи Комплексна модель захисту мережевої інфраструктури для організації підприємств

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Топології та архітектури мережевих інфраструктур банківських установ, технології сегментації мережі (IP-сегментація, MAC-фільтрація), засоби. міжмережевого екранування та демілітаризовані зони (ДМЗ), системи виявлення та запобігання вторгненням (IDS/IPS), VPN-технології та шифрування трафіку, біометричні системи аутентифікації, антивірусні шифрування та аутентифікації, технології бездротового зв'язку та їх захист, рішення корпоративного рівня, методології підвищення обізнаності персоналу з кібербезпеки, архітектурна схема банківського відділення ПриватБанку №91, модель загроз і порушника інформаційної безпеки

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Аналіз сучасних методів захисту мережевої інфраструктури, дослідження Трирівневого підходу захисту (кінцеві пристрої, комутатори, маршрутизатори), оцінка ризиків та розробка моделі загроз і порушника інформаційної безпеки з побудовою матриць безпеки, проектування мережевої топології банківського відділення з IP-сегментацією, впровадження комплексної моделі захисту з технічними засобами (міжмережеві екрани, IDS/IPS, VPN, ДМЗ) та програмними рішеннями (антивірус, MAC-фільтрація, двофакторна аутентифікація), розробка програми підвищення обізнаності працівників, адаптація моделі захисту для різних галузей.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розробка комплексної моделі захисту мережевої інфраструктури , яка може бути адаптована для впровадження в організаціях різних підприємств.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав	_____	Сергій ДАКОВ
	(підпис)	(ім’я, прізвище)
Завдання прийняв до виконання	_____	Валерій ЛОСЄВ
	(підпис)	(ім’я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок – кінець)	Відмітка про виконання
1	Уточнення постановки задачі та аналіз вимог	29.11.2024 – 09.12.2024	виконано
2	Аналіз літератури з кібербезпеки банківських систем	10.12.2024 – 25.12.2024	виконано

3	Обґрунтування вибору рішень та технологій захисту	26.12.2024 – 05.01.2025	виконано
4	Вибір об'єкта дослідження та проектування базової інфраструктури	06.01.2025 – 25.01.2025	виконано
5	Дослідження засобів захисту мережевої інфраструктури за три рівневою інфраструктурою	26.01.2025 – 10.02.2025	виконано
6	Оцінка ризиків та розробка моделі загроз і порушника інформаційної безпеки	11.02.2025 – 28.02.2025	виконано
7	Проектування мережевої топології та IP-сегментація банківського відділення	01.03.2025 – 12.03.2025	виконано
8	Впровадження рішень захисту третього рівня (міжмережеві екрани, ДМЗ, IDS/IPS, VPN)	13.03.2025 – 28.03.2025	виконано
9	Впровадження рішень захисту другого рівня (MAC-фільтрація, політики контролю доступу)	29.03.2025 – 13.04.2025	виконано
10	Впровадження рішень захисту першого рівня (антивірус, біометрія, навчання персоналу)	14.04.2025 – 29.04.2025	Не виконано
11	Адаптація комплексної моделі захисту для різних галузей	30.04.2025 – 10.05.2025	виконано
12	Формування рекомендацій та оформлення пояснювальної записки	11.05.2025 – 28.05.2025	виконано

13	Підготовка до захисту кваліфікаційної роботи	29.05.2025 – 13.06.2025	виконано

Завдання видав _____ Сергій ДАКОВ
(підпис) (ім’я, прізвище)

Завдання прийняв до виконання _____ Валерій ЛОСЄВ
(підпис) (ім’я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 86 сторінок, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. Крім того, робота містить два додатки із загальною кількістю сторінок 18. У пояснювальній записці кваліфікаційної роботи міститься 66 рисунків і 26 таблиць.

Метою роботи є підвищення ефективності захисту мережевої інфраструктури підприємства шляхом впровадження і інтеграції сучасних технічних і програмних засобів захисту мережі.

Для досягнення зазначеної мети поставлено наступні завдання:

1. Проаналізувати сучасні засоби та методи забезпечення кібербезпеки мережевої інфраструктури.
2. Оцінити ризики та розробити моделі загроз інформаційної безпеки
3. Розробити комплексну модель захисту мережевої інфраструктури для організації підприємства

Об'єктом дослідження є процес захисту інформації в мережевих інфраструктурах підприємств.

Предметом дослідження є засоби та методи захисту мережевої інфраструктури організації на основі сучасних концепцій та технологій.

Практичною цінністю отриманих результатів є розробка комплексної моделі захисту мережевої інфраструктури з інтеграцією технічних та програмних засобів кібербезпеки, що дозволяє підвищити ефективність протидії сучасним кіберзагрозам у корпоративному середовищі.

Ключові слова: мережева інфраструктура, кібербезпека, міжмережеві екрани, системи виявлення вторгнень, SIEM, оцінка ризиків, модель загроз, сегментація мережі, захист банківських систем, комплексна модель захисту.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АПТ	–	Advanced Persistent Threat (прогресивні постійні загрози)
ДМЗ	–	Демілітарізована зона
ІТ	–	Інформаційні технології
ІТС	–	Інформаційно-телекомунікаційна система
MAC	–	Media Access Control (адреса управління доступом до середовища)
НБУ	–	Національний банк України
ОТ	–	Operational Technology (операційні технології)
ОС	–	Операційна система
ПЗ	–	Програмне забезпечення
ПК	–	Персональний комп’ютер
РП	–	Ранг пріоритету
США	–	Сполучені Штати Америки
AES	–	Advanced Encryption Standard (розширений стандарт шифрування)
API	–	Application Programming Interface (інтерфейс програмування додатків)
CIA	–	Confidentiality, Integrity, Availability (конфіденційність, цілісність, доступність)
DDoS	–	Distributed Denial of Service (розподілена атака відмови в обслуговуванні)
DHCP	–	Dynamic Host Configuration Protocol (протокол динамічної конфігурації хоста)
DICOM	–	Digital Imaging and Communications in Medicine (цифрова візуалізація та комунікації в медицині)
DLP	–	Data Loss Prevention (запобігання втраті даних)
DNS	–	Domain Name System (система доменних імен)
DNSSEC	–	Domain Name System Security Extensions (розширення безпеки системи доменних імен)
DoS	–	Denial of Service (відмова в обслуговуванні)
ESET	–	European Software & Engineering Team (європейська команда програмного забезпечення та інженерії)
FTP	–	File Transfer Protocol (протокол передачі файлів)
HIPAA	–	Health Insurance Portability and Accountability Act (акт портабельності та підзвітності медичного страхування)

HMI	–	Human Machine Interface (інтерфейс людина-машина)
HTTP	–	HyperText Transfer Protocol (протокол передачі гіпертексту)
IBM	–	International Business Machines (міжнародні бізнес-машини)
IDS	–	Intrusion Detection System (система виявлення вторгнень)
IKEv2	–	Internet Key Exchange version 2 (обмін ключами Інтернету версії 2)
IoT	–	Internet of Things (Інтернет речей)
IDS	–	Intrusion Detection System (Система виявлення вторгнень)
IP	–	Internet Protocol (Інтернет-протокол)
IPS	–	Intrusion Prevention System (система запобігання вторгненням)
MITM	–	Man-in-the-Middle (людина посередині)
NIST	–	National Institute of Standards and Technology (національний інститут стандартів і технологій)
PSK	–	Pre-Shared Key (попередньо розподілений ключ)
RCE	–	Remote Code Execution (віддалене виконання коду)
SCADA	–	Supervisory Control and Data Acquisition (диспетчерське управління та збір даних)
SELKS	–	Suricata, Elasticsearch, Logstash, Kibana, Scirius (інтегрований пакет безпеки)
SHA	–	Secure Hash Algorithm (алгоритм безпечного хешування)
SIEM	–	Security Information and Event Management (управління інформацією та подіями безпеки)
SIM	–	Subscriber Identity Module (модуль ідентифікації абонента)
SMS	–	Short Message Service (служба коротких повідомлень)
SSID	–	Service Set Identifier (ідентифікатор набору сервісів)
SSL	–	Secure Sockets Layer (рівень захищених сокетів)
TCP	–	Transmission Control Protocol (протокол управління передачею)
UDP	–	User Datagram Protocol (протокол користувацьких дейтаграм)
USB	–	Universal Serial Bus (універсальна послідовна шина)
VLAN	–	Virtual Local Area Network (віртуальна локальна мережа)
VPN	–	Virtual Private Network (віртуальна приватна мережа)
Wi-Fi	–	Wireless Fidelity (бездротова достовірність)

ВСТУП

Актуальність теми дослідження - розробка комплексної моделі захисту мережевої інфраструктури стає надзвичайно важливою у світлі постійної еволюції кіберзагроз та катастрофічного зростання кіберзлочинності. За даними Cybersecurity Ventures, глобальні збитки від кібератак зросли з 3 трлн доларів у 2015 році до прогнозованих 10,5 трлн доларів у 2025 році [1], що становить зростання на 350%. IBM Security повідомляє, що середня вартість порушення даних у 2024 році склала 4,88 млн доларів, при цьому час ідентифікації та локалізації інциденту становить у середньому 287 днів [2].

Сучасні хакерські атаки стають все більш винахідливими та складними, використовуючи штучний інтелект та автоматизовані інструменти. За звітом Check Point Research, у 2024 році спостерігалося зростання кібератак на 38% порівняно з попереднім роком, при цьому 74% організацій зазнали успішних фішингових атак [3]. Особливо тривожним є той факт, що 95% успішних атак на корпоративні мережі є результатом людської помилки [4], що підкреслює важливість комплексного підходу до кібербезпеки.

Зростання обсягу та значимості даних в сучасному бізнес-середовищі підсилює необхідність впровадження ефективних заходів захисту мереж. За дослідженням Statista, щоденно генерується 2,5 квінтільйона байт даних, а 90% світових даних було створено лише за останні два роки. Компрометація чи втрата таких обсягів інформації може призвести до серйозних фінансових втрат: за даними Ponemon Institute, 83% організацій зазнали більше ніж одного порушення даних, а середня вартість відновлення репутації становить 1,42 млн доларів.

Статистика кіберінцидентів демонструє критичну ситуацію в галузі інформаційної безпеки. За звітом Verizon Data Breach Investigations Report 2024, 68% порушень безпеки пов'язані з людським фактором, включаючи соціальну інженерію, помилки та зловживання привілеями. Крім того, 76% атак

спрямовані на отримання фінансової вигоди, а середній час між початком атаки та її виявленням становить 207 днів [5].

У контексті швидкого розвитку технологій та постійно мінливого ландшафту кіберзагроз, розробка комплексних моделей захисту стає критично важливою. За прогнозами Gartner, до 2025 року 99% вразливостей, які експлуатуються хакерами, будуть відомі організаціям щонайменше рік, що підкреслює важливість проактивного підходу до кібербезпеки. Водночас, лише 3% бюджету IT організацій витрачається на кібербезпеку, що є недостатнім для протидії сучасним загрозам.

Метою кваліфікаційної роботи є підвищення ефективності захисту мережевої інфраструктури підприємства шляхом розробки та впровадження комплексної моделі захисту, що інтегрує сучасні технічні і програмні засоби захисту мережі

Об’єкт дослідження – процес захисту інформації в мережевих інфраструктурах підриємств

Предмет дослідження – засоби та методи захисту мережевої інфраструктури організації на основі сучасних концепцій та технологій.

Завдання дослідження:

1. Огляд засобів та методів забезпечення кібербезпеки мережевої інфраструктури.
2. Оцінка ризиків та розробка моделі загроз/порушника інформаційної безпеки
3. Розробка комплексної моделі захисту мережевої інфраструктури для організації підприємств

РОЗДІЛ 1
АНАЛІЗ БАЗОВИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

1.1 Вибір об'єкта дослідження та проєктування базової інфраструктури як підґрунтя для визначення засобів кібербезпеки

У сучасних умовах стрімкого розвитку інформаційних технологій, питання захисту мережевої інфраструктури є пріоритетним для фінансових установ. Банківський сектор, як один із найвразливіших до кіберзагроз, потребує надійних, масштабованих і безпечних рішень для захисту власних інформаційних ресурсів та даних клієнтів.

Для реалізації практичного аспекту дипломної роботи було обрано банківську сферу як ключову галузь, що потребує високого рівня інформаційної безпеки. З огляду на рівень цифрової зрілості та активне впровадження інноваційних технологій, було вирішено обрати в якості прикладу саме ПриватБанк — лідера банківського ринку України, який відомий своїми розвиненими ІТ-рішеннями, масштабною мережею відділень та відкритістю до інновацій.

У межах дослідження об'єктом проектування обрано відділення №91 (Рис. 1.1), як один із типових філіалів банку. Для аналізу та моделювання було використано надану планувальну документацію приміщення, що включає зонування відділення, схему розміщення робочих місць, клієнтських зон, технічних і допоміжних приміщень.

Рисунок 1.1 Відділення ПриватБанк №91

Основною метою цього етапу є проєктування базової мережевої інфраструктури банківського відділення із урахуванням принципів інформаційної безпеки та вимог до надійності, відмовостійкості та масштабованості мережі.

Після визначення зонального планування та загальної інфраструктури приміщення банківського відділення №91 наступним кроком є облаштування робочих місць необхідним технічним обладнанням (Рис. 1.2). Це є базовою складовою етапу розгортання мережевої інфраструктури, оскільки саме на ці пристрої буде покладено щоденну взаємодію працівників з внутрішніми інформаційними системами банку, клієнтськими базами та мережевими ресурсами.

Враховуючи функціональні особливості кожної зони, а також специфіку роботи працівників, для оснащення було передбачено використання таких категорій техніки:

- Персональні комп’ютери (ПК): встановлюються у касовій зоні, кабінетах керівництва, залах обслуговування та технічних приміщеннях. ПК забезпечують стабільну продуктивність при тривалій роботі з банківськими системами, виконують функції обліку, обробки платежів, звітності тощо.

- Планшети: встановлюються у, залах обслуговування, для робити зклієнтами.
- Принтери: встановлюються централізовано у зручному доступі для декількох працівників одразу. Ці пристрої використовуються для друку, сканування та копіювання документів, а також для обробки клієнтських заявок.

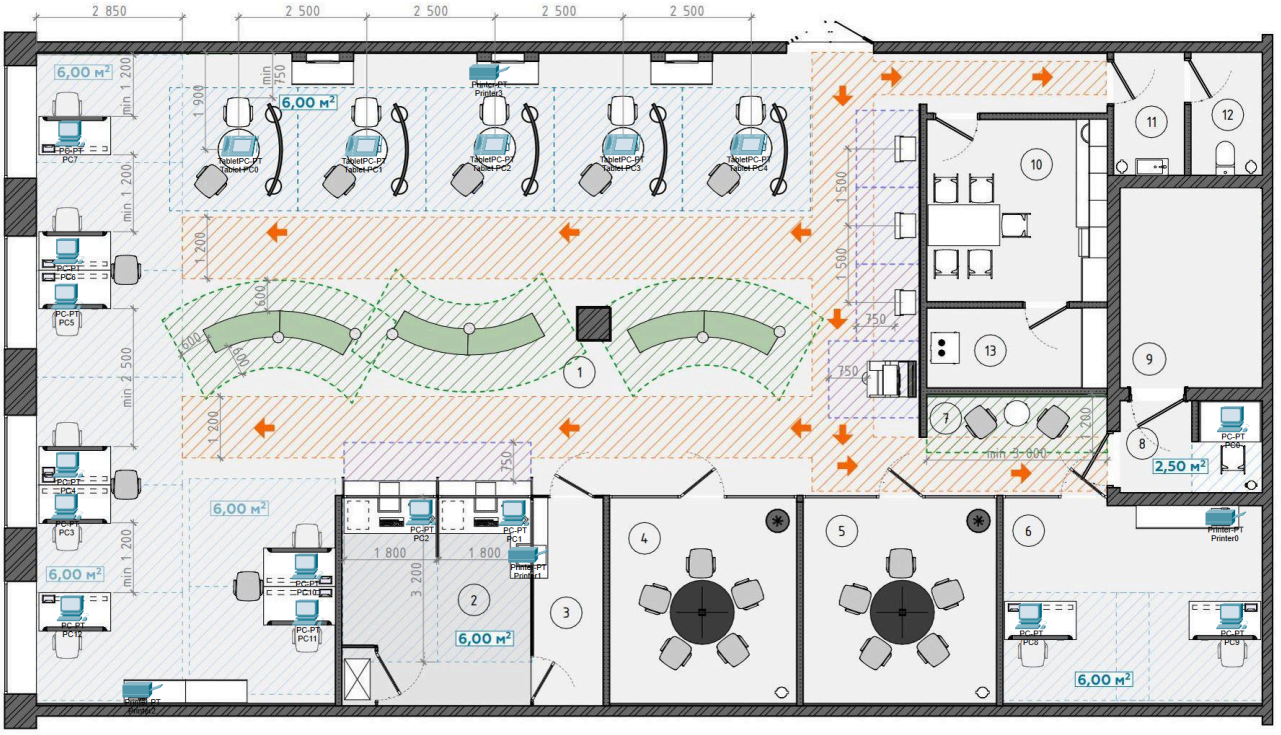

Рисунок 1.2 Облаштування робочих мість технічним обладнанням

У контексті побудови надійної та безпечної мережевої інфраструктури банківського відділення, ключове значення має впровадження спеціалізованого мережевого обладнання (Рис. 1.3), яке забезпечує основу для стабільної роботи всіх інформаційних систем. Саме цей етап проєктування є центральним для формування ефективної, масштабованої та захищеної IT-архітектури, яка відповідає сучасним вимогам фінансового сектору до захисту даних та безперебійності сервісів.

Ураховуючи критичну важливість безпеки комунікацій у банківському середовищі, на цьому етапі здійснюється детальне розміщення та конфігурація активного мережевого обладнання — маршрутизаторів, комутаторів, бездротових точок доступу, серверів і міжмережевих екранів. Кожен із цих

пристроїв виконує визначену функціональну роль у загальній інфраструктурі, забезпечуючи швидкість, контроль доступу, ізоляцію сегментів мережі, а також захист від потенційних загроз.

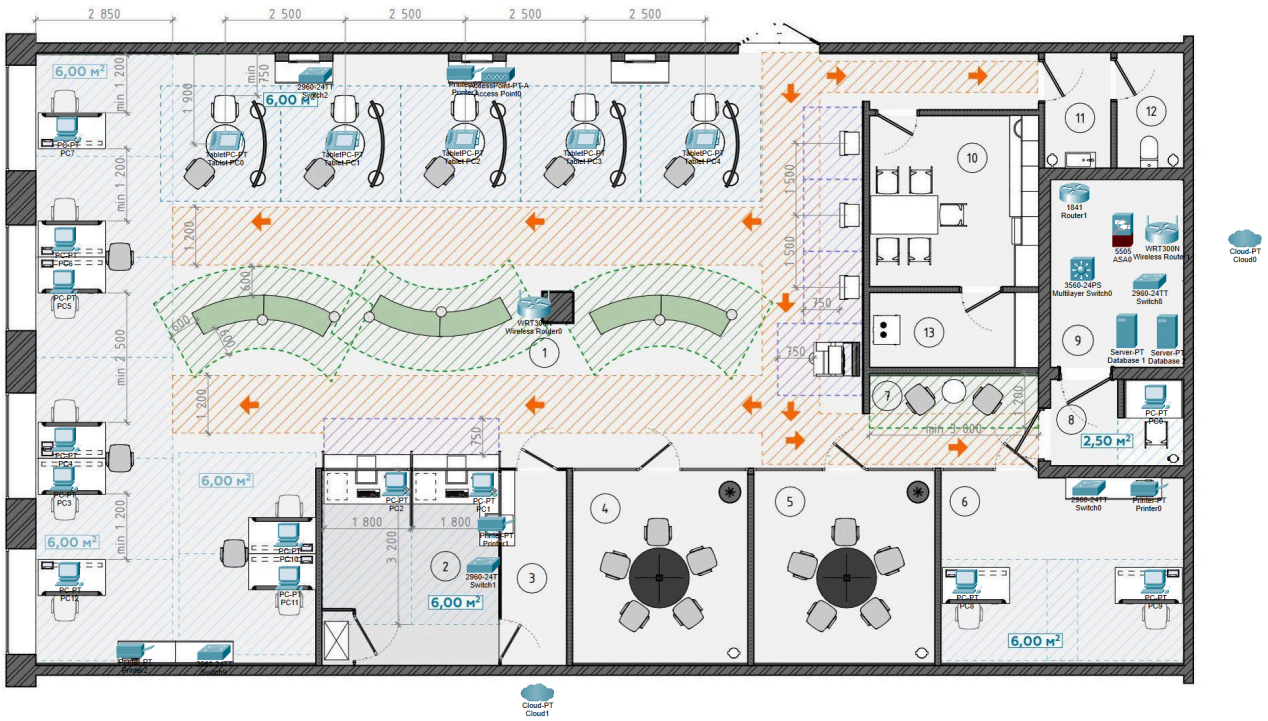

Рисунок 1.3 Втановлення спеціального мережевого обладнання

Ретельно продумана інтеграція цього обладнання у фізичний простір відділення дозволяє не лише оптимізувати топологію мережі, а й створити гнучке середовище для подальшого масштабування й адаптації до нових викликів кібербезпеки. Завдяки зонуванню приміщення, визначенню функціональних ролей робочих місць та відповідному підбору технічних засобів, формується технологічно збалансована система, здатна забезпечити високий рівень інформаційної безпеки та підтримати щоденну операційну діяльність банку на найвищому рівні.

Упровадження зазначеного мережевого обладнання створює фундамент для реалізації комплексної архітектури захищеного інформаційного середовища. З метою досягнення високого рівня функціональної стійкості та інформаційної безпеки, подальша увага буде зосереджена на розробці

структурної моделі мережі, впровадженні механізмів сегментування (VLAN), налаштуванні маршрутизації, фільтрації трафіку за допомогою брандмауерів, а також інтеграції систем централізованого моніторингу та контролю доступу.

Ці аспекти, які є критично важливими для забезпечення цілісності, доступності та конфіденційності даних у банківському середовищі, будуть детально розглянуті в наступних розділах дипломної роботи.

1.2 Визначення рішень для захисту мережевої інфраструктури першого рівня

Захист мереж у сучасних реаліях розвитку цифровізації, став невід’ємною частиною життя і кожного підприємства. Інструменти штучного інтелекту роблять загрози більш складними, що посилює нагальність проблеми. Зростання кіберзагроз спонукає організації інвестувати більше у свій захист. Будувати нові системи захисту, об’єднувати вже існуючі. Але немає такої системи, яку неможливо взламати. Тому і з розвитком технологій захисту в один крок ідуть технології, ідеї і підходи зламів і компрометації. За нинішніх темпів зростання збитки від кібератак становитимуть близько 10,5 трильйонів доларів щорічно до 2025 року, що на 300 відсотків більше, ніж у 2015 році [6].

Для уникнення наслідків треба розгорнути комплексний захист мережі. Для полегшення роботи і визначення можливих рішень захисту. Розіб’єм мережу на 3 рівня (Рис.1.4), до яких будемо застосовувати різні рішення захисту.

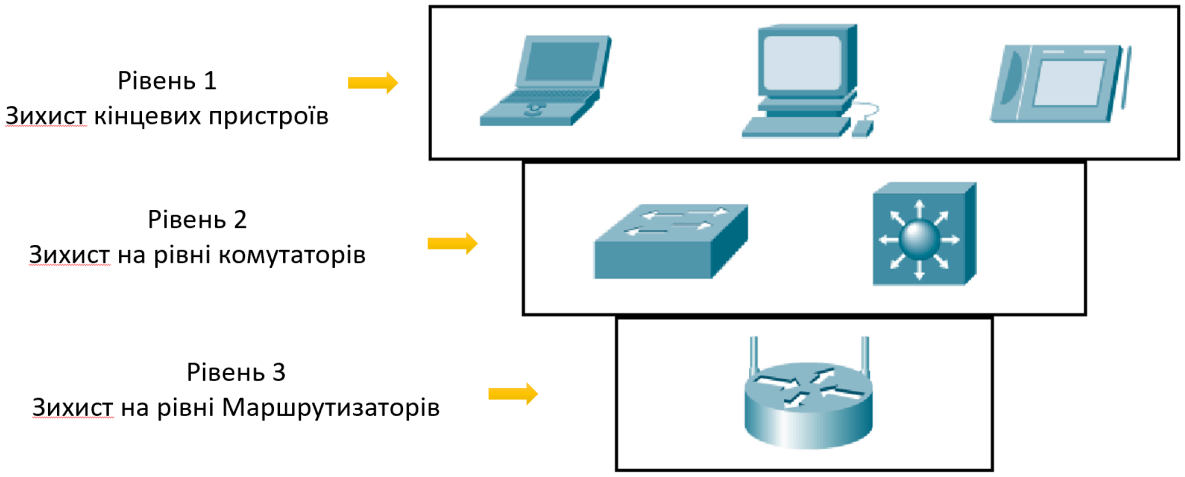

Рисунок 1.4 Захист мережі за 3-ма рівнями

Рівень 1 Представляє собою всі кінцеві пристрої, вони можуть включати комп’ютери, ноутбуки, телефони, планшети, тобто все, чим користуються користувачі системи. Для того щоб розібратись у методах захисту, треба визначити, що може загрожувати цим пристроям.

Одним із головних факторів небезпеки на рівні кінцевих пристроїв є фішинг та соціальна інженерія. Вплив на користувачів системи. Це кібератака, під час якої кіберзлочинці намагаються змусити жертву розкрити конфіденційну інформацію, видаючи себе за когось, ким вона не є, наприклад, за компанію чи члена сім'ї. Фішинг може здійснюватися через електронну пошту, текстові повідомлення та телефонні дзвінки , і спирається на методи соціальної інженерії [7], щоб психологічно маніпулювати жертвами та змусити їх передати свої дані.

Соціальна інженерія — це техніка психологічної маніпуляції, яку використовують зловмисники для здійснення різних атак. Атаки соціальної інженерії можуть відбуватися онлайн або особисто. Онлайн-атаки соціальної інженерії можуть мати форму фішингу, претексту та програмного забезпечення для залякування . Фізичні атаки соціальної інженерії можуть відбуватися, коли неавторизована особа маніпулює своїм шляхом до обмеженої зони, іноді

видаючи себе за водія доставки або працівника прибиральника. Соціальна інженерія спирається на людські помилки або слабкі місця, а не на вразливості системи чи пристрою.

Так як це є просто психологічним впливом на людину, необхідно впровадити програми підвищення рівня обізнаності працівників. Щоб створити стійку культуру безпеки в організації, знизити ризики, пов’язані з людським фактором.

Не менш значущим може бути завдання шкоди кінцевим пристроям користувачів за допомогою шкідливого програмного забезпечення. У їх перелік можуть входити трояни, шпигунські програми, хробаки, і тому подібне, загалом кажучи віруси. Зараження можуть бути викликані різними способами, скачуванням файлів через інтернет, переходом за шкідливими посиланнями відправленими на mail, або ж вставивши заражений USB накопичувач у комп’ютер.

Антивірус, є прекрасним рішення захисту від загроз цього типу. Бо антивіруснуні ПЗ мають на меті виявлення та видалення комп’ютерних вірусів і інших шкідливих програм. Антивірусне програмне забезпечення зазвичай працює за одним із двох принципів: воно або сканує програми та файли, коли вони потрапляють на ваш пристрій, і порівнює їх з відомими вірусами назвати цей принцип можна назвати реактивним захистом, або сканує програми, які вже є на вашому пристрої, шукаючи будь-яку підозрілу поведінку [8], який можна назвати проактивним захистом.

Windows має вбудоване рішення, яке називається Windows Defender, це потужне рішення, яке включає як реактивний захист так і проактивний захист. Але цього рішення, за умови роботи підприємства, яке працює з конфіденційними даними, не достатньо. Відповідні причини - це недостатній рівень захисту, бо вбудоване рішення може пропустити складні цільові атаки, відсутність детального моніторингу а також обмежені можливості швидкого реагування на загрози.

Саме тому варто використовувати професійні, корпоративні антивірусні програмні забезпечення.

Однак загрози першого рівня не обмежуються віртуальними атаками. Серйозну небезпеку може також становити фізичний доступ до обладнання працівників. Ця загроза інформації розкривається тріадою CIA. Загрозою цілісності, доступності і конфіденційності даних. Відповідно отримавши фізичний доступ до обладнання зловмисник може підмінити інформацію, зашифрувати данні після, шантажуючи користувача, або ж скомпрометувавши конфіденційну інформації і знову ж шантажуючи або продаючи ці дані зацікавленим особам.

Рішення по захисту буде доволі просте, використовувати двофакторну аутентифікацію, одним фактором з яких буде біометричний захист. Тобто в комплексі використовувати пароль для входу в систему і якусь унікальну фізіологічну характеристику. Ці технології, такі як сканування відбитків пальців, розпізнавання голосу та обличчя, а також аналіз геометрії руки, стали доступними для широкого застосування[18], що відкриває нові можливості для забезпечення безпеки інформації у різних галузях. Найпоширенішим і найдешевшим з рішень є відбиток пальця. Що забезпечить легкість доступу і гарний рівень захисту.

1.3 Визначення рішень для захисту мережевої інфраструктури другого рівня

Рівень 2 представляє собою захист на рівні комутаторів та мережевої інфраструктури, підтримує з’єднання пристроїв дротами, та їх правильну взаємодію.

Уявимо собі ситуацію, підключення неавторизованого користувача до системи як фізично через порт до комутаторів так і віддалено. Шлях його запитів буде направлений до пристроїв директорів, або ж серверів. Ми

зацікавлені у тому, щоб зупинити цей доступ саме в таких випадках і з'являється у нагоді MAC-фільтрація, яка створює початковий рівень контролю, дозволяючи доступ до мережі лише пристроям з попередньо зареєстрованими MAC-адресами. При спробі підключення неавторизованого пристрою комутатор автоматично блокує з'єднання на рівні порту, не дозволяючи зловмиснику навіть отримати IP-адресу в мережі. На відміну від IP-фільтрації, у якій компонент системи може отримати той самий IP адрес, що і мережевий пристрій, який вже містить доступ, кожен компонент системи, має свій унікальний індифікатор, який складається з 16 знаків і у які можуть входити як англійські літери так і цифри.

Для реалізації ефективної MAC-фільтрації необхідно додати у невеличкому сегменті мережі, який охоплюється комутатором, правила пропуску пристроїв, MAC адреси яких ми беремо завчасно. Простіше кажучи, за портом 1, пропускаємо саме цей пристрій, за іншими не пропускаємо взагалі. Ці провила прописуються на самих комутаторах. Але треба зауважити, що ця база повинна регулярно оновлюватися при додаванні нового обладнання або виведенні застарілого з експлуатації.

Для прикладу відтворемо невеличку мережу, у якій знаходяться 2 комп’ютери 1 комутатор і 1 роутер. На комутатор прописуємо, що мають дозвіл проходження PC0 і PC1, за їх MAC адресами до відповідних портів 1 і 2. І відтворюємо маршрутизацію пакетів (Рис.1.5). Отримуємо успіх.

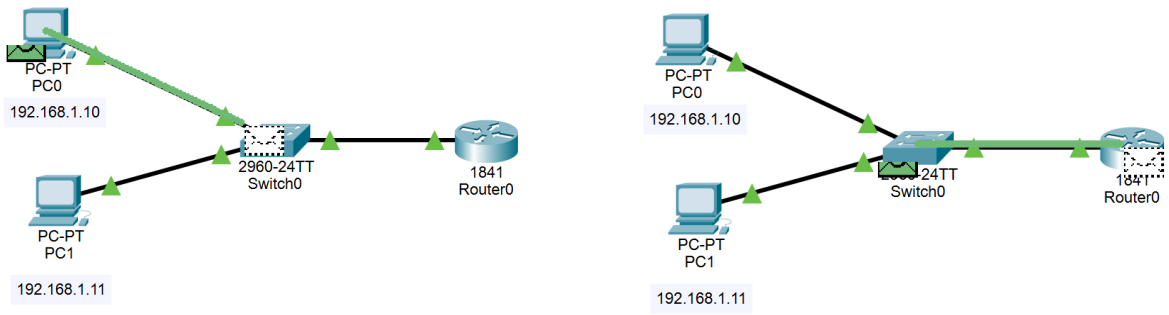

Рисунок 1.5 Перевірка маршрутизації пакетів

Для перевірки роботи фільтрації додаємо новий комп’ютер, ставимо той самий IP і підключемо до першого порта. Перевіримо маршрутизацію (Рис 1.6).

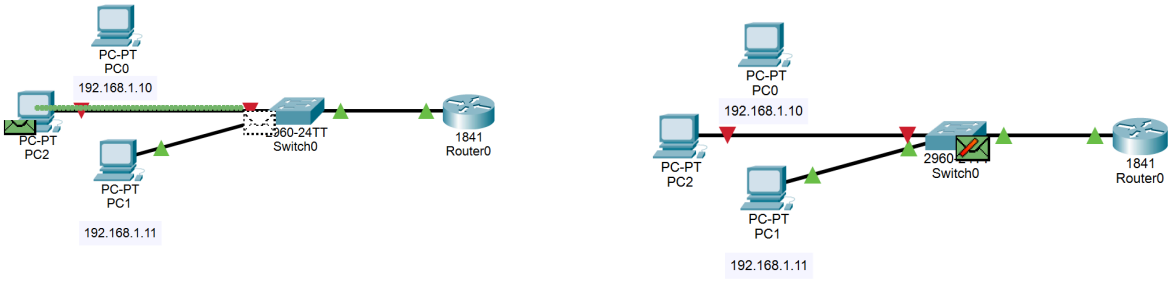

Рисунок 1.6 Перевірка роботи фільтрації

Як бачимо інший комп’ютер з тією ж IP адресою не приймає.

Сегментація мережі — це фундаментальна стратегія мережевої безпеки, яка передбачає поділ більшої мережі на менші підмережі або сегменти. Кожен сегмент функціонує як ізольована сутність із власним набором елементів керування та політик безпеки [9], створюючи межі, що обмежують здатність загроз поширюватися в мережі. Цього можна досягти як за допомогою фізичної сегментації, де використовуються окремі мережеві пристрої та обладнання, так і віртуальної сегментації, яка використовує віртуалізацію мережі для досягнення того ж ефекту.

Сегментація мережі відіграє ключову роль у мінімізації масштабів кібератаки шляхом зменшення поверхні атаки. Розділивши мережу на менші сегменти, кожен з яких має власні виділені ресурси та засоби контролю безпеки, потенційний вплив та масштаби кібератаки значно зменшуються.

Коли зловмисник отримує несанкціонований доступ до сегмента, сегментація мережі гарантує, що його діяльність залишається ізольованою в межах цього конкретного сегмента. Така ізоляція запобігає поширенню атаки на інші сегменти або критичні системи в мережі. В результаті, здатність зловмисника переміщатися по мережі вбік, мінімізуючи загальну шкоду, яку він може завдати.

Ізолюючи атаку в межах одного сегмента, сегментація мережі ефективно зменшує поверхню атаки. Замість того, щоб усю мережу піддавали кібератаці, скомпрометовано лише певний сегмент. Це значно звужує масштаб атаки, що полегшує мережевим адміністраторам стримування, розслідування та пом'якшення наслідків інциденту.

Крім того, сегментація мережі значною мірою сприяє легшому усуненню несправностей та їх обслуговуванню. Розділивши мережу на менші сегменти, мережеві адміністратори можуть ізолювати певні області та легко виявляти й усувати проблеми, які можуть виникнути. Коли виникає проблема в мережі, її можна локалізувати в конкретному сегменті, де вона виникає, що зменшує обсяг зусиль з усунення несправностей. Такий цілеспрямований підхід економить час і ресурси, дозволяючи швидше вирішувати проблеми з мережею.

Сегментація мережі також є вирішальною стратегією для підвищення загальної продуктивності мережі. Розділяючи більшу мережу на підмережі або сегменти, організації можуть ефективно зменшити перевантаження мережі та контролювати потік трафіку. Ця політика сегментації допомагає гарантувати, що кожен сегмент відповідає за певний набір завдань, запобігаючи перевантаженню та забезпечуючи плавнішу передачу даних.

1.4 Визначення рішень для захисту мережевої інфраструктури третього рівня

Рівень 3 представляє собою захист на рівні маршрутизаторів. Тобто обміну даними між різними мережами, а також при надходженні інформації з інтернету.

На цьому рівні організації стикаються з різноманітними загрозами: несанкціонованими мережевими з'єднаннями з зовнішніх джерел, DDoS атаками через перевантаження каналів зв'язку, прямими атаками на внутрішню

мережу через публічні сервіси, зараженням систем вірусами з зовнішніх джерел та перехопленням трафіку в незахищених мережах.

Для протидії цим загрозам на третьому рівні застосовується спеціалізовані засоби захисту.

Брандмауери виконують роль першої лінії оборони, фільтруючи вхідний та вихідний трафік за допомогою попередньо визначених правил та політик [10], які дозволяють або забороняють передачу даних. Вони ефективно блокують несанкціоновані з'єднання з зовнішніх джерел та обмежують DDoS атаки шляхом контролю кількості одночасних підключень.

ДМЗ (Демілітаризована зона) створює буферну зону між публічним інтернетом та локальною мережею [11], забезпечуючи додатковий рівень безпеки між довіреними та недовіреними мережами. Розміщення публічних сервісів у ДМЗ запобігає прямим атакам на внутрішню мережу навіть у випадку компрометації зовнішньо доступних ресурсів.

Системи запобігання вторгненням (IPS) відстежують мережевий трафік у реальному часі на наявність шкідливої активності та можуть автоматично блокувати або відкидати підозрілий трафік, захищаючи від зараження вірусами та експлуатації вразливостей.

Системи виявлення вторгнень (IDS) доповнюють IPS, виявляючи шкідливу активність та створюючи детальні звіти для подальшого аналізу інцидентів безпеки. Віртуальні приватні мережі

(VPN) забезпечують захищене з'єднання між кінцевими точками через додатковий рівень шифрування, що гарантує захист від перехоплення трафіку в незахищених мережах та атак типу "людина посередині".

Висновки за розділом №1

У першому розділі проведено комплексний аналіз сучасних засобів та методів забезпечення кібербезпеки мережевої інфраструктури підприємств на прикладі банківського сектору.

Обрано об'єкт дослідження — відділення ПриватБанку №91 як типовий приклад банківської установи з розвиненою ІТ-інфраструктурою. Здійснено детальне планування базової мережевої архітектури з урахуванням зонального розподілу приміщень, функціональних особливостей робочих місць та специфіки банківської діяльності. Розроблено схему розміщення технічного обладнання, що включає персональні комп'ютери, планшети, принтери та спеціалізоване мережеве обладнання (маршрутизатори, комутатори, сервери, міжмережеві екрани).

Систематизовано сучасні підходи до захисту мережевої інфраструктури за трирівневою моделлю безпеки. На першому рівні (кінцеві пристрої) ідентифіковано основні загрози: фішинг, соціальна інженерія, шкідливе програмне забезпечення та фізичний несанкціонований доступ. Визначено відповідні засоби протидії: програми підвищення кібер-обізнаності персоналу, корпоративні антивірусні рішення та двофакторна аутентифікація з біометричним захистом.

На другому рівні (комутатори та мережева інфраструктура) досліджено методи MAC-фільтрації та сегментації мережі. Обґрунтовано ефективність MAC-фільтрації для запобігання підключенню неавторизованих пристроїв через контроль унікальних ідентифікаторів обладнання. Проаналізовано переваги мережевої сегментації для мінімізації масштабів кібератак, покращення продуктивності та спрощення адміністрування.

На третьому рівні (маршрутизатори та міжмережевий обмін) досліджено засоби захисту від зовнішніх загроз. Визначено роль брандмауерів як першої лінії оборони для фільтрації трафіку за попередньо визначеними правилами. Обґрунтовано необхідність створення демілітаризованої зони (ДМЗ) для ізоляції публічних сервісів від внутрішньої мережі. Проаналізовано важливість

систем виявлення (IDS) та запобігання вторгненням (IPS) для моніторингу та блокування шкідливої активності в реальному часі.

Результати першого розділу створюють теоретичне підґрунтя для подальшої розробки методології оцінки ризиків та практичного впровадження комплексної моделі захисту мережевої інфраструктури банківської установи з урахуванням сучасних викликів інформаційної безпеки.

РОЗДІЛ 2
ОЦІНКА РИЗИКІВ ТА РОЗРОБКА МОДЕЛІ ЗАГРОЗ І ПОРУШНИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Визначення активів захисту потенційних уразливостей та загроз

Порушення основних властивостей інформації може становити серйозну загрозу для сучасних організацій. Інформація набуває складнішого контролю та стає більш схильною до різноманітних загроз і вразливостей, таких як комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, пожежа або повінь. Також варто зауважити, що інформаційні ресурси мають свою вартість і цінність, як матеріальні активи. Оцінка ризиків є ключовою складовою процесу забезпечення інформаційної безпеки [12], оскільки вона дозволяє визначити масштаби загроз та ймовірність їх реалізації.

У зв'язку з цим, важливо мати на увазі поняття ризику інформаційної безпеки, яке описує потенційну можливість використання вразливостей інформаційного активу або групи активів для завдання шкоди об'єктам або інтересам суб'єктів інформаційних відносин (Рис. 2.1). Отже, для проведення аналізу ризиків потрібні наступні дані про інформаційну систему: перелік цінної інформації з визначенням рівня критичності, відомості про уразливість інформаційної системи і загрози, які можуть на неї вплинути.

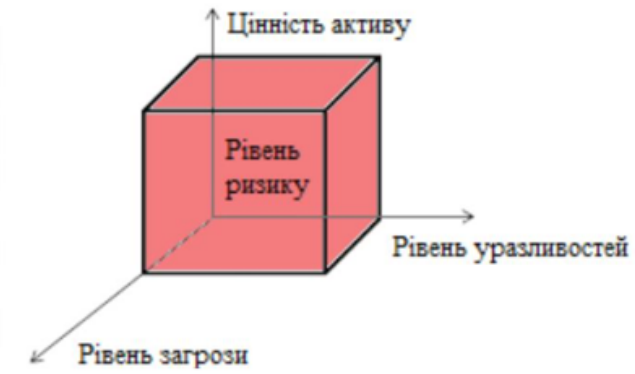

Рисунок 2.1 Рівень ризику

Варто відзначити, що навіть найбільш ретельно розроблена політика безпеки чи найсучасніший брандмауер не можуть гарантувати повного захисту від потенційно шкідливих подій у сфері інформаційної безпеки. Складність та різноманітність сучасного інформаційного середовища призводять до існування залишкових ризиків, незалежно від якості заходів безпеки, що були впроваджені. Крім того, завжди існує ймовірність з'явлення нових, дотепер невідомих загроз інформаційній безпеці. Недостатня готовність організації до реагування на подібні ситуації може значно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки. Ось чому так важливо проводити аналіз та оцінку ризиків інформаційної безпеки.

Формуємо список основних інформаційних активів банку і одразу ділимо їх на дві групи:

- Дані:
  - Фінансові дані
  - Персональні дані клієнтів
  - Внутрішні операційні дані
  - Юридична документація
  - Резервні копії даних
  - Документація з кібербезпеки
  - Аналітичні дані та звіти
  - Дані про партнерів та постачальників
- Обладнання:
  - Веб-ресурси та онлайн-платформи
  - IT-інфраструктура

Обґрунтування інформаційних активів:

Фінансові дані є основою банківської діяльності, оскільки вони відображають фінансовий стан клієнтів та операції банку. Вони дозволяють

здійснювати бухгалтерський облік, управління ризиками та фінансовий аналіз, що є критично важливим для прийняття обґрунтованих рішень.

Банки обробляють велику кількість особистої інформації для ідентифікації клієнтів та надання їм послуг. Ці дані допомагають у забезпеченні безпеки транзакцій, дотриманні регуляторних вимог та наданні персоналізованих банківських послуг.

Внутрішні операційні дані відображають внутрішню діяльність банку, включаючи управління персоналом та адміністративні процеси. Вони забезпечують ефективне управління банком та підтримують внутрішню безпеку.

Юридична документація включає договори, нормативні документи та ліцензії. Вона забезпечує юридичну відповідність, регулює відносини з клієнтами та партнерами і захищає банк від правових ризиків.

Резервні копії даних створюються для захисту від втрати інформації внаслідок збоїв або кібератак. Вони дозволяють відновити критично важливі дані, забезпечуючи безперервність бізнес-процесів банку.

Документація з кібербезпеки містить політики, процедури та інструкції з захисту інформаційних активів. Вона захищає банк від кіберзагроз, забезпечуючи безпеку даних та дотримання стандартів безпеки.

Аналітичні дані та звіти включають ринкову аналітику, фінансові звіти та прогнози. Вони допомагають у прийнятті стратегічних рішень, плануванні та аналізі діяльності банку.

Дані про партнерів та постачальників містять інформацію про контракти, угоди та умови співпраці. Вони важливі для управління відносинами з постачальниками та забезпечення безперебійного постачання послуг і товарів.

Дані про IT-інфраструктуру включають конфігурації серверів, мережевого обладнання та програмного забезпечення. Вони забезпечують стабільну та безперебійну роботу всіх IT-систем банку.

Веб-ресурси та онлайн-платформи включають дані про інтернет-банкінг, мобільні додатки та інші онлайн-сервіси. Вони надають клієнтам зручний доступ до банківських послуг та підвищують ефективність обслуговування.

Ймовірні уразливості:

- Фізична безпека
- База даних
- Помилки співробітників
- Веб-сервер
- Передача даних та лінії зв’язку
- ПК співробітників компанії
- Обчислювальний сервер

Обґрунтування ймовірних уразливостей:

Фізична безпека є критично важливою для захисту обладнання, документів та інших цінних ресурсів банку. Забезпечення адекватної фізичної безпеки допомагає запобігти крадіжкам, втраті або пошкодженню обладнання та документів, а також забезпечує конфіденційність інформації.

База даних містить важливу і конфіденційну інформацію про клієнтів, транзакції та фінансові операції банку. Її належне управління та захист дозволяє банку зберігати, оновлювати та аналізувати великий обсяг інформації, необхідної для проведення банківських операцій та прийняття стратегічних рішень.

Помилки співробітників можуть призвести до витоку конфіденційної інформації, недоступності послуг або інших проблем безпеки. Виявлення та усунення помилок допомагає забезпечити безпеку банку та зменшити ризики фінансових втрат та порушень безпеки.

Веб-сервер використовується для надання онлайн-сервісів клієнтам, таких як інтернет-банкінг та доступ до банківського веб-сайту. Правильна конфігурація та захист веб-сервера допомагає забезпечити безпеку та доступність онлайн-сервісів банку для клієнтів.

Лінії зв’язку та мережеві канали використовуються для передачі конфіденційної інформації між відділеннями банку та зовнішніми системами. Забезпечення безпеки та надійності цих каналів допомагає запобігти перехопленню, зміні або витоку конфіденційної інформації.

Комп’ютери співробітників використовуються для роботи з конфіденційною інформацією банку та доступу до банківських систем. Захист ПК співробітників від малвари та несанкціонованого доступу допомагає запобігти витоку конфіденційної інформації та забезпечити безпеку внутрішніх систем банку.

Загрози:

- Відмова в обслуговуванні (DoS)
- Шкідливе ПЗ
- Помилки користувача
- Спам
- «Фішинг»
- Ворожий агент

Засоби контролю:

- Система виявлення вторгнень (IDS)
- Навчання персоналу
- Міжмережеві екрани
- Політика безпеки
- Конфігурація архітектури мережі
- Демілітаризована зона (ДМЗ)
- Контроль території

Обґрунтування засобів контролю:

IDS виявляє потенційні загрози та сповіщає про можливі вторгнення, що дозволяє оперативно реагувати на кібератаки та запобігати шкоді банку.

Навчені працівники з кібербезпеки збільшують загальну обізнаність з потенційними загрозами та допомагають зменшити ризики безпеки шляхом своєчасного виявлення та реагування на інциденти.

Міжмережеві екрани фільтрують трафік мережі, захищаючи внутрішню мережу банку від зовнішніх атак та забезпечуючи безпеку та конфіденційність даних.

Ефективна політика безпеки встановлює правила та процедури для захисту інформації та систем банку, забезпечуючи відповідність законодавству та захищаючи конфіденційність клієнтів.

Вірно сконфігурована мережева архітектура зменшує ризики атак та забезпечує безпеку та ефективність обміну даними всередині банку та зовні.

ДМЗ встановлюється як зона, що розташована поза внутрішньою мережею банку, контролюючи доступ до важливих ресурсів та захищаючи внутрішні системи від зовнішніх атак.

Ефективний контроль території забезпечує фізичний захист приміщень та обладнання банку, запобігаючи несанкціонованому доступу та забезпечуючи безпеку активів.

Побудова матриць (матриця уразливостей (Таб 2.1), матриця загроз (Таб 2.2) та матриця контролю (Таб 2.3)).

Таблиця №2.1

Матриця уразливостей

Матриця уразливостей Шкала взаємозв'язку Немає Слабкий Помірний Сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 - критичний	**Активи:**	Фінансові дані	Персональні дані клієнтів	Внутрішні операційні дані	Юридична документація	Резервні копії даних	Документація з кібербезпеки	Аналітичні дані та звіти	Дані про партнерів та постачальників	Веб-ресурси та онлайн-платформи	IT-інфраструктура
1	2	3	4	5	6	7	8	9	10	11	12
Уразливості:	РП	4	5	3	3	5	5	4	2	4	5
Фізична безпека	4	7	9	1	9	6	9	9	9	0	8
База даних	5	5	9	3	0	2	6	6	7	4	8

Продовження табл. 2.1

1	2	3	4	5	6	7	8	9	10	11	12
Помилки співробітників	5	3	6	3	3	8	6	3	5	1	6
Веб-сервер	4	4	7	9	6	9	6	4	9	9	9
Передача даних та лінії зв'язку	3	2	4	2	3	1	2	3	7	0	1

ПК співробітників компанії	4	0	3	6	1	3	6	2	8	1	4
Обчислювальний сервер	3	0	0	3	0	9	6	9	0	3	8

Таблиця №2.2

Матриця загроз

Матриця загроз Шкала взаємозв'язку Немає Слабкий Помірний Сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 - критичний	**Уразливості:**	Фізична безпека	База даних	Помилки співробітників	Веб-сервер	Передача даних та лінії зв'язку	ПК співробітників компанії	Обчислювальний сервер
Загрози:	РП	4	5	5	4	3	4	3
Відмова в обслуговуванні (DoS)	4	0	2	0	9	0	7	9
Шкідливе ПЗ	3	0	8	8	6	0	9	5
Помилки користувача	2	0	0	0	7	9	1	7
Спам	4	0	1	0	0	0	9	3
«Фішинг»	5	0	3	9	0	0	9	4
Ворожий агент	5	9	9	5	8	5	8	7

Таблиця №2.3

Матриця контролю

Матриця контролю Шкала взаємозв'язку Немає Слабкий Помірний Сильний 0 1 3 9 Ранг пріоритету (РП) 1 – незначний 2 – невеликий 3 – середній 4 – серйозний 5 - критичний	**Загрози:**	Відмова в обслуговуванні (DoS)	Шкідливе ПЗ	Помилки користувача	Спам	«Фішинг»	Ворожий агент
Засоби контролю:	РП	4	3	2	4	5	5
Система виявлення вторгнень	5	5	9	1	0	0	5
Навчання персоналу	5	4	7	8	9	9	7
Міжмережеві екрани	4	9	6	2	6	2	1
Політика безпеки	4	1	9	6	8	9	8
Конфігурація архітектури м.	3	6	8	2	2	0	7
Демілітаризована зона (ДМЗ)	3	2	7	3	7	6	5
Контроль території	3	0	5	0	0	0	9

2.2 Модель загроз

На основі проведеного аналізу активів та уразливостей мережевої інфраструктури банківського відділення виникає необхідність розробки детальної моделі загроз інформаційної безпеки. Ця модель є критично важливою для розуміння повного спектру ризиків, з якими може зіткнутися банківська установа в процесі своєї діяльності.

Модель загроз включає систематизацію потенційних атак за різними критеріями: від джерела походження (людський фактор, технічні засоби, стихійні явища) до способу впливу на інформаційні системи. Особлива увага приділяється специфічним загрозам банківського сектору, включаючи мережеві атаки, загрози прикладного програмного забезпечення та операційних систем.

Детальний опис моделі загроз та порушника (див. Додаток А).

2.2 Модель порушника

А також є необхідність розробки детальної моделі порушника інформаційної безпеки. Модель порушника деталізує можливості та характеристики потенційних атакуючих, враховуючи як внутрішні загрози (співробітники різних рівнів доступу), так і зовнішні (професійні кіберзлочинці, конкуренти, випадкові порушники). Кожна категорія порушників аналізується з точки зору їх технічних можливостей, методів дії, тривалості атак та місця їх здійснення.

Детальний опис моделі загроз та порушника (див. Додаток Б).

Висновки за розділом №2

У другому розділі проведено комплексну оцінку ризиків та розроблено модель загроз і порушників інформаційної безпеки для мережевої інфраструктури банківського відділення.

Здійснено систематизацію інформаційних активів банку за двома основними категоріями: дані (10 типів, включаючи фінансові дані, персональні дані клієнтів, внутрішні операційні дані, юридичну документацію, резервні копії та документацію з кібербезпеки) та обладнання (веб-ресурси та IT-інфраструктура). Для кожного активу визначено рівень критичності від 2 до 5 балів, що дозволило встановити пріоритетність заходів захисту.

Ідентифіковано сім ключових категорій уразливостей мережевої інфраструктури: фізична безпека, база даних, помилки співробітників, веб-сервер, передача даних та лінії зв'язку, ПК співробітників і обчислювальний сервер. Визначено шість основних типів загроз (DoS-атаки, шкідливе ПЗ, помилки користувачів, спам, фішинг, ворожі агенти) та сім засобів контролю (IDS, навчання персоналу, міжмережеві екрани, політика безпеки, конфігурація архітектури, ДМЗ, контроль території).

Побудовано три взаємопов'язані матриці безпеки з використанням 4-бальної шкали взаємозв'язку (0-1-3-9), що забезпечило кількісну оцінку ступеня впливу кожної загрози на конкретні активи та ефективність засобів контролю. Матриці дозволили виявити найкритичніші точки ризику та оптимізувати розподіл ресурсів на захист.

Розроблено багаторівневу модель загроз, структуровану за чотирма категоріями: загальні загрози (6 типів), мережеві загрози (5 типів), загрози прикладного програмного забезпечення (3 типи) та загрози операційних систем (4 типи). Кожна загроза класифікована за типом впливу згідно з тріадою CIA: порушення конфіденційності (К), цілісності (Ц), доступності (Д) та втрата спостереженості (С).

Створено детальну модель порушника, що включає класифікацію 8 функціональних ділянок банку, 4 форми представлення інформації та 16 категорій потенційних порушників. Модель охоплює як внутрішні загрози (9 категорій: від касирів до віддалених працівників), так і зовнішні (7 категорій: від конкурентів до незадоволених клієнтів), з деталізацією їх можливостей, методів дії (7 типів), часових рамок (3 періоди) та місця здійснення атак (3 локації).

Запропоновано науково обґрунтовану методику оцінки ризиків на основі матричного аналізу взаємозв'язків "актив-уразливість-загроза-контроль", що дозволяє здійснювати кількісну оцінку рівня ризику та ефективності заходів захисту.

Результати дослідження формують комплексну теоретичну базу для проектування та впровадження технічних і організаційних засобів захисту мережевої інфраструктури банківської установи з урахуванням реальних загроз, специфіки діяльності та обмежених ресурсів на забезпечення кібербезпеки.

РОЗДІЛ 3
РОЗРОБКА КОМПЛЕКСНОЇ МОДЕЛІ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ДЛЯ ОРГАНІЗАЦІЇ ПІДПРИЄМСТВ

3.1 Проектування мережевої топології та IP-сегментація банківського відділення

Для детального аналізу та демонстрації засобів захисту було взято розроблену у попередніх розділах схему банківського відділення ПриватБанку №91 з розміщенням технічного обладнання по зонах. З цієї архітектурної схеми було вилучено план приміщення та створено мережеву топологію (Рис. 3.1), залишено лише мережеву інфраструктуру.

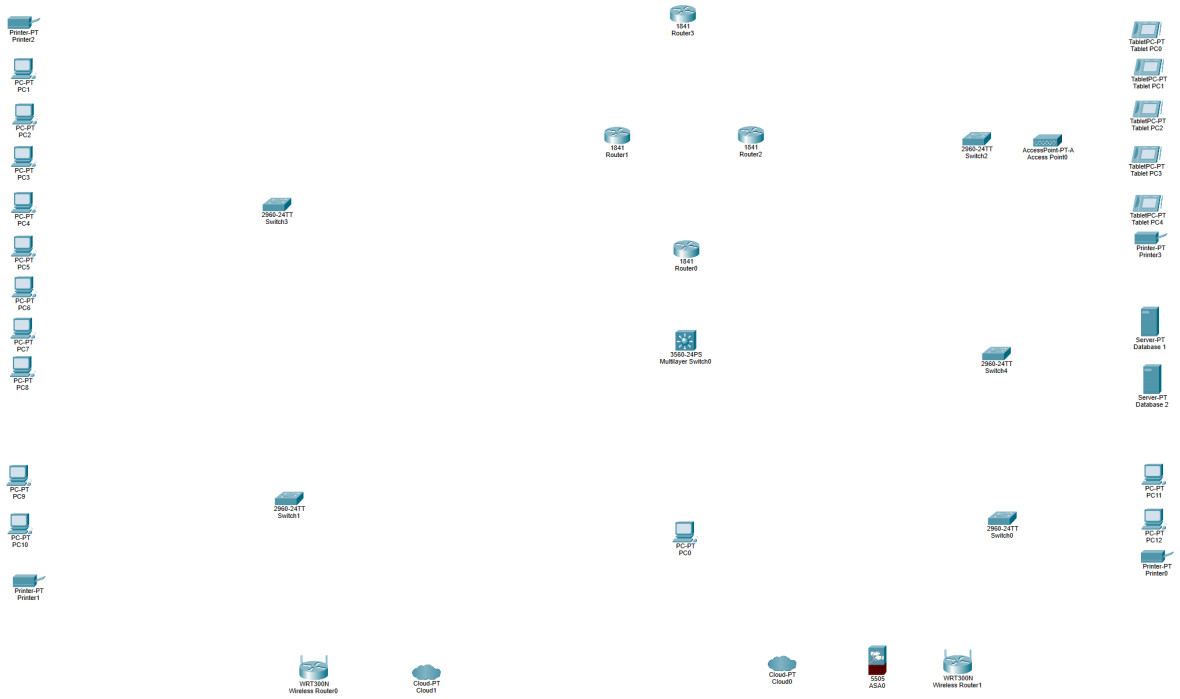

Рисунок 3.1 Загальна схема мережевої топології банківського відділення

Тепер робимо сегментацію за IP-адресами Зона прийому та обслуговування юридичних та фізичних осіб встановлюємо IP-адреси

192.168.1.0/24 (Рис. 3.2). У цій зоні ми маємо 8 комп'ютерів, яким встановлюємо статичні IP-адреси з 192.168.1.1/24 до 192.168.1.8/24 (Рис. 3.3). А також принтер, якому присуджуємо 192.168.1.100/24 (Рис. 3.4). Після завершення налаштувань з'єднуємо мережевими дротами Ethernet пристрої з комутатором Switch3 (Рис. 3.5).

Комп'ютери отримали послідовні IP-адреси для зручності адміністрування та логічної організації мережі. Принтер Printer2 отримав адресу 192.168.1.100/24 - таку IP-адресу було обрано для зручності визначення та ідентифікації допоміжних пристроїв у мережі, відокремлюючи їх від основних робочих станцій. Для всіх пристроїв використовувалася маска підмережі 255.255.255.0, що відповідає нотації /24.

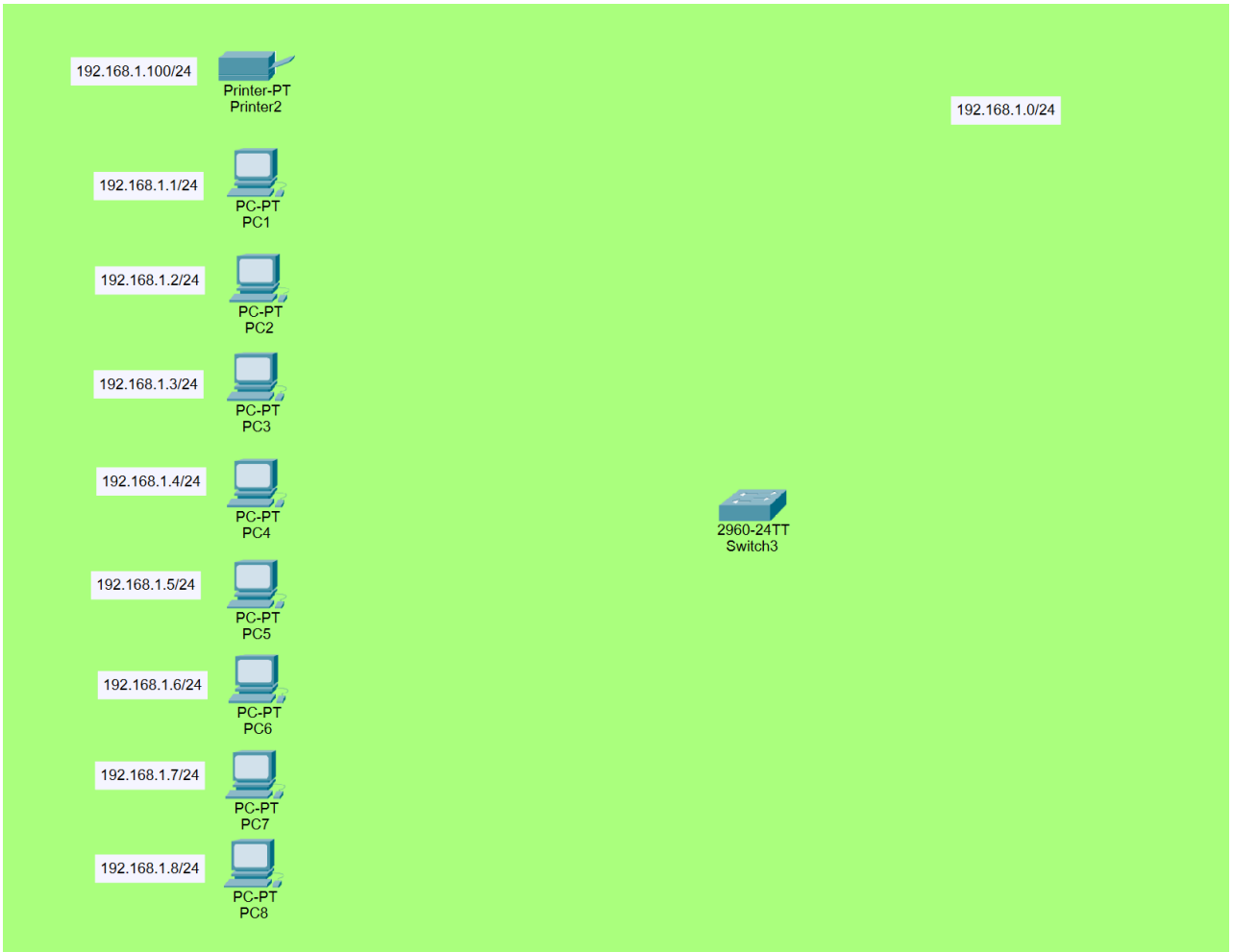

Рисунок 3.2 Сегментація зони обслуговування юридичних та фізичних

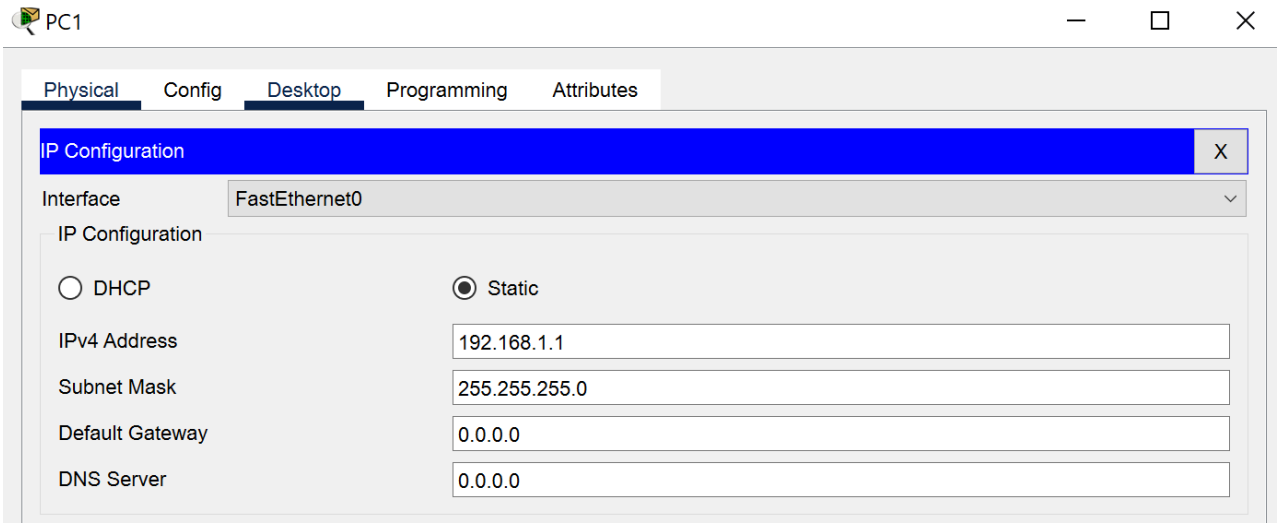

Рисунок 3.3. Встановлення статичних IP адрес робочим станціям працівників

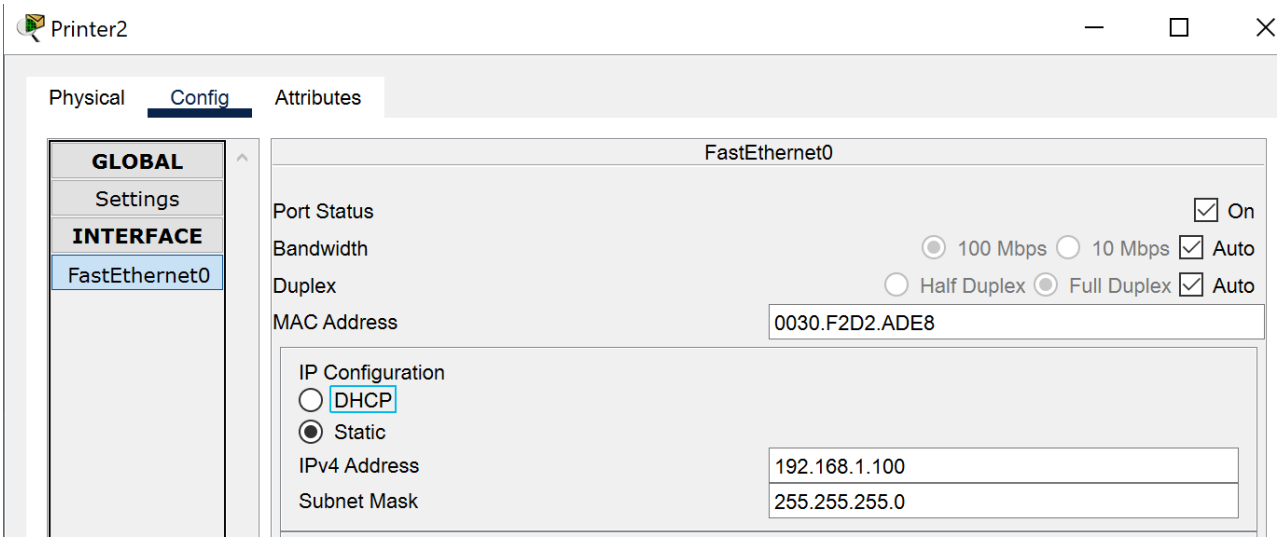

Рисунок 3.4 Встановлення статичної IP адреси принтеру

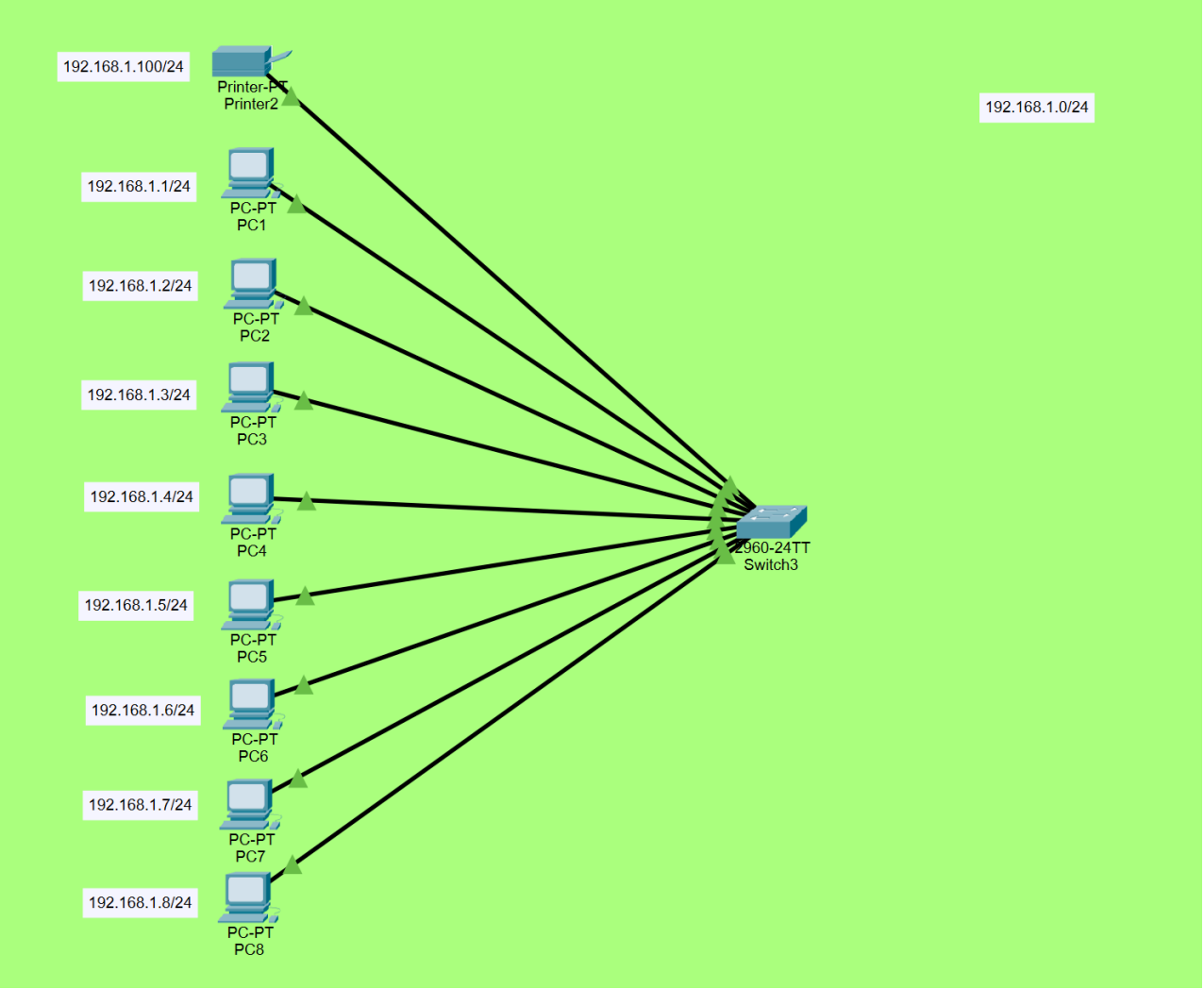

Рисунок 3.5 Під’єднання пристроїв до комутатора зони

Касова зона отримала мережевий сегмент 192.168.2.0/24 (Рис. 3.6). У цій зоні ми розмістили 2 касові робочі станції з IP-адресами PC9 - 192.168.2.1/24 та PC10 - 192.168.2.2/24 (Рис. 3.7). Додатково встановлено принтер Printer1 з IP-адресою 192.168.2.100/24 (Рис. 3.8). Всі пристрої касової зони підключені до комутатора Switch1 за допомогою Ethernet кабелів (Рис. 3.9). Ця касова зона є критично важливим сегментом мережі, оскільки через неї проходять всі фінансові операції банку.

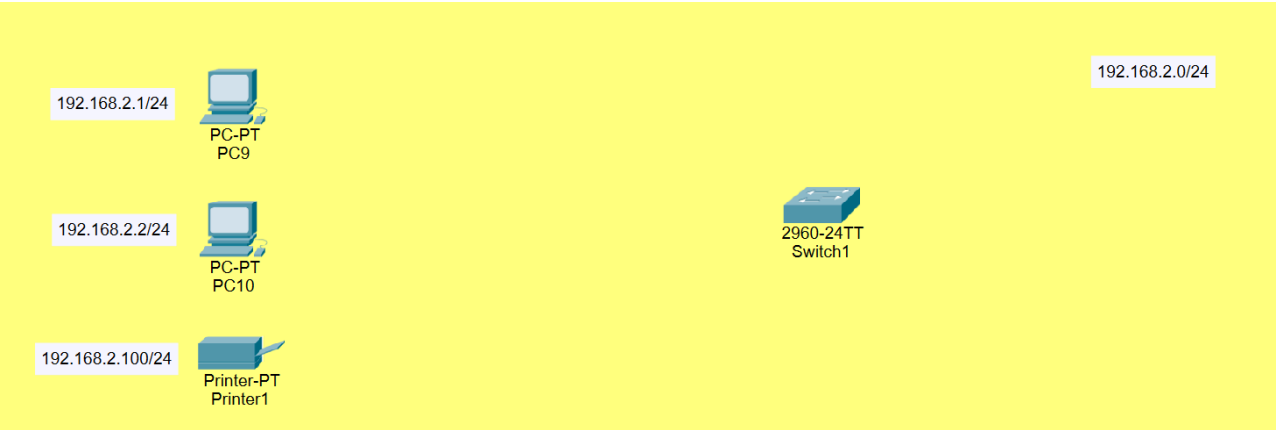

Рисунок 3.6 Сегментація касової зони

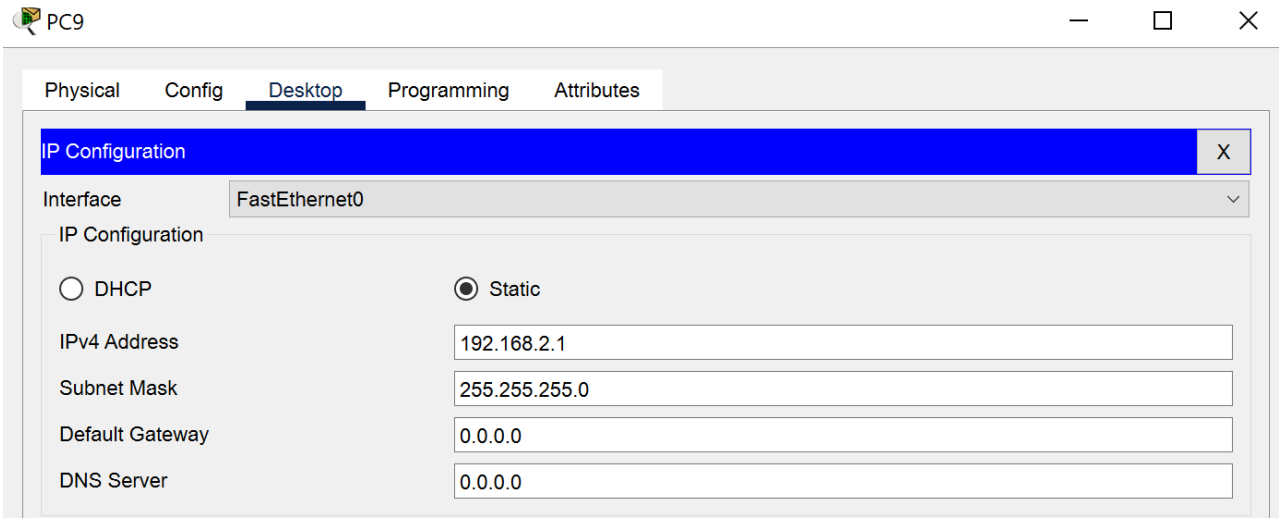

Рисунок 3.7 Встановлення статичних IP адрес робочим станціям працівників

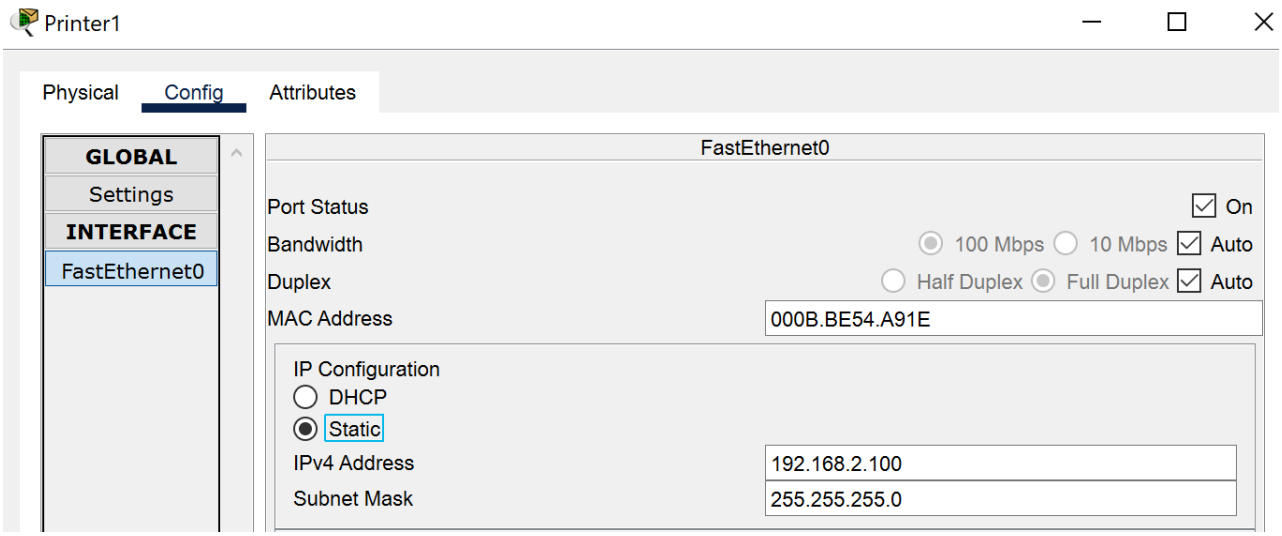

Рисунок 3.8 Встановлення статичної IP адреси принтеру

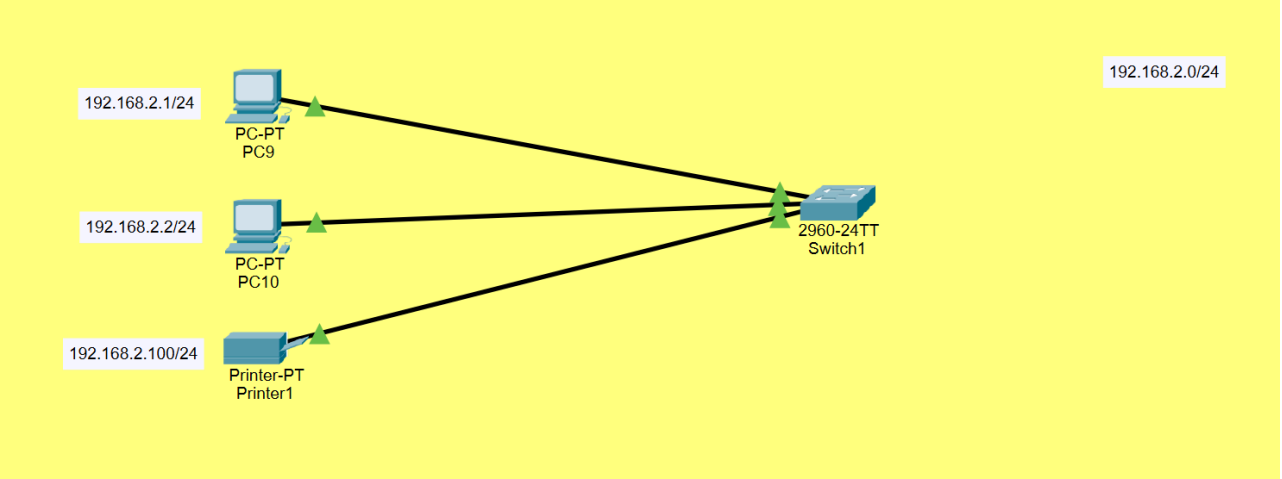

Рисунок 3.9 Під’єднання пристроїв до комутатора зони

Зона прийому та обслуговування фізичних осіб налаштована з мережевим сегментом 192.168.3.0/24 (Рис. 3.10). У цій зоні ми розгорнули 5 планшетів з IP-адресами від Tablet PC0 - 192.168.3.1/24 до Tablet PC4 - 192.168.3.5/24 (Рис. 3.11). Додатково встановлено принтер Printer3 з IP-адресою 192.168.3.100/24 (Рис. 3.12).

Спочатку підключаємо всі 5 планшетів до точки доступу AccessPoint0 через бездротове з'єднання Wi-Fi. Кожний планшет налаштовується для підключення до бездротової мережі з ідентифікатором SSID "WorkTablet" та паролем "Tr25b_ye5&3f". На точці доступу налаштовано захищений протокол WPA2-PSK з шифруванням AES для забезпечення безпеки бездротового з'єднання (Рис. 3.13). Планшети автоматично отримують свої статичні IP-адреси у діапазоні 192.168.3.1/24 - 192.168.3.5/24 після успішної автентифікації у Wi-Fi мережі (Рис. 3.14) (Рис. 3.15).

Після завершення налаштування всіх планшетів та їх успішного підключення до точки доступу, ми з'єднуємо AccessPoint0 з комутатором Switch2 за допомогою Ethernet кабелю. Одночасно принтер Printer3 також підключається до того ж комутатора Switch2 за допомогою Ethernet кабелю (Рис. 3.16). Таким чином, всі пристрої зони прийому та обслуговування фізичних осіб об'єднуються в єдиний мережевий сегмент через комутатор. Ця

зона забезпечує мобільність консультантів при роботі з клієнтами завдяки використанню планшетів з бездротовим підключенням.

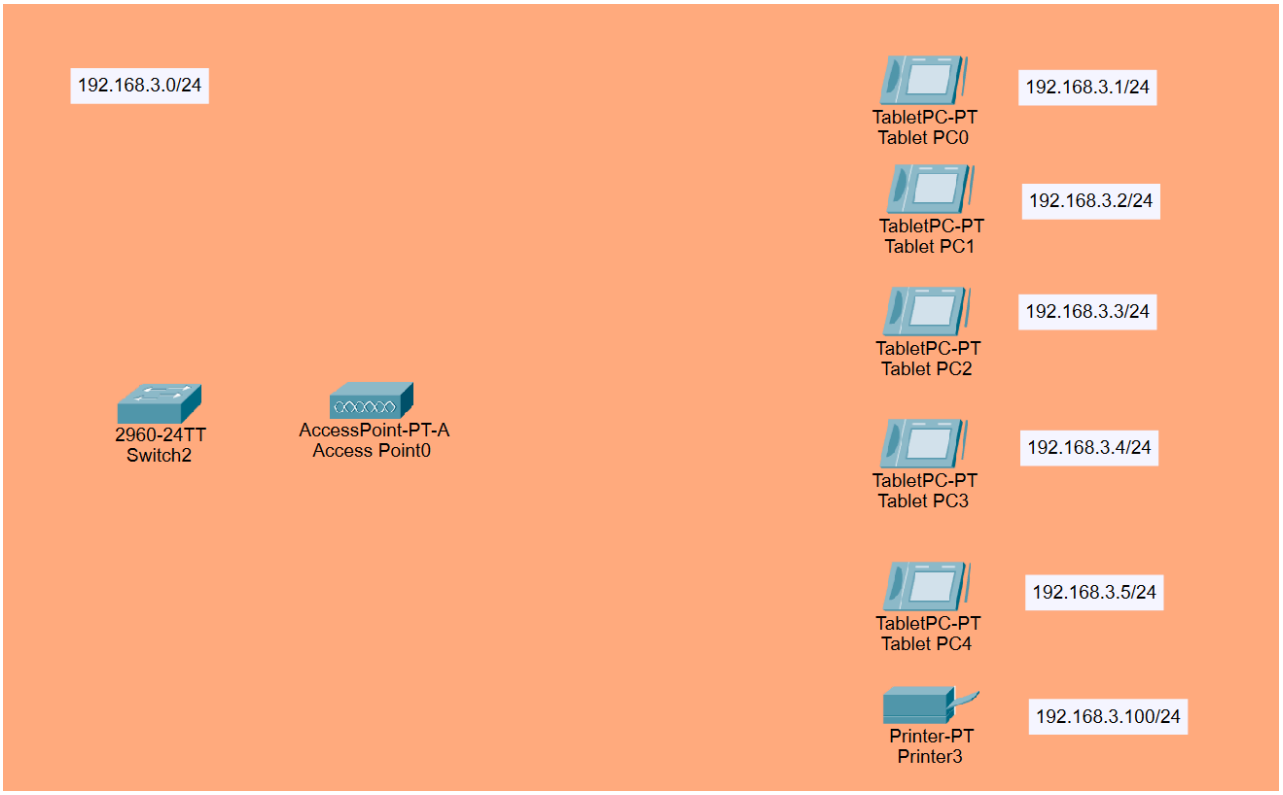

Рисунок 3.10 Сегментація зони обслуговування фізичних

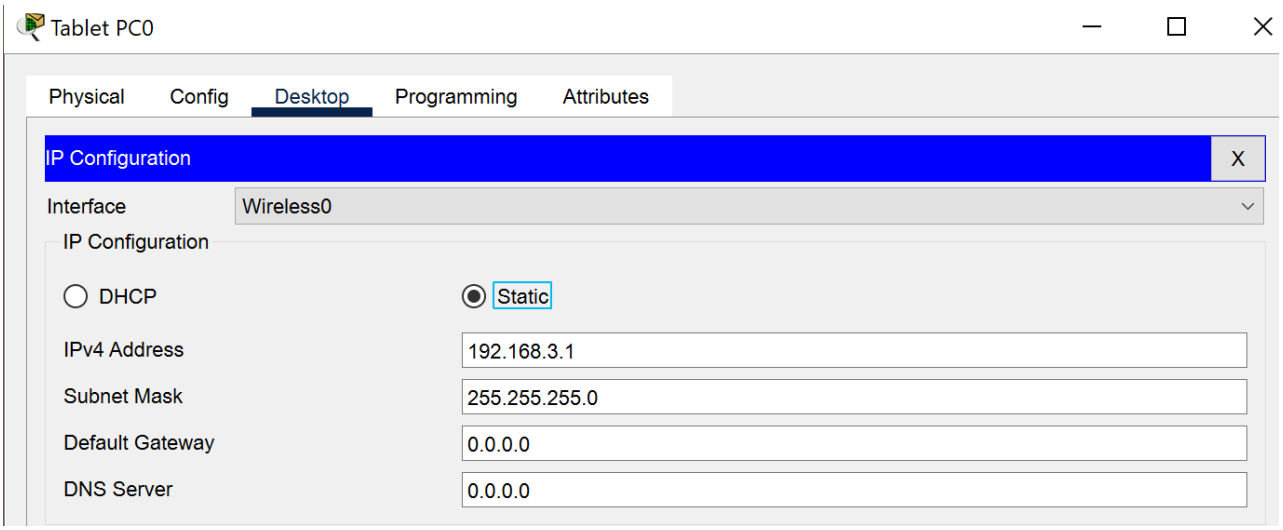

Рисунок 3.11 Встановлення статичних IP адрес робочим станціям працівників

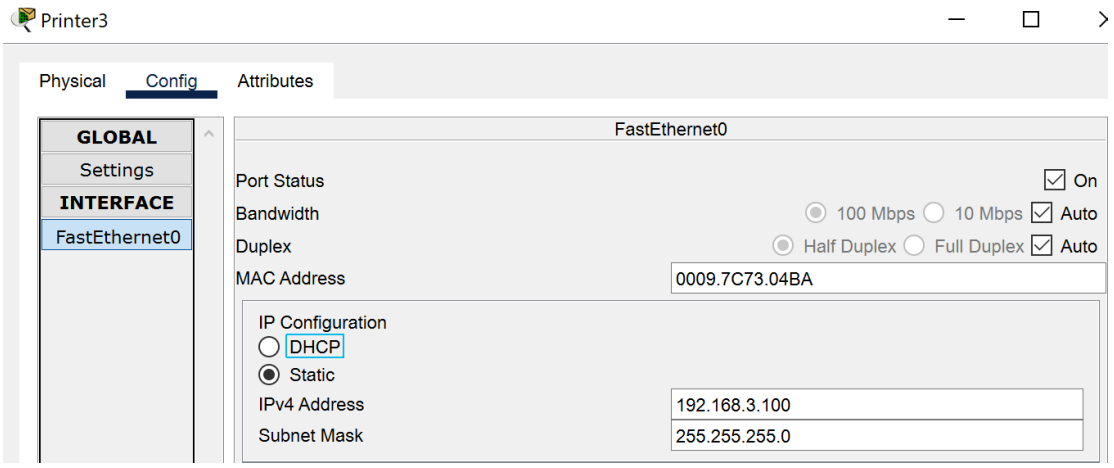

Рисунок 3.12 Встановлення статичної IP адреси принтеру

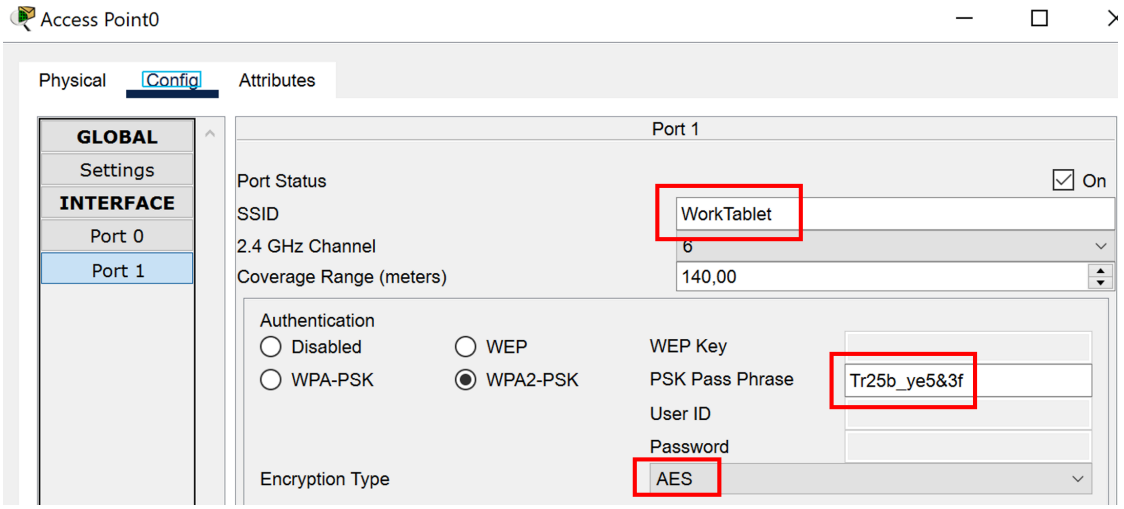

Рисунок 3.13 Налаштування Access Point

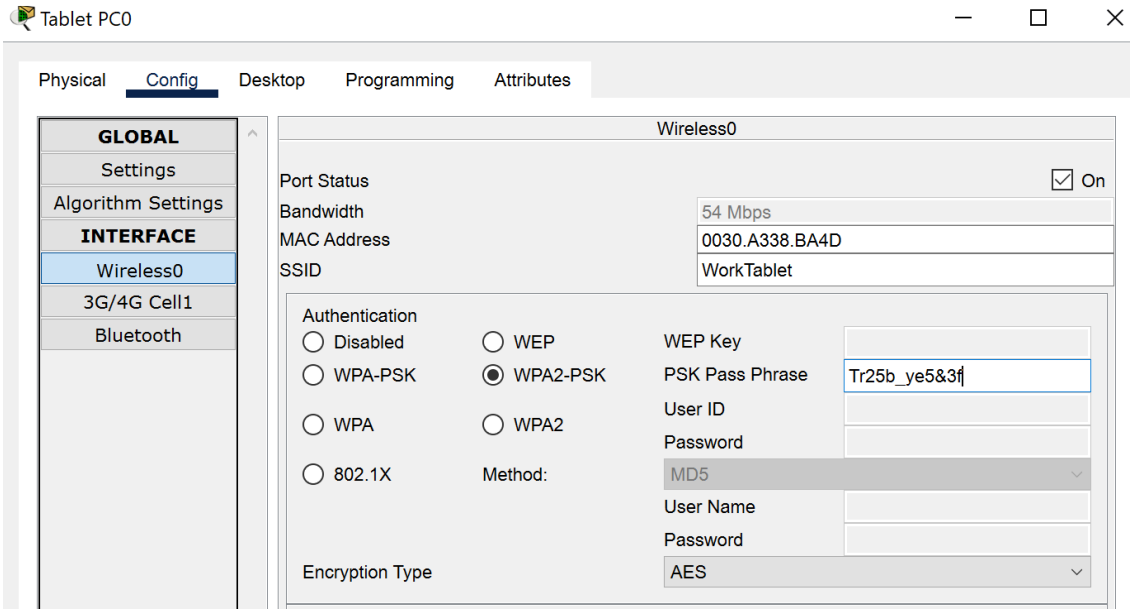

Рисунок 3.14 Підключення планшетів до Access Point

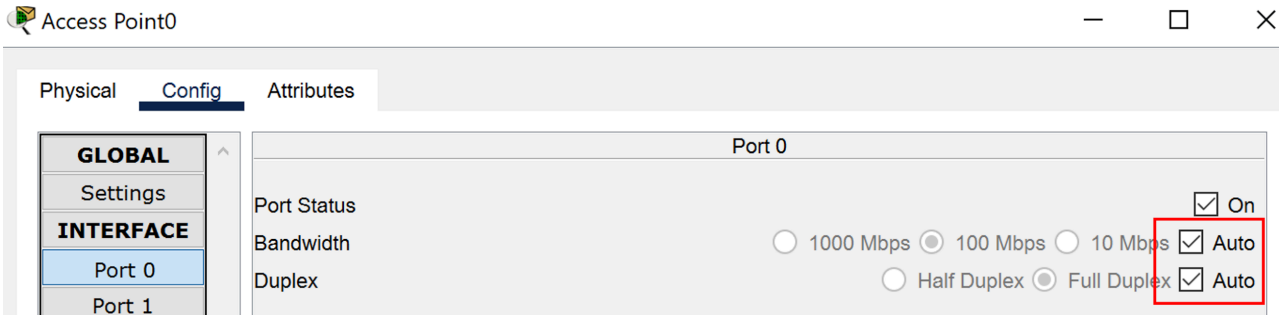

Рисунок 3.15 Встановлення автоматичних параметрів на параметри передачі

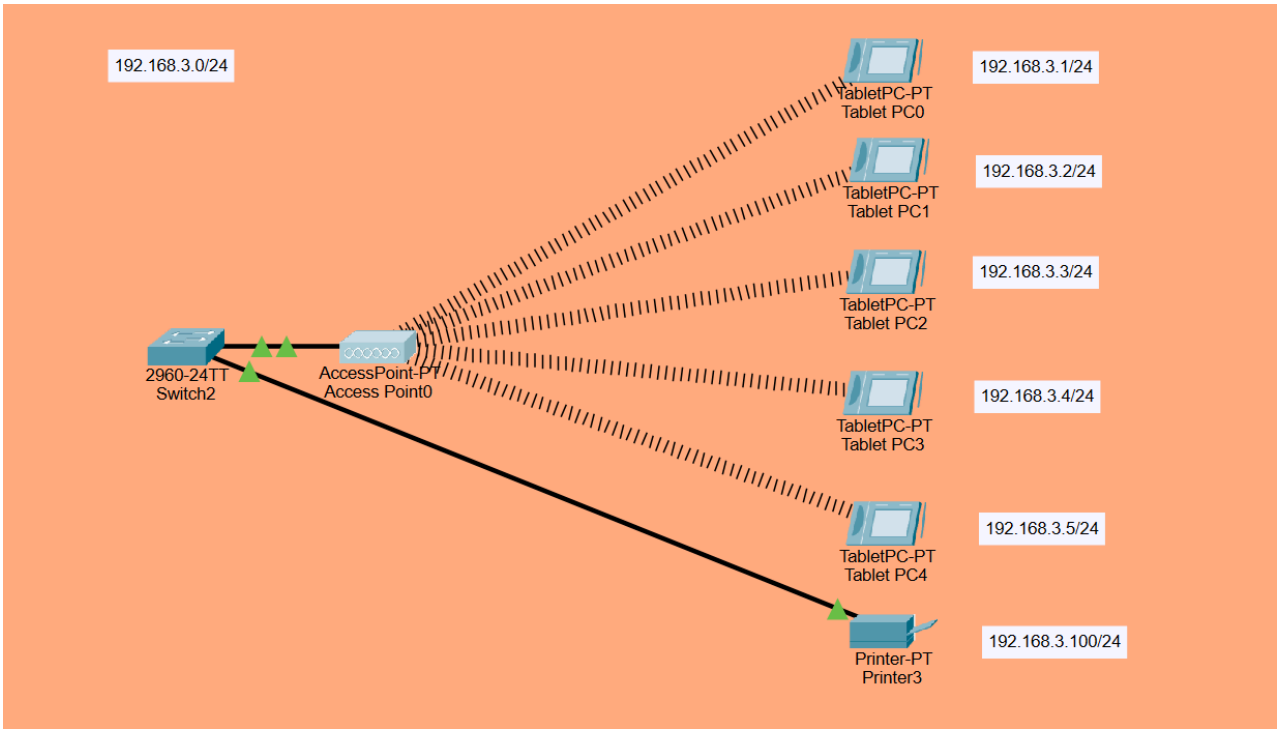

Рисунок 3.16 Під’єднання пристроїв до комутатора зони

Переходимо до налаштування серверної зони бази даних з мережевим сегментом 192.168.4.0/24 (Рис. 3.17). У цій зоні ми розгорнули 2 сервери баз даних з IP-адресами Database 1 - 192.168.4.100/24 та Database 2 - 192.168.4.101/24 (Рис. 3.18). Ці сервери є критично важливими компонентами банківської інфраструктури, оскільки зберігають та обробляють всю інформацію про клієнтів, фінансові операції та інші важливі дані банку.

Спочатку налаштовуємо IP-конфігурацію для кожного сервера. На сервері Database 1 встановлюємо статичну IP-адресу 192.168.4.100/24 з маскою підмережі 255.255.255.0. Аналогічно налаштовуємо сервер Database 2 з IP-адресою 192.168.4.101/24 та тією ж маскою підмережі. Такі IP-адреси було обрано для зручності ідентифікації серверного обладнання у мережі, відокремлюючи їх від клієнтських робочих станцій.

Після завершення налаштування IP-конфігурації на обох серверах, ми підключаємо їх до комутатора Switch4 за допомогою Ethernet кабелів. Сервер Database 1 підключається до одного з портів комутатора, а сервер Database 2 - до іншого порту того ж комутатора. Таким чином, обидва сервери об'єднуються в єдиний мережевий сегмент серверної зони через комутатор Switch4 (Рис. 3.19). Ця зона забезпечує централізоване зберігання та управління всіма даними банківського відділення з можливістю резервування та відмовостійкості завдяки використанню двох серверів баз даних.

Рисунок 3.17 Сегментація серверної зони

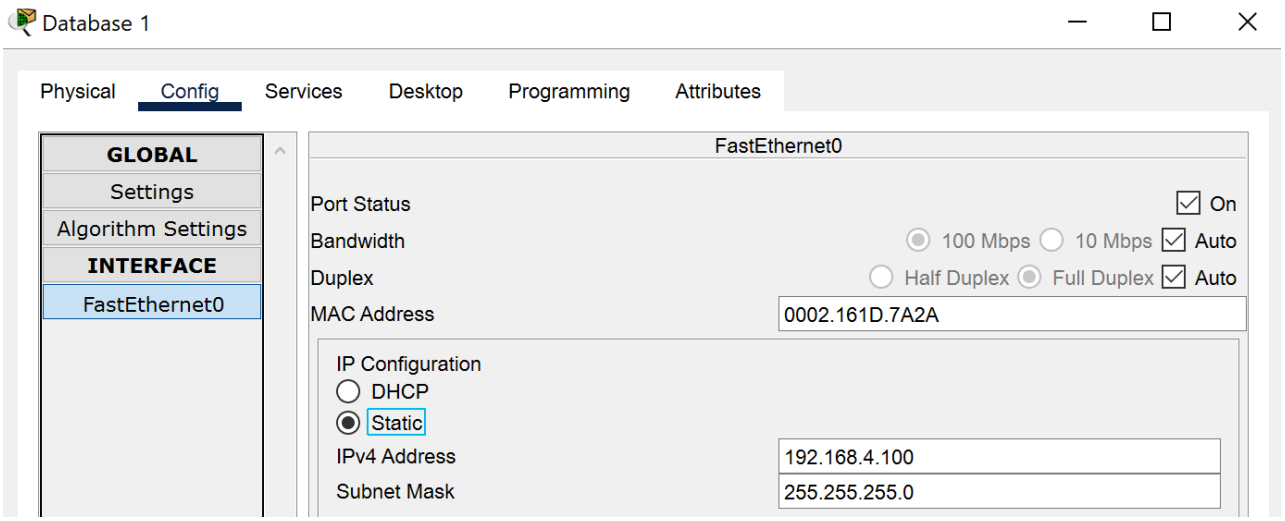

Рисунок 3.18 Встановлення статичних IP адрес серверам даних

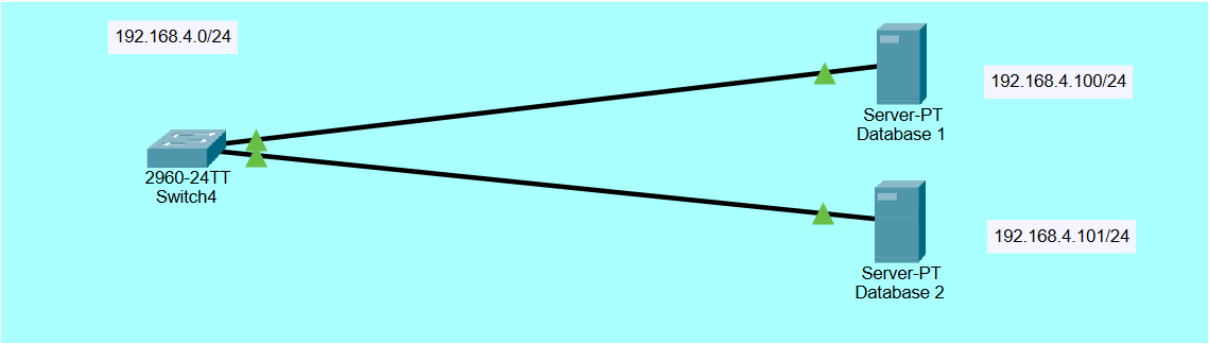

Рисунок 3.19 Під’єднання пристроїв до комутатора зони

Переходимо до налаштування зони директорів з мережевим сегментом 192.168.5.0/24 (Рис. 3.20). У цій зоні ми розгорнули 2 директорські комп'ютери з IP-адресами PC11 - 192.168.5.1/24 та PC12 - 192.168.5.2/24 (Рис. 3.21). Додатково встановлено принтер Printer0 з IP-адресою 192.168.5.100/24 (Рис. 3.22). Ця зона призначена для забезпечення роботи керівного складу банківського відділення та потребує підвищеного рівня безпеки й конфіденційності.

Спочатку налаштовуємо IP-конфігурацію для кожного директорського комп'ютера. На комп'ютері PC11 встановлюємо статичну IP-адресу 192.168.5.1/24 з маскою підмережі 255.255.255.0. Аналогічно налаштовуємо комп'ютер PC12 з IP-адресою 192.168.5.2/24 та тією ж маскою підмережі.

Принтер Printer0 отримує адресу 192.168.5.100/24 для зручності ідентифікації допоміжних пристроїв у директорській зоні.

Після завершення налаштування IP-конфігурації на всіх пристроях, ми підключаємо їх до комутатора Switch0 за допомогою Ethernet кабелів (Рис. 3.23).

Рисунок 3.20 Сегментація зони директорів

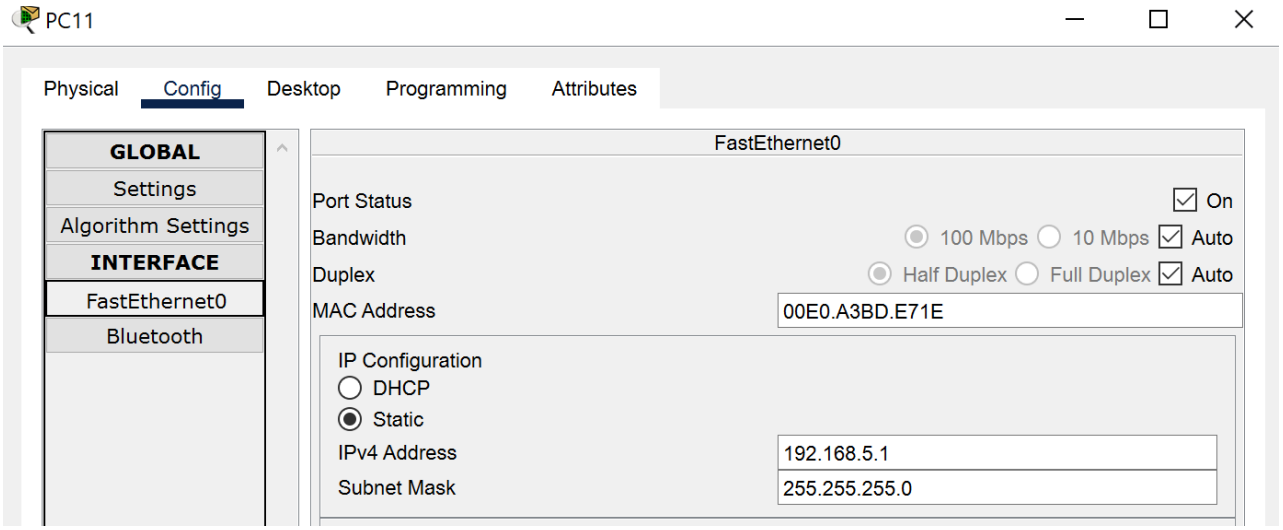

Рисунок 3.21 Встановлення статичних IP адрес робочим станціям директорів

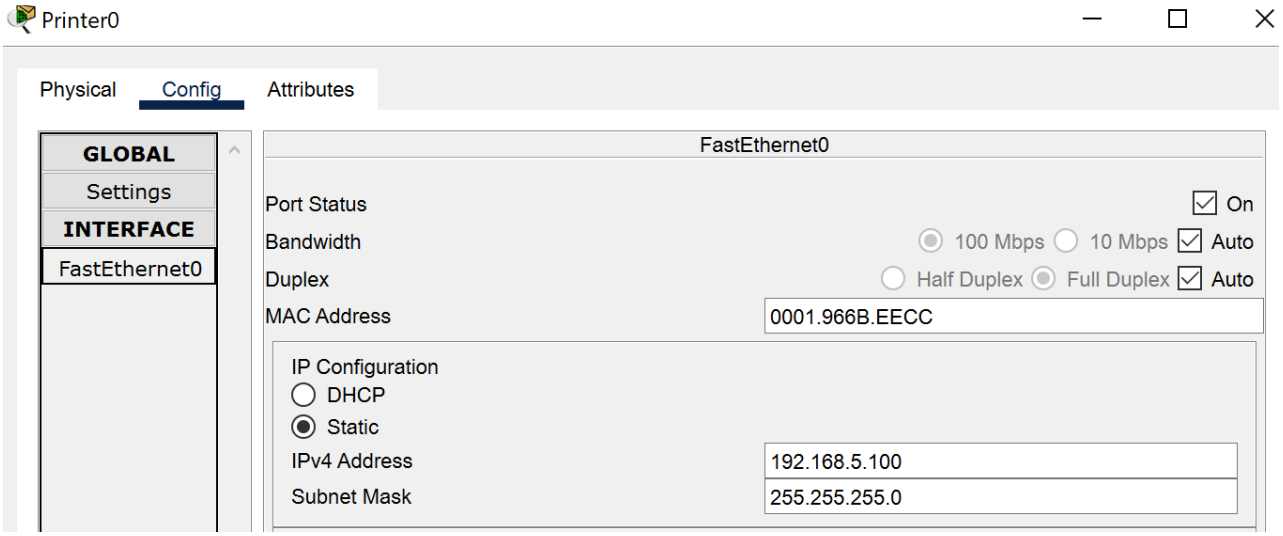

Рисунок 3.22 Встановлення статичної IP адреси принтеру

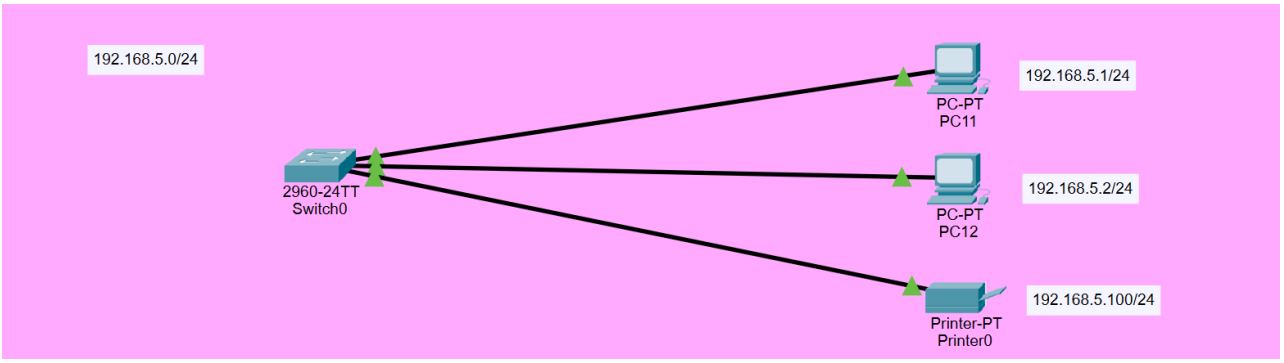

Рисунок 3.23 Під’єднання пристроїв до комутатора зони

Переходимо до налаштування зони адміністратора з мережевим сегментом 192.168.6.0/24 (Рис. 3.24). У цій зоні ми розмістили 1 адміністративний комп'ютер PC0 з IP-адресою 192.168.6.1/24 (Рис. 3.25). Ця зона є найбільш критичною з точки зору безпеки, оскільки забезпечує централізоване управління всією мережевою інфраструктурою банківського відділення та потребує максимального рівня захисту й обмеженого доступу.

Спочатку налаштовуємо IP-конфігурацію для адміністративного комп'ютера. На комп'ютері PC0 встановлюємо статичну IP-адресу 192.168.6.1/24 з маскою підмережі 255.255.255.0. Таку IP-адресу було обрано для зручності ідентифікації адміністративного обладнання у мережі та його відокремлення від інших зон банківського відділення.

Після завершення налаштування IP-конфігурації адміністративний комп'ютер PC0 підключається безпосередньо до центрального багаторівневого комутатора Multilayer Switch0 за допомогою Ethernet кабелю. До цього ж багаторівневого комутатора також будуть підключені всі інші комутатори Switch0, Switch1, Switch2, Switch3 та Switch4 з різних зон банківського відділення. Ця зона забезпечує системному адміністратору можливість централізованого управління всіма мережевими пристроями, моніторингу роботи системи та впровадження політик безпеки у всіх сегментах мережі банківського відділення через єдину точку доступу.

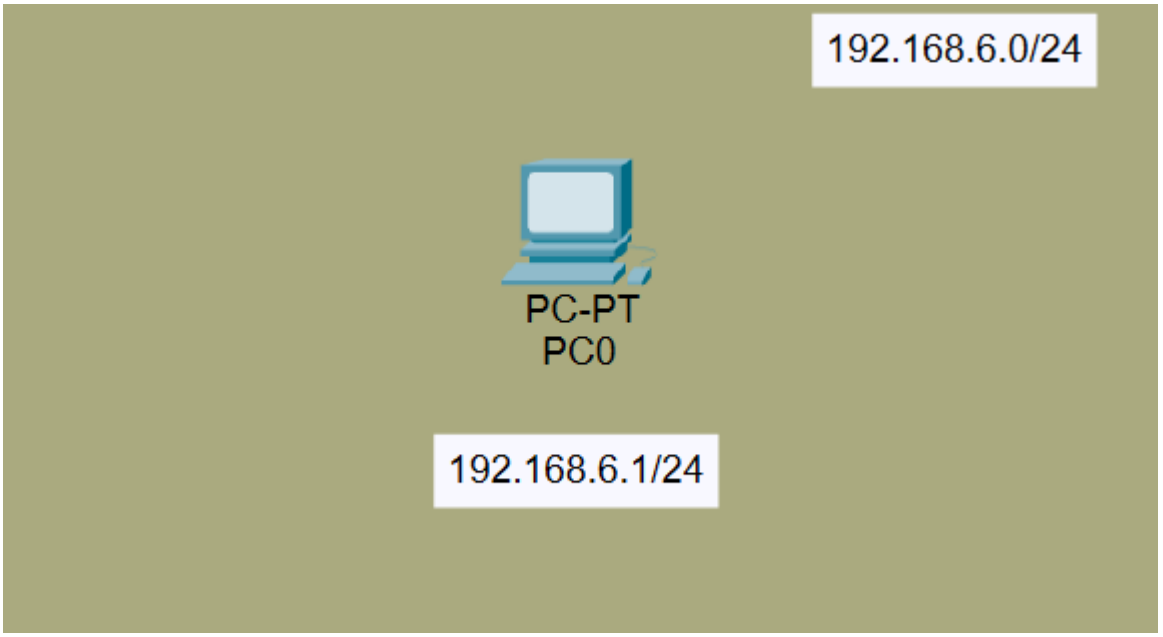

Рисунок 3.24 Сегментація зони адміністраторів

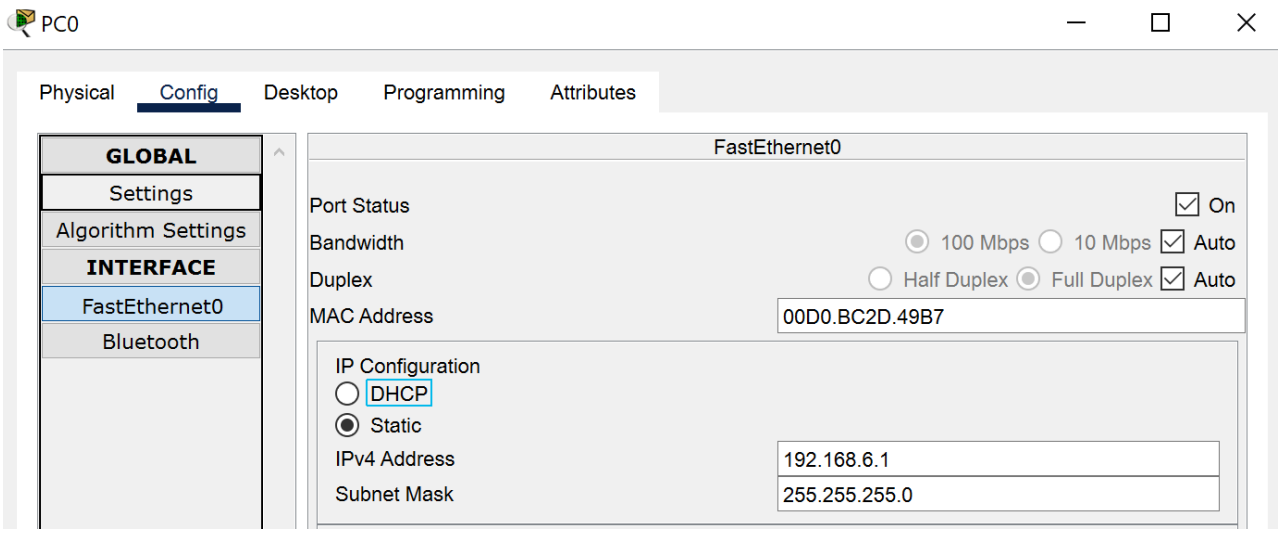

Рисунок 3.25 Встановлення статичної IP адреси робочі станці адміністратора

Переходимо до налаштування зони з'єднання до інтернету з мережевим сегментом 192.168.10.0/24 (Рис. 3.26). Ця зона забезпечує підключення всієї мережевої інфраструктури банківського відділення до глобальної мережі Інтернет та включає критично важливі компоненти для забезпечення зовнішнього зв'язку та безпеки. У цій зоні розміщено два бездротових маршрутизатори та міжмережний екран: Wireless Router0 з IP-адресою 192.168.10.1/24 для підключення нашої мережевої інфраструктури до інтернету, Wireless Router1 як окрема бездротова точка доступу до інтернету для клієнтів відділення, та міжмережний екран для забезпечення додаткового рівня захисту мережі.

Спочатку налаштовуємо IP-конфігурацію для основного маршрутизатора. На маршрутизаторі Wireless Router0 встановлюємо статичну IP-адресу 192.168.10.1/24 (Рис. 3.27) з маскою підмережі 255.255.255.0 в LAN налаштуваннях. Ця IP-адреса обрана як стандартна адреса шлюзу для забезпечення маршрутизації трафіку між внутрішньою мережею банківського відділення та зовнішніми мережами. Маршрутизатор Wireless Router1 налаштовується як автономна бездротова точка доступу для забезпечення інтернет-з'єднання клієнтам банку без доступу до внутрішньої корпоративної мережі.

Після завершення налаштування IP-конфігурації основний маршрутизатор Wireless Router0 підключається до центрального багаторівневого комутатора Multilayer Switch0 за допомогою Ethernet кабелю (Рис. 3.28). Міжмережний екран розміщується між маршрутизатором та зовнішніми з'єднаннями для фільтрації трафіку та блокування потенційних загроз. Маршрутизатор Wireless Router1 залишається автономним пристроєм для забезпечення безпечного Wi-Fi доступу клієнтів. Ця зона забезпечує контрольований та захищений доступ всіх пристроїв банківського відділення до глобальної мережі з багаторівневим захистом через міжмережний екран та ізольованим доступом для відвідувачів банку.

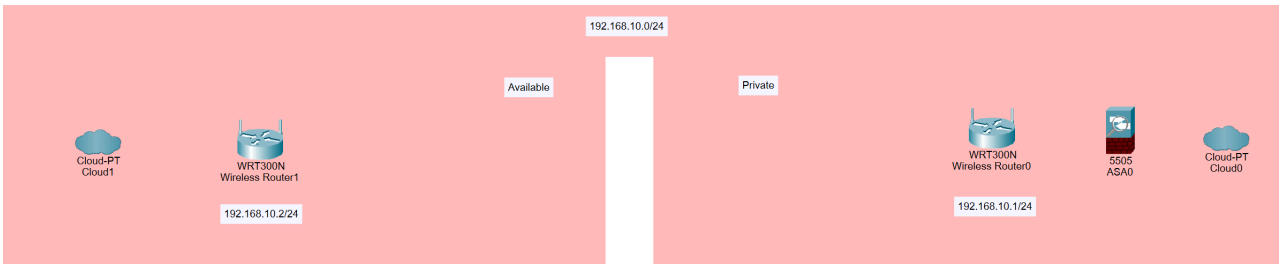

Рисунок 3.26 Сегментація мережевої зони

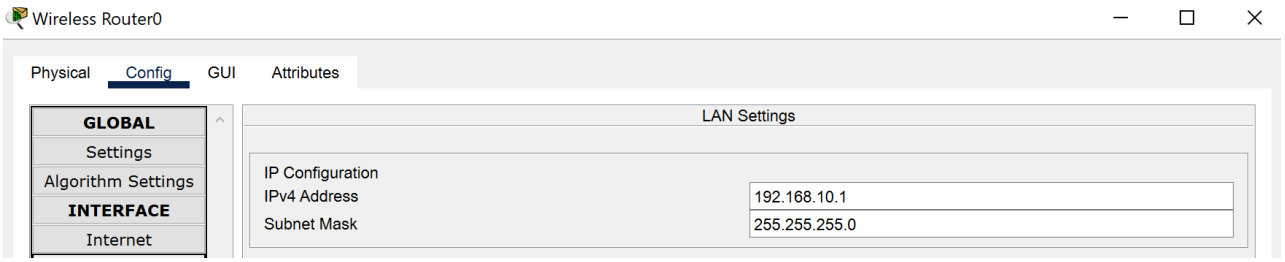

Рисунок 3.27 Встановлення статичних IP адрес роутерам

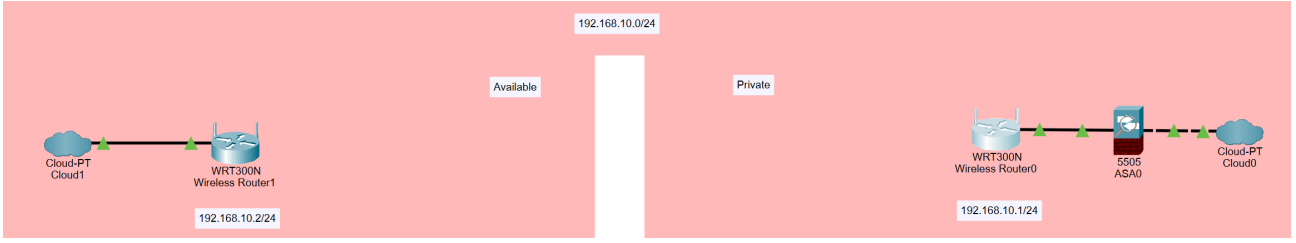

Рисунок 3.28 З’єднання роутерів з мережою інтернет

Для забезпечення максимального рівня безпеки на основному маршрутизаторі Wireless Router0 було відключено бездротову функціональність. Це критично важливо для запобігання несанкціонованому доступу до корпоративної мережі банку через бездротові з'єднання, оскільки будь-який зловмисник або сторонній пристрій могли б потенційно підключитися до основної мережевої інфраструктури та отримати доступ до конфіденційних банківських систем і даних клієнтів (Рис. 3.29).

У налаштуваннях маршрутизатора встановлено Coverage Range на 0.00 метрів (Рис. 3.30), що повністю припиняє трансляцію Wi-Fi сигналу, залишено Authentication як Disabled та очищено поле SSID. Ці дії призводять до повного відключення бездротової функції, оскільки нульовий радіус покриття означає відсутність Wi-Fi сигналу, порожнє SSID робить мережу невидимою для пристроїв, а відключена аутентифікація блокує будь-які спроби підключення.

Результатом цих налаштувань стало автоматичне переключення ноутбука (Рис. 3.31) Laptop0 (взято для прикладу) з мережі "Private" на мережу "Available", що демонструє ефективність відключення Wi-Fi на Router0.

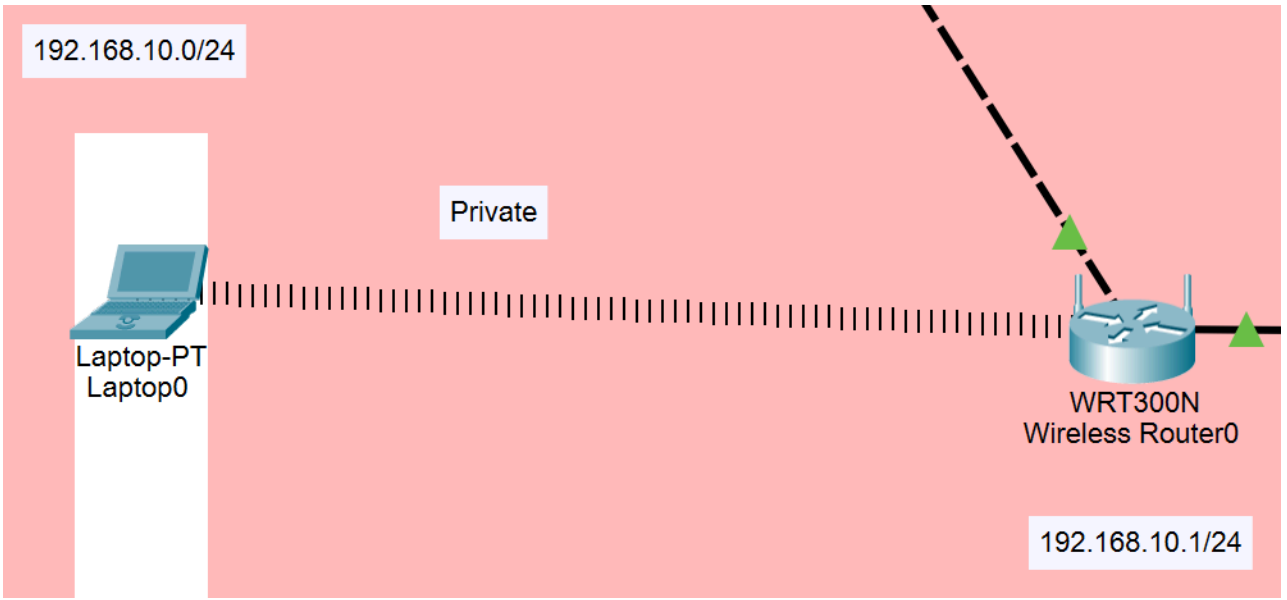

Рисунок 3.29 Підєднаня пристроїв до приватної мережі

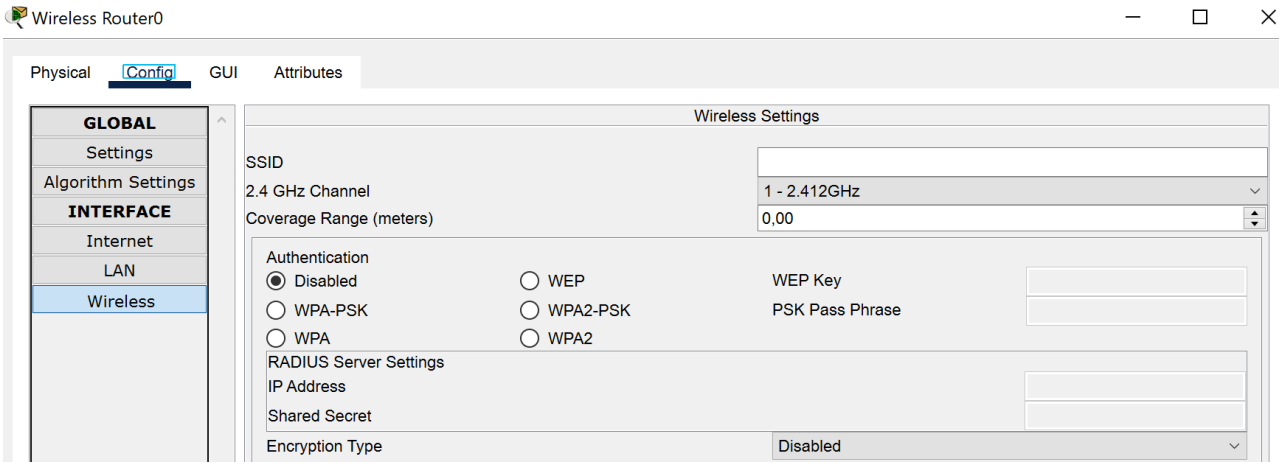

Рисунок 3.30 Прибирання зони покриття роутера

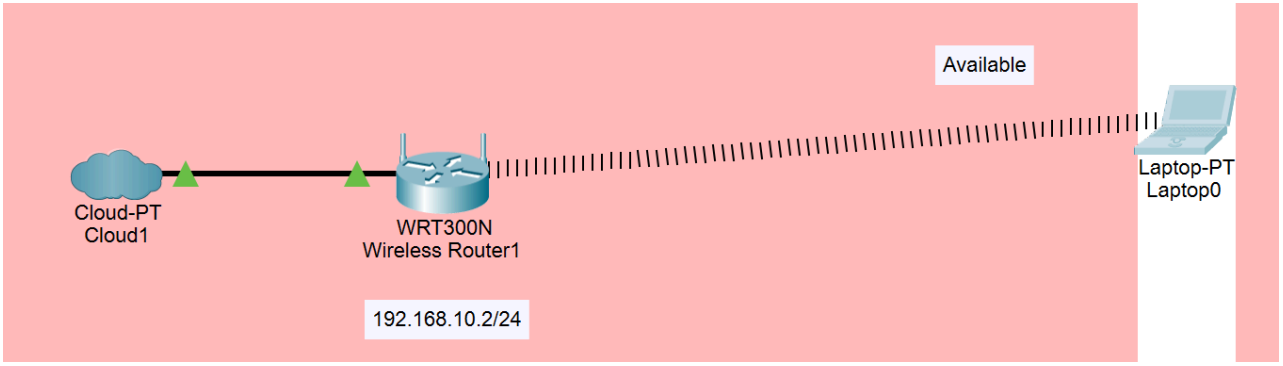

Рисунок 3.31 Автоматичне перепідключення до локальної мережі

Для підвищення безпеки клієнтського доступу до інтернету на маршрутизаторі Wireless Router1 було налаштовано захищену бездротову мережу з паролем. У налаштуваннях бездротової мережі встановлено SSID "ClientWIFI" для зручної ідентифікації клієнтської мережі, активовано протокол безпеки WPA2-PSK як найбільш надійний метод аутентифікації для захисту від несанкціонованого доступу, та встановлено пароль "PRIVATBANK91" у полі PSK Pass Phrase (Рис. 3.32).

Радіус покриття встановлено на 250 метрів, що забезпечує достатнє покриття для клієнтської зони банківського відділення. Такі налаштування безпеки запобігають підключенню сторонніх осіб до клієнтської Wi-Fi мережі без відома адміністрації банку, при цьому надаючи авторизованим відвідувачам

надійний та захищений доступ до інтернет-ресурсів, ізольований від корпоративної мережевої інфраструктури.

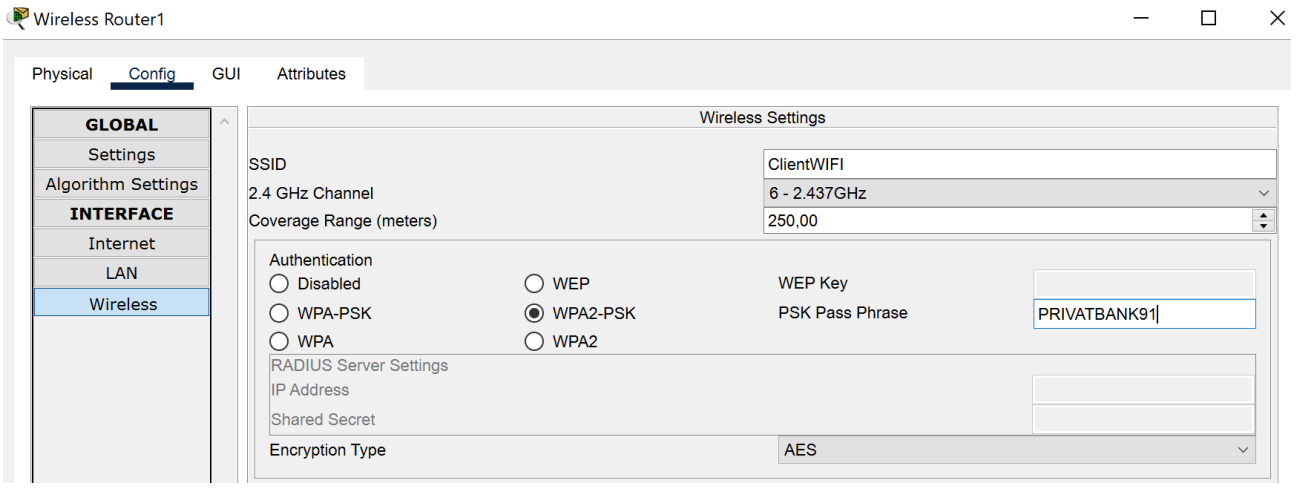

Рисунок 3.32 Налаштування паролю на локальному роутері

Сегментація мережі банківського відділення на окремі IP-діапазони була впроваджена з метою забезпечення безпеки, контролю доступу та ефективного управління мережевою інфраструктурою. Кожна зона отримала унікальний мережевий сегмент для логічного відокремлення різних типів пристроїв та рівнів доступу до банківських систем.

Основною метою такого підходу є створення ізольованих мережевих сегментів, що дозволяє обмежити поширення потенційних кіберзагроз між різними зонами банківського відділення. У випадку компрометації одного сегменту, зловмисники не зможуть автоматично отримати доступ до інших критично важливих систем, що значно підвищує загальний рівень інформаційної безпеки установи.

У результаті отримуємо готову топологію банкової мережі відділення №91, готової до впровадження рішень з захисту безпеки.

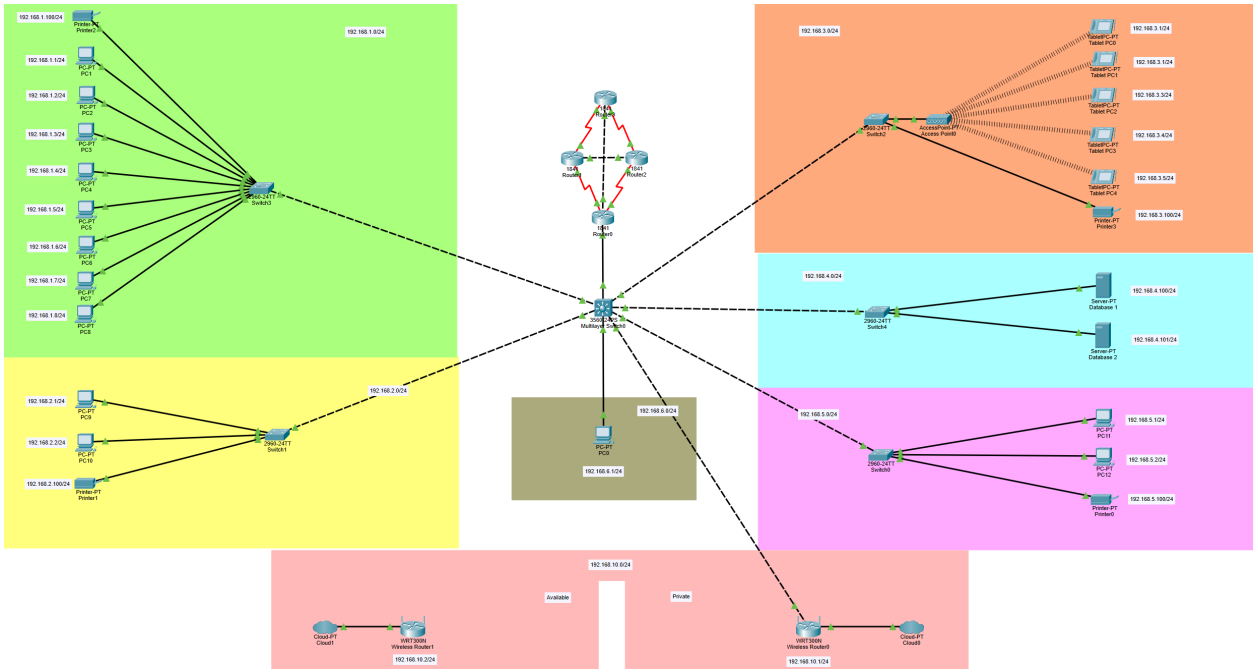

Рисунок 3.33 Результат топології

3.2 Впровадження рішень захисту третього рівня (мережевий рівень)

У розділі 1.2 було розглянуто основні рішень для захисту мережевої інфраструктури. Для побудови комплексної моделі, необхідно застосувати всі ці рішення на нашій мережі. Охоплюючи всі можливі небезпечні фактори, які можуть загрожувати мережі. Вровадження почнемо з 3-го рівня захисту.

Першим етапом буде встановлення міжмережних екранів у кретичних точках. Першою важливою є точка, яка встановлюється між внутрішньою мережею та інтернетом, називатись вона буде периметровий міжмережний екран (Рис. 3.34).

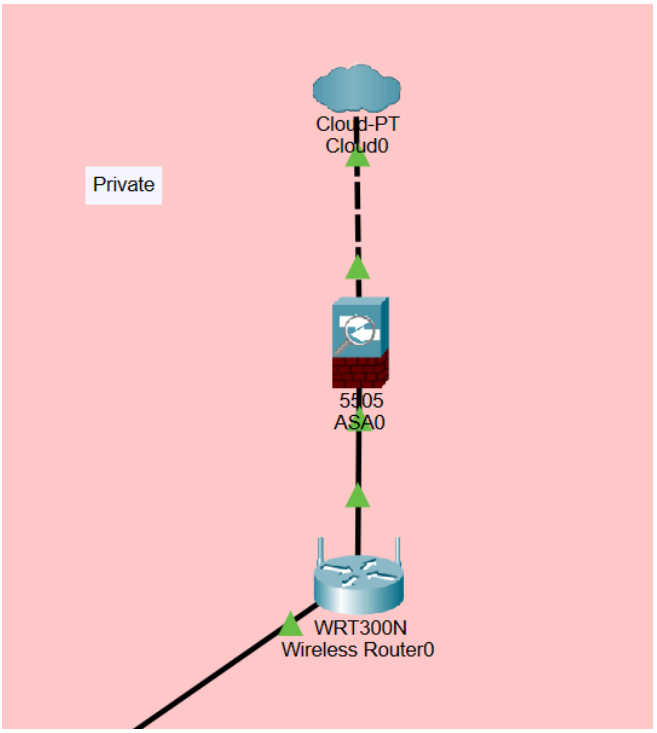

Рисунок 3.34 Периметровий міжмережний екран

Наступний міжмережний екран обов'язково треба встановити перед критичними серверами та важливими сегментами мережі, називатись буде внутрішни міжмережний екран (Рис. 3.35).

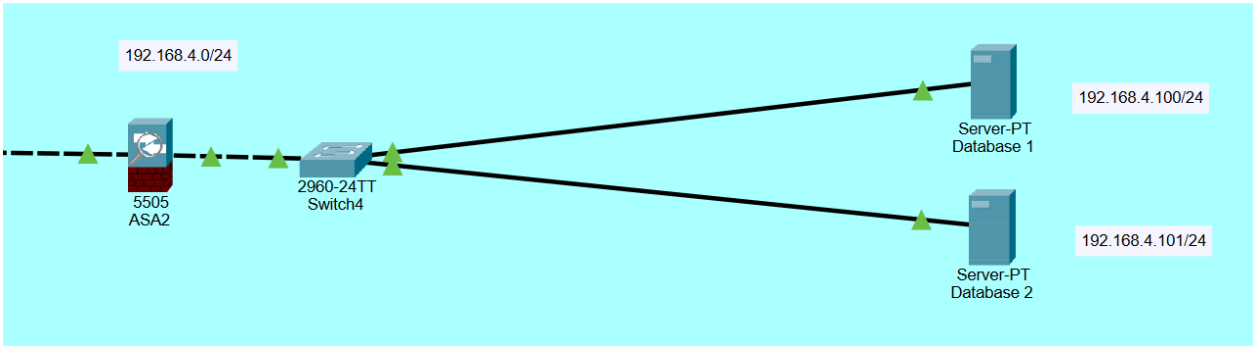

Рисунок 3.35 Внутрішни міжмережний екран

І останні міжмережні екрани – це Сегментні (Рис. 3.36), вони встановлюються між різними сегментами мережі, наприклад між відділами банку.

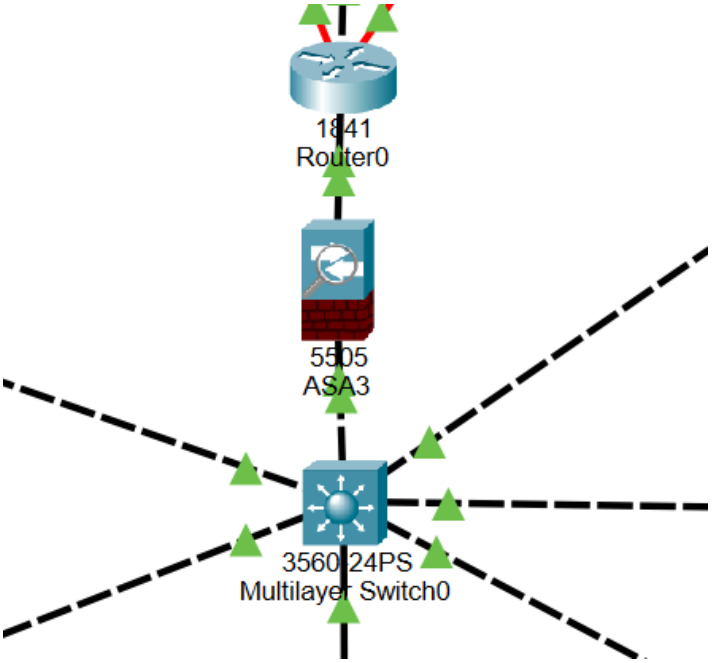

Рисунок 3.36 Сегментний міжмережний екран

Всі міжмережні екрани встановлені, вони забезпечать контроль доступу через фільтрацію трафіку за IP-адресами, портами та протоколами і захистять від мережевих атак (DDoS, port scanning, SYN flood).

Переходячи до другого етапу встановлюємо демілітаризована зону, яка працює як ізольований сегмент мережі між зовнішнім інтернетом та внутрішньою корпоративною мережею, де розміщуються публічні сервіси (веб-сервери, поштові сервери, DNS). Вона захищається двома міжмережними екранами: зовнішнім (між інтернетом та ДМЗ) та внутрішнім (між ДМЗ та локальною мережею) (Рис. 3.37). Так, як зовнішній міжмережний екран встановлений, додаємо також внутрішній

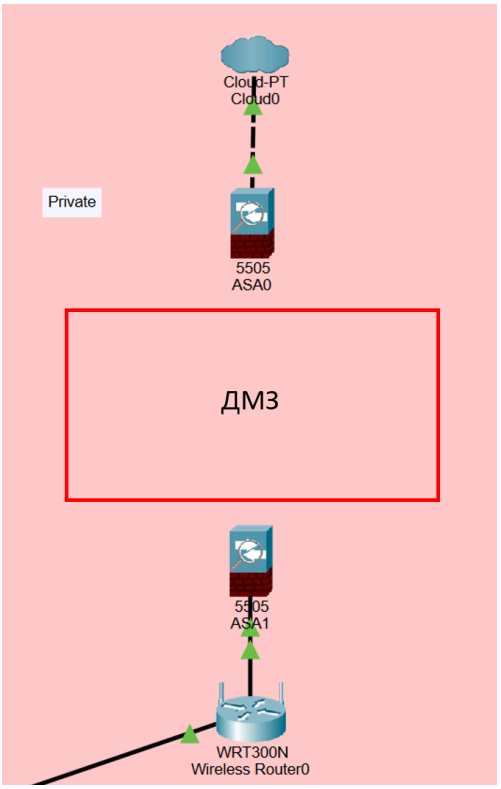

Рисунок 3.37 Встановлення демілітаризованої зони

Відповідно у цю зону заносимо сервери з'єднані комутатором. А саме: File Server, Web Server, Mail Server, DNS Server (Рис. 3.38).

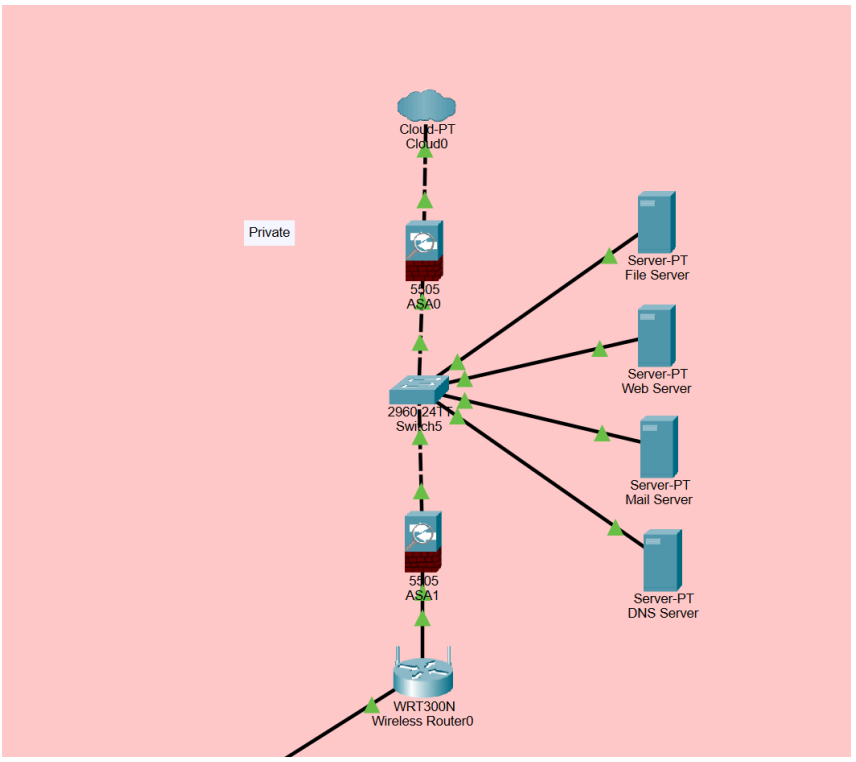

Рисунок 3.38 Розміщення серверів у ДМЗ

Підхід ДМЗ ускладнює для хакера отримання прямого доступу до даних та внутрішніх серверів організації через Інтернет. Якщо зловмисник зможе проникнути через зовнішній брандмауер і скомпрометувати систему в демілітаризованій зоні, йому також доведеться подолати внутрішній брандмауер, перш ніж отримати доступ до конфіденційних корпоративних даних.

Системи запобігання вторгненням (IPS) і Системи виявлення вторгнень (IDS), IPS відстежує мережевий трафік на наявність шкідливої активності [14]. Залежно від правил запобігання, він може повідомляти про трафік, блокувати його або відкидати для захисту мережі. А IDS виявляє шкідливу активність і сповіщає про неї. Ці рішення є окремими, але їх можна, а також варто застосовувати разом, оскільки вони доповнюють один одного і забезпечують комплексний захист мережі. IPS працює в режимі реального часу, активно блокуючи відомі загрози, але може пропустити складні або нові типи атак, а також іноді помилково заблокувати легітимний трафік. IDS працює в пасивному режимі, детально аналізуючи весь трафік без втручання в його передачу, що дозволяє виявляти довготривалі APT атаки, аномальну поведінку та складні багатоетапні вторгнення, які можуть бути непомітними для IPS.

Систему будемо використовувати Suricata, бо вона має підтримку як IPS так і IDS з можливістю їх об’єдання [15]. А також має потужні можливості для створення власних правил виявлення, забезпечує детальне логування для аудиту та розслідувань. Найкращім рішенням розміщення Suricata буде не в розріз, а зеркалення трафіку на ного. Тобто треба зробити підключення маршрутизатора, будемо використовувати MicroTic, і проганяти трафік через Suricata (Рис. 3.39).

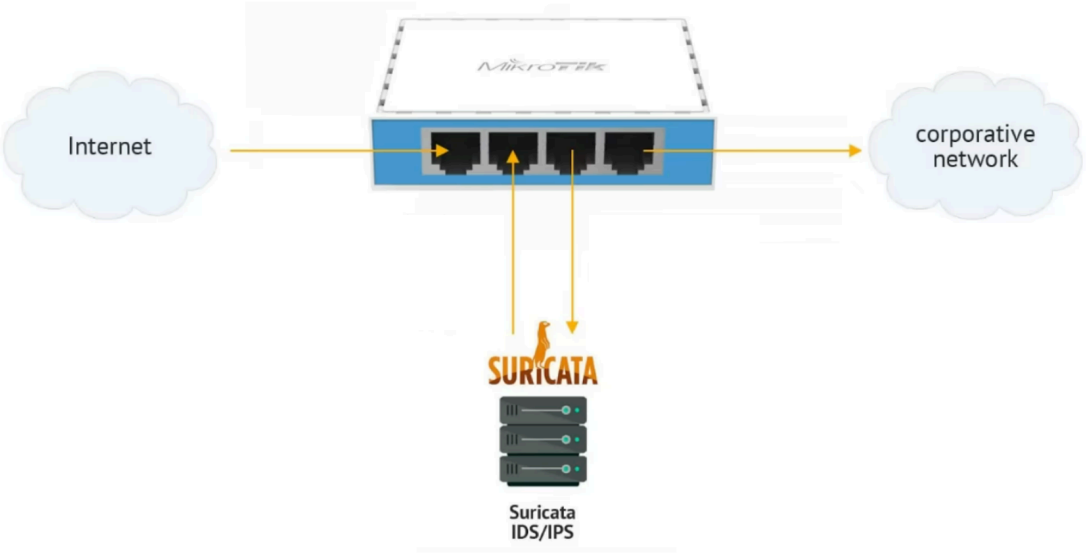

Рисунок 3.39 Зображення схеми підключення MicroTic і Suricata

Для легкості реалізації, будемо використовувати продукт SELKS у якому зіброно Suricata, а також рішення Kibana (забезпечує візуалізацію даних безпеки через інтерактивні дашборди, графіки та звіти для аналізу інцидентів та трендів атак). Scirius (Веб-інтерфейс для управління правилами Suricata, дозволяючи легко додавати, модифікувати правила виявлення загроз та керувати політиками безпеки). EveBox (альтернативний інтерфейс для швидкої обробки та класифікації алертів Suricata, забезпечуючи ефективний workflow для аналітиків безпеки).

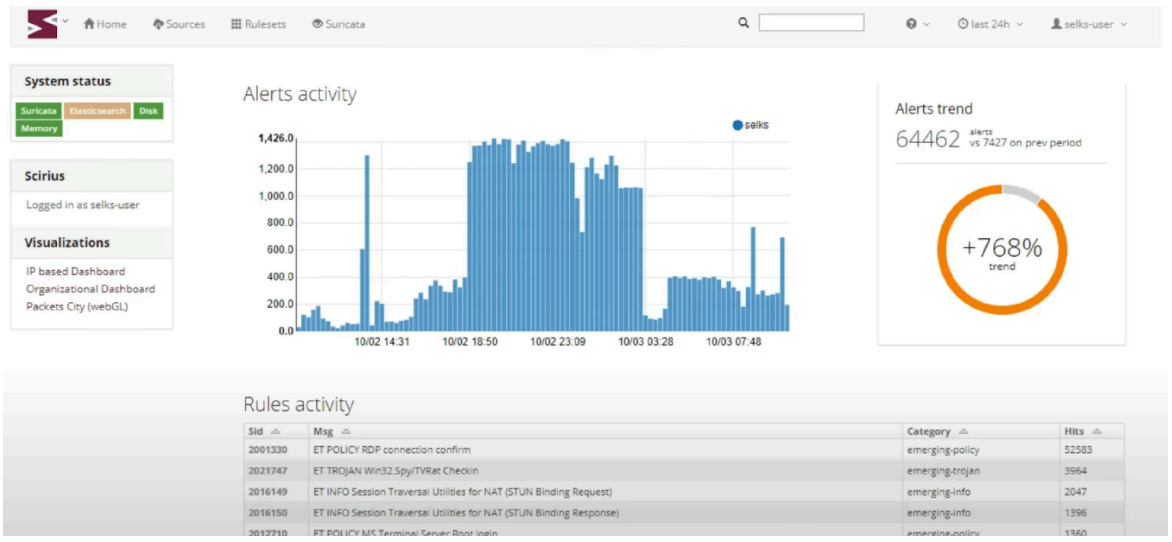

Рисунок 3.40 SELKS система

Розміщаємо це рішення після міжмережевого екрану і перед Switch5 (Рис. 41)

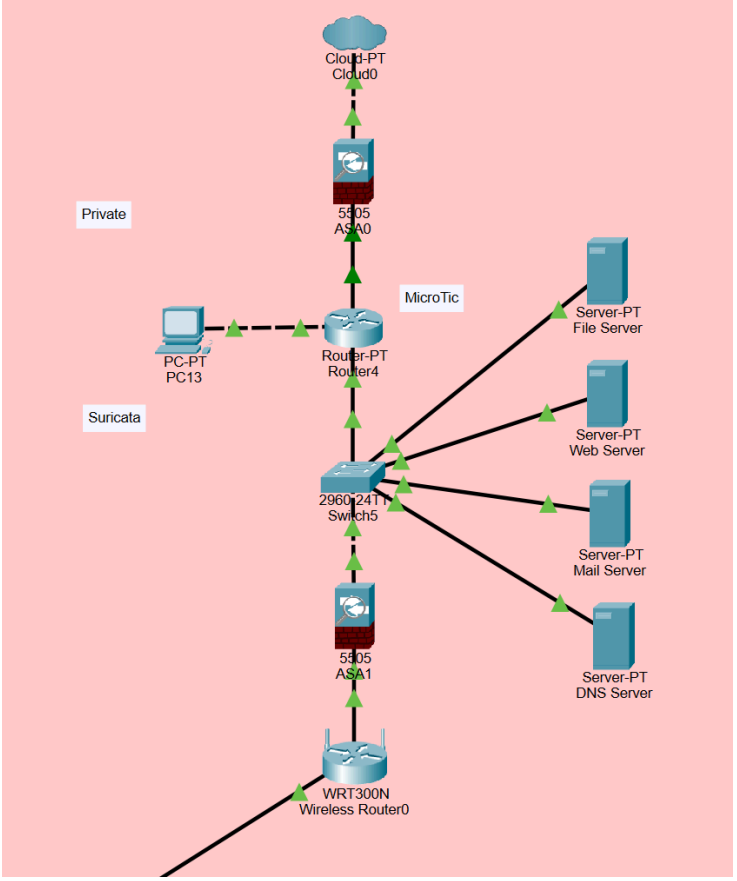

Рисунок 3.41 Розміщення MicroTic і Suricata на схемі мережі

Залишилось реалізувати VPN тунелювання, працює це через створення віртуального зашифрованого каналу між пристроями користувачів та мережею [16]. Реалізовувати будемо через зовнішній міжмережний екран.

Спочатку налаштовуємо мережеві інтерфейси для VPN-клієнта - створюємо основу для безпечного виходу в інтернет з усіх корпоративних мереж. Outside інтерфейс отримує реальний IP від провайдера та має рівень безпеки 0 для зв'язку з VPN-серверами. Inside інтерфейс стає централізованим шлюзом з адресою 192.168.1.1, через який ASA буде обслуговувати всі

підмережі організації від 192.168.1.0 до 192.168.6.0, включаючи серверну мережу 192.168.4.0 (Рис. 3.42).

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
ciscoasa#
ciscoasa# enable
ciscoasa# configure terminal
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
ciscoasa(config-if)# exit
ciscoasa(config)# interface Ethernet0/1
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
ciscoasa(config-if)# exit
ciscoasa(config)#
```

Рисунок 3.42 Налаштування мережевих інтерфейсів міжмережевого екрану для VPN-підключення

Далі конфігуруємо криптографічні протоколи для підключення до VPN-провайдера - активуємо IKEv2 та встановлюємо банківський рівень безпеки з AES-256 шифруванням і SHA-256 для перевірки цілісності. Ці алгоритми забезпечують максимальний захист для всього корпоративного трафіку незалежно від кількості мереж, що використовуються в організації (Рис. 3.43).

```
ciscoasa(config)# crypto ikev2 enable outside
ciscoasa(config)# crypto ikev2 policy 10
ciscoasa(config-ikev2-policy)# encryption aes-256
ciscoasa(config-ikev2-policy)# integrity sha256
ciscoasa(config-ikev2-policy)# group 14
ciscoasa(config-ikev2-policy)# prf sha256
ciscoasa(config-ikev2-policy)# exit
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal VPN_PROVIDER
ciscoasa(config-ipsec-proposal)# protocol esp encryption aes-256
ciscoasa(config-ipsec-proposal)# protocol esp integrity sha256
ciscoasa(config-ipsec-proposal)# exit
ciscoasa(config)#
```

Рисунок 3.43 Конфігурація криптографічних протоколів IKEv2 з шифруванням AES-256

Потім створюємо комплексні правила трафіку для захисту всіх корпоративних мереж - access-list VPN_INTERNET містить шість окремих правил для кожної підмережі (192.168.1.0 через 192.168.6.0), що гарантує шифрування трафіку з усіх сегментів мережі. Особливу увагу приділяємо серверній мережі 192.168.4.0, оскільки сервери часто містять критично важливі дані, які потребують додаткового захисту при виході в інтернет (Рис. 3.44).

```
ciscoasa(config)# access-list VPN_INTERNET extended permit ip 192.168.1.0
255.255.255.0 any
ciscoasa(config)# access-list VPN_INTERNET extended permit ip 192.168.2.0
255.255.255.0 any
ciscoasa(config)# access-list VPN_INTERNET extended permit ip 192.168.3.0
255.255.255.0 any
ciscoasa(config)# access-list VPN_INTERNET extended permit ip 192.168.4.0
255.255.255.0 any
ciscoasa(config)# access-list VPN_INTERNET extended permit ip 192.168.5.0
255.255.255.0 any
ciscoasa(config)# access-list VPN_INTERNET extended permit ip 192.168.6.0
255.255.255.0 any
ciscoasa(config)# crypto map INTERNET_VPN 10 match address VPN_INTERNET
ciscoasa(config)# crypto map INTERNET_VPN 10 set peer 185.159.158.240
WARNING: The IP address 185.159.158.240 is being used for the peer
ciscoasa(config)# crypto map INTERNET_VPN 10 set ikev2 ipsec-proposal VPN_PROVIDER
ciscoasa(config)# crypto map INTERNET_VPN interface outside
ciscoasa(config)#
```

Рисунок 3.44 Створення правил трафіку для всіх корпоративних підмереж у VPN

Наступним кроком налаштовуємо надійну автентифікацію з VPN-провайдером - встановлюємо tunnel group з простим але ефективним pre-shared key "25", який забезпечує швидку автентифікацію та стабільне з'єднання для всього корпоративного трафіку (Рис. 3.45).

```
ciscoasa(config)# tunnel-group 185.159.158.240 type ipsec-l2l
ciscoasa(config)# tunnel-group 185.159.158.240 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key 25
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 25
ciscoasa(config-tunnel-ipsec)# exit
ciscoasa(config)#
```

Рисунок 3.45 Налаштування групи тунелю та автентифікації з pre-shared key

Після цього конфігуруємо розподілену маршрутизацію та NAT для всієї мережевої інфраструктури - створюємо індивідуальні network objects для кожної підмережі, включаючи спеціалізований SERVER_NETWORK для критично

важливої серверної мережі 192.168.4.0. Кожен сегмент мережі отримує власне NAT правило, що дозволяє всім корпоративним пристроям - від робочих станцій до серверів та мережевого обладнання - безпечно виходити в інтернет з повністю прихованими внутрішніми IP-адресами (Рис. 3.46).

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 185.159.158.240
ciscoasa(config)# object network NETWORK_1
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network SERVER_NETWORK
ciscoasa(config-network-object)# subnet 192.168.4.0 255.255.255.0
ciscoasa(config-network-object)# exit
ciscoasa(config)# nat (inside,outside) source dynamic NETWORK_1 interface
ciscoasa(config)# nat (inside,outside) source dynamic SERVER_NETWORK interface
INFO: Creating NAT rules for all networks (2-6 similar)
ciscoasa(config)# access-list OUTSIDE_IN extended permit esp any any
ciscoasa(config)# access-list OUTSIDE_IN extended permit udp any any eq isakmp
ciscoasa(config)# access-list OUTSIDE_IN extended permit udp any any eq 4500
ciscoasa(config)# access-group OUTSIDE_IN in interface outside
ciscoasa(config)#
```

Рисунок 3.46 Конфігурація NAT-правил та мережевих об'єктів для підмереж

Нарешті зберігаємо конфігурацію та підтверджуємо функціонування захищеної корпоративної мережі - вся мережева інфраструктура організації, включаючи шість підмереж та серверний сегмент, тепер отримує корпоративний рівень безпеки з повною анонімністю, шифруванням та захистом від кібератак при роботі в інтернеті (Рис. 3.47).

```
ciscoasa(config)# exit
ciscoasa# write memory
Building configuration...
Cryptochecksum: 51d4a82e 3c96b044 ef8b1957 6f81c7d3
2048 bytes copied in 0.580 secs
[OK]
ciscoasa# show crypto ikev2 sa
IKEv2 SAs:
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local Remote
1 192.168.1.1/500 185.159.158.240/500
ciscoasa# show crypto ipsec sa | include encaps
#pkts encaps: 342, #pkts encrypt: 342, #pkts digest: 342
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 35/45/55 ms
INFO: All internet traffic is now encrypted via VPN tunnel
ciscoasa#
```

Рисунок 3.47 Збереження конфігурації та підтвердження функціонування VPN

3.3 Впровадження рішень захисту другого рівня (рівень комутаторів)

Далі переходимо до реалізації захисту, визначеного у 2-му рівні. А саме MAC-фільтрацію і політики контролю доступу. Визначаємо тільки ці пункти, бо IP сегментація вже була розроблена, при побудові топології.

Задача побудови нашої системи з MAC-фільтрацією, визначити всі прилади мережі і не допустити інші. Якщо розглянути більш детально. Також забезпечити повний доступ до областей комутаторів зі звичайними співробітниками, а до директорів заборонити всім користувачам, тільки трафік з серверів і адміна і відповідно їх самий.

Починаємо з огляду маршрутизатора Зони прийому та обслуговування юридичних та фізичних осіб. Визначаємо порт з яким будемо працювати (Рис. 48). І потім робимо кількість прийнятних MAC адрес портом обмеженою, перше, ми робимо для fastEthernet 0/1, де підключено тільки 1 комп’ютер ПК1 (Рис. 49). Тому кількість MAC адрес встановлюється 1. Після прописуємо той MAC адрес, який видав нам сам комп’ютер (Рис. 50).

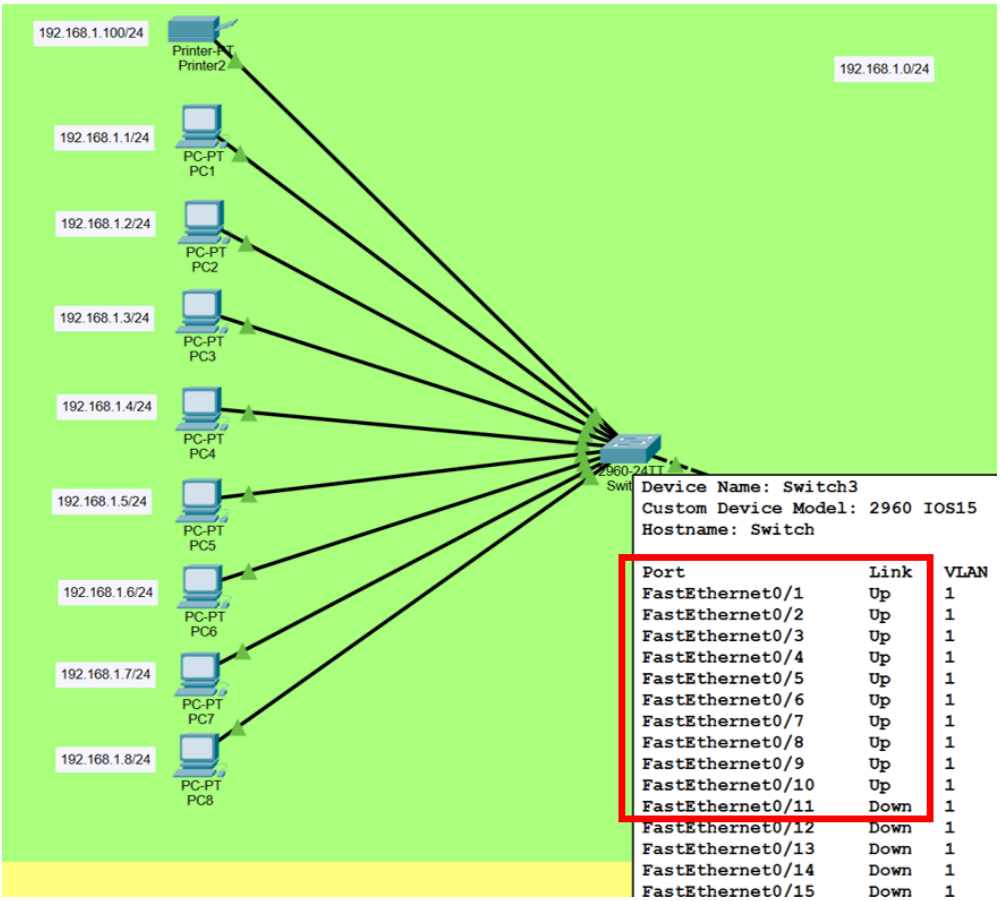

Рисунок 3.48 Порти комутатора

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0090.2B1E.0C3D
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
```

Рисунок 3.49 Додавання MAC адреса ПК до порта комутатора

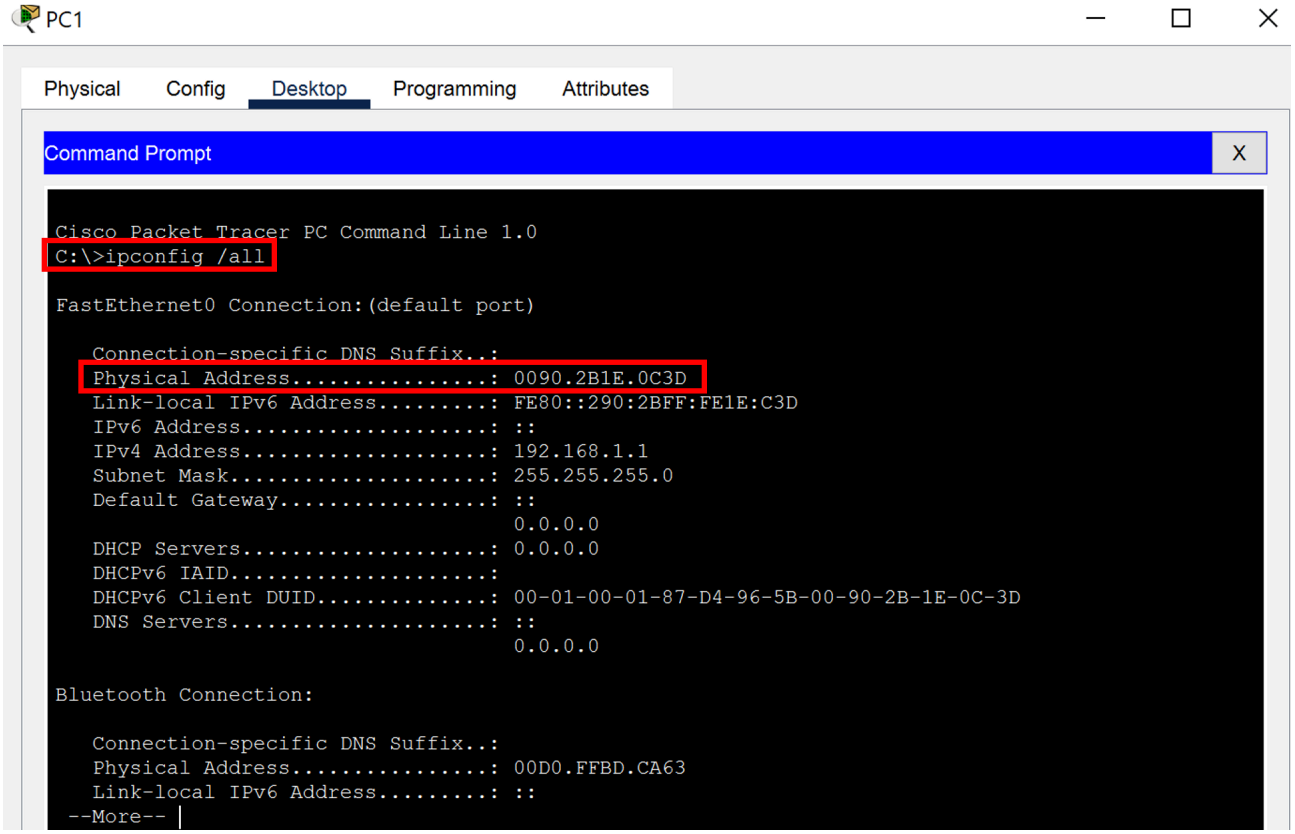

Рисунок 3.50. MAC адрес ПК1

Ті самі дії ми проробляємо з усіма іншими пристроями підключеними до комутатора. Детальну увагу приділяємо 10-му порту він виходить за межі і підключається до Multilayer Switch, що у свою чергу поєднує всі інші пристрої мережі. Так як це звичайний робочий ПК, ми робимо під'єднання всіх інших пристроїв, окрім принтерів. Для цього прорахуємо їх кількість і проробимо ті самі дії, але вже додаючі всі пристрої (Рис. 51).

```
Switch(config)#interface FastEthernet0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 12
Switch(config-if)#switchport port-security mac-address 0000.0CB9.8C55
Switch(config-if)#switchport port-security mac-address 0001.4306.6AD2
Switch(config-if)#switchport port-security mac-address 0030.A338.BA4D
```

Рисунок 3.51 Додавання на 10 порт MAC адреси всіх пристроїв мережі

А також блокуємо повністю доступ до інших портів (Рис. 52).

```
Switch(config)#interface range FastEthernet0/11-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 0
```

Рисунок 3.52 Блокування всіх інших портів комутатора

Відповідно при спробі підключення пристрою, все буде мати вигляд приблизно наступний (Рис. 53).

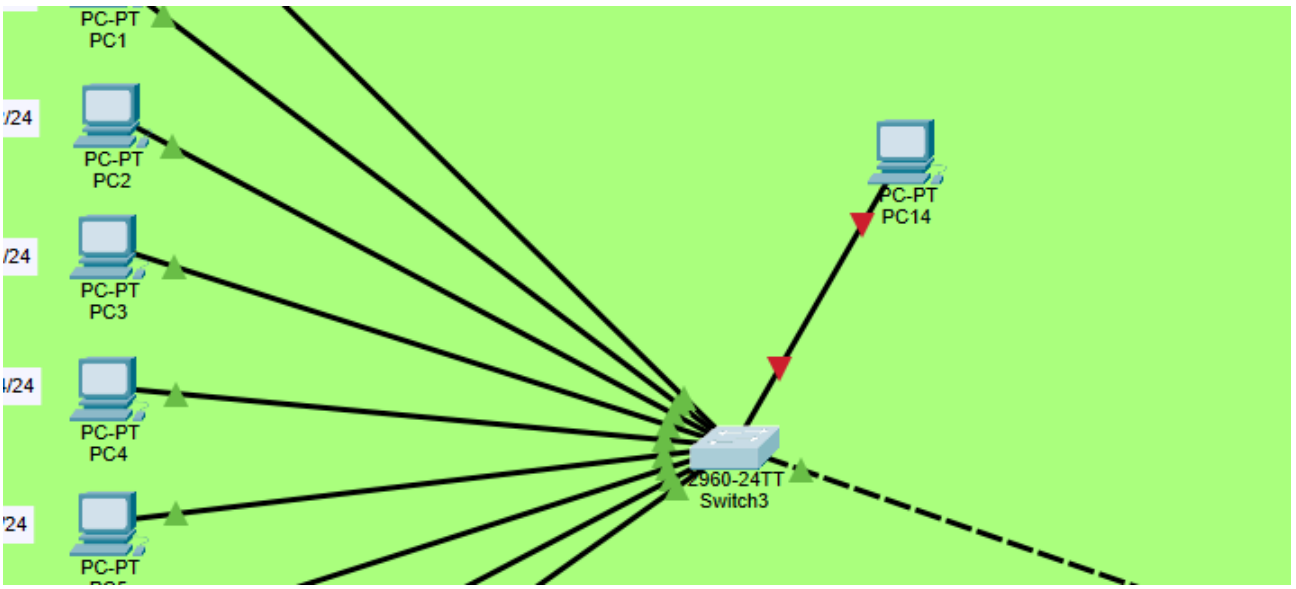

Рисунок 3.53. Демонстрація навдалого підключення до виключеного порта

Проводимо ті самі налаштування для кожної сигментованої частини, але переходячи до частини з комп’ютерами деректорів, Switch0, отримує тільки доступ до MAC адрес самих комп'ютерів директорів, комп'ютера адміністратора. А також серверів. Всі інші пристрої не будуть мати доступу (Рис. 54).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 00E0.A3BD.E71E
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#
```

Рисунок 3.54. MAC фільтрація комутатора зони директорів

При спробі надсилання пакетів, зі станцій звичайних співробітників, трафік блокується і не іде до комп'ютерів директорів (Рис. 55).

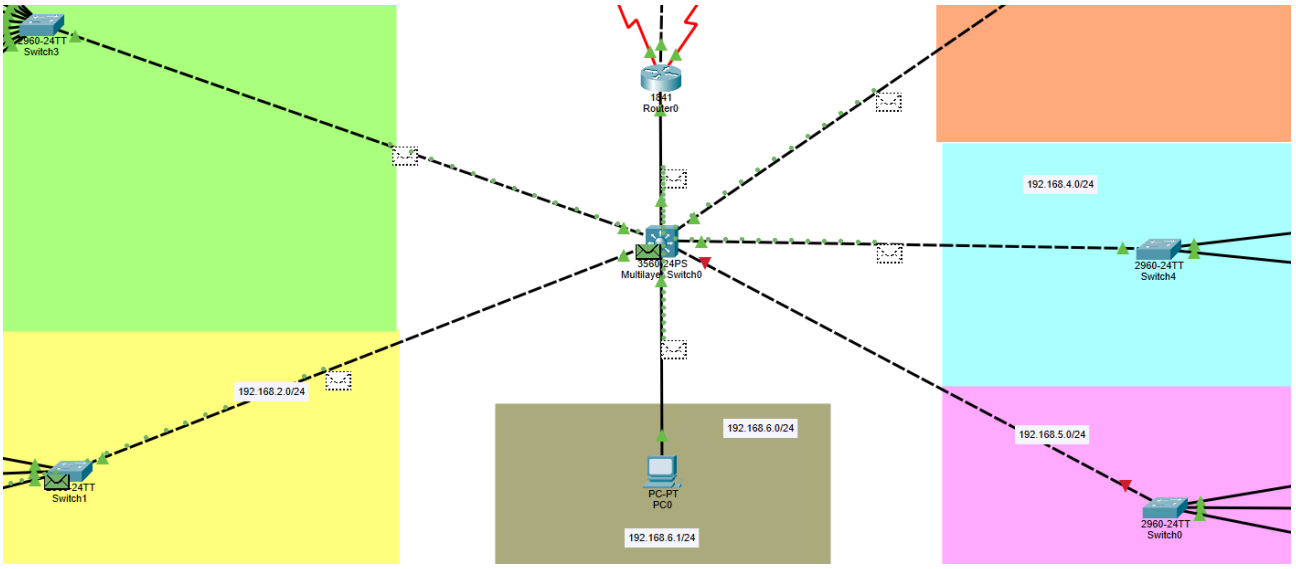

Рисунок 3.55 Демонстрація навдалої маршрутизації пакетів з зони звичайних працівників, до зони директорів

3.4 Впровадження рішень захисту першого рівня (рівень кінцевих пристроїв)

Залишилось реалізувати і впровадити рішення 1-го рівня.

Головним пунктом буде опис програми підвищення рівня обізнаності. Вона буде включати впровадження регулярних семінарів, навчань та кампаній з підвищення обізнаності. Тобто кожен тиждень, ефективним буде понеділок, працівники будуть відпочившими і краще запам’ятовувати інформацію, що допоможе на практиці протягом робочого тижня. Але звернемо увагу, не можна ставити зустрічі по навчанню на самий ранок, бо це забере ефективність запам’ятовування із-за можливих сонливих ранкових уподобань. Оптимальним часом, буде зустріч з 12 до 14 години для, перед обідньою перервою.

Ми визначились з форматом підвищення рівня обізнаності і часом коли це краще проводити. Тепер перейдемо до самих семінарів. По перше розділимо заняття на два типи, проходження різноманітних інтернет курсів, і усне подання інформації від запрошеного спеціаліста. Більш детально розглянемо проходження інтернет курсів. Обов’язково курси будуть проходитись в один визначений час, з певною внутрішньою системою оцінювання, для деяких платформ, під наглядом спеціаліста, за для уникнення халатності зі сторони працівників! Прекрасними для такого виду підвищення кваліфікації, є безкоштовна платформа з непоганим наповненням і різноманітністю курсів “Дія Освіта” у якій у першу чергу можна розглянути курс під назвою “Кібергігієна” І ще одним прекрасним рішенням, буде заключення міжнародної співпраці, з професійною освітньою платформою “Cisco”. Що стосовно усних семінарів, пропонується запрошення спеціалістів з кібербезпеки, які будуть надавати матеріали для обов’язкового запам’ятовування і розуміння.

Що стосується нашого підприємства, такого як банк. Є максимально важливим підвищення обізнаності серед працівників. Саме тому, необхідно впровадити Що місячне поглиблене і спеціалізоване навчання працівників, кожен 4 тиждень замість звичайних курсів. Поєднання викладення усного від спеціаліста і письмового тесту. Ане інформація яка буде подаватися, буде включаючи, переказ певної наукової літератури, переказ NIST стандартів, розглядання конкретних проблем і випадків, але зауважимо, все, що стосується тематики кібергігієни і кіберзагроз, на нашому підприємстві.

Детальніше оглянемо, ази і основу того, що саме можна вписати у курс підвищення рівня обізнаності працівників і що є обов’язковим при отриманні будь-якої посади у компанії, у нашому випадку у банку. Розкриємо умовні застереження від соціальної інженерії:

- Уважно перевіряйте правопис адрес сайтів.
- Не піддавайтеся емоційним закликам і не переходьте на сайти/фото/відео одразу. Порахуйте до 10 і згадайте, що це може бути прикладом соціальної інженерії.
- При введенні логіну/паролю на сайтах звертайте увагу на будь-які незвичайні зміни у вигляді сторінок. Якщо щось викликає підозру, перевірте оригінальність ресурсу ще раз.
- Будьте критичними до електронних листів, особливо до посилань від незнайомих відправників повідомлень.

Впровадження такої структури навчання, зможе кардинально підвищити рівень обізнаності працівників. І значно знизити ризики фішингу і соціальної інженерії у межах нашої компанії.

Переходимо до захисту кінцевих пристроїв за допомогою антивірусів. Вибір продукту пав на акулу ринку ESET Endpoint Protection Advanced (Рис. 56), він буде оптимальним рішенням для банківського сектору.

Рисунок 3.56 Антивірус ESET

ESET Endpoint Protection Advanced представляє собою ідеальне поєднання високого рівня безпеки та економічної ефективності для банківських установ. Цей антивірусний продукт має понад 30-річний досвід у сфері кібербезпеки [17] та демонструє винятково легку архітектуру, яка практично не сповільнює роботу критичних банківських додатків. Унікальна система аналізу поведінки DeepGuard аналізує активність додатків у реальному часі та виявляє підозрілу поведінку навіть від невідомих загроз, що особливо ефективно проти сучасних банківських троянів та програм-вимагачів. Рішення має рекордну кількість найвищих нагород від провідних незалежних лабораторій тестування, включаючи сертифікати VB100 та рейтинги ADVANCED+, що підтверджує його надійність та стабільність роботи.

Важливим фактором вибору ESET є його широке впровадження в державному секторі України, наявність локальної підтримки та розуміння специфіки вітчизняного фінансового ринку. Продукт забезпечує відповідність вимогам НБУ щодо кібербезпеки банківських установ та пропонує відмінне

співвідношення ціна-якість з гнучкою ліцензійною моделлю. Централізована консоль управління ESET PROTECT дозволяє ефективно керувати безпекою тисяч робочих станцій з єдиної точки, що значно знижує операційні витрати. Додатково рішення включає двофакторну аутентифікацію для адміністраторів, захист мобільних пристроїв та забезпечує швидку технічну підтримку через мережу сертифікованих партнерів в Україні.

Переходимо до двофакторної аутентифікації. Перший фактор захисту на кожному пристрої встановлено за вбудованою структурою паролю. Він легко налаштовується і використовується при спробі розблокування пристроя. Цей пароль гарно і надійно буде захищати комп’ютери і планшети працівників від третіх осіб.

Але для підвищення рівня захищеності впровадимо терміни на які будуть дійсні паролі. Гарним варіантом буде 1 місячний термін. Виданий випадковою генерацією пароль, який буде складатись з англійських літер, цифр і спеціальних символів. Кожен працівник зобов’язаний буде запам’ятати цей пароль і використовувати для входу у систему протягом 1 місяця, пслся чого пароль буде оновлено.

Бувають такі ситуації, коли зловмисники зламують, або дізнаються паролі. На такі випадки вводмо 2-гий фактор захисту, який буде покладаний на біометрію, унікальні риси кожної людини. Найпростішим і найдешевшим варіантом буде використання відбитку пальця. У випадку з планшетами, ці пристрої підтримують цю функцію у вбудованому форматі Touch ID. А щодо ПК, ми впровадимо спеціалізовані настільні USB-зчитувачи відбитків пальців (Рис. 57), які впровадимо на кожному комп’ютері.

Рисунок 3.57 Настільні USB-зчитувачи відбитків пальців

3.5 Результати розробки комплексної моделі захисту мережевої інфраструктури

Система рішень впроваджених у попередніх підрозділах забезпечить високий рівень безпеки при збереженні зручності для щоденної роботи банківських співробітників та відповідатиме вимогам регуляторів у сфері фінансових послуг.

Результатом впровадження всіх рішень буде дійсна і готова до роботи мережева інфраструктура банкового відділення (Рис. 58). Яка буде включати наступні рішення:

- Двофакторну аутентифікацію на кожному ПК і планшеті мережі з біометричним доступом
- Антивірусне програмне забезпечення ESET на кожному ПК і планшеті мережі

- MAC фільтрація на кожному комутаторі
- IP сегментація всієї мережі
- Міжмережні екрани на кретичних точках
- Демілітарізована зона
- IPS і IDS системи
- VPN тунелювання

А також побудована структура підвищеня обізненості працівників.

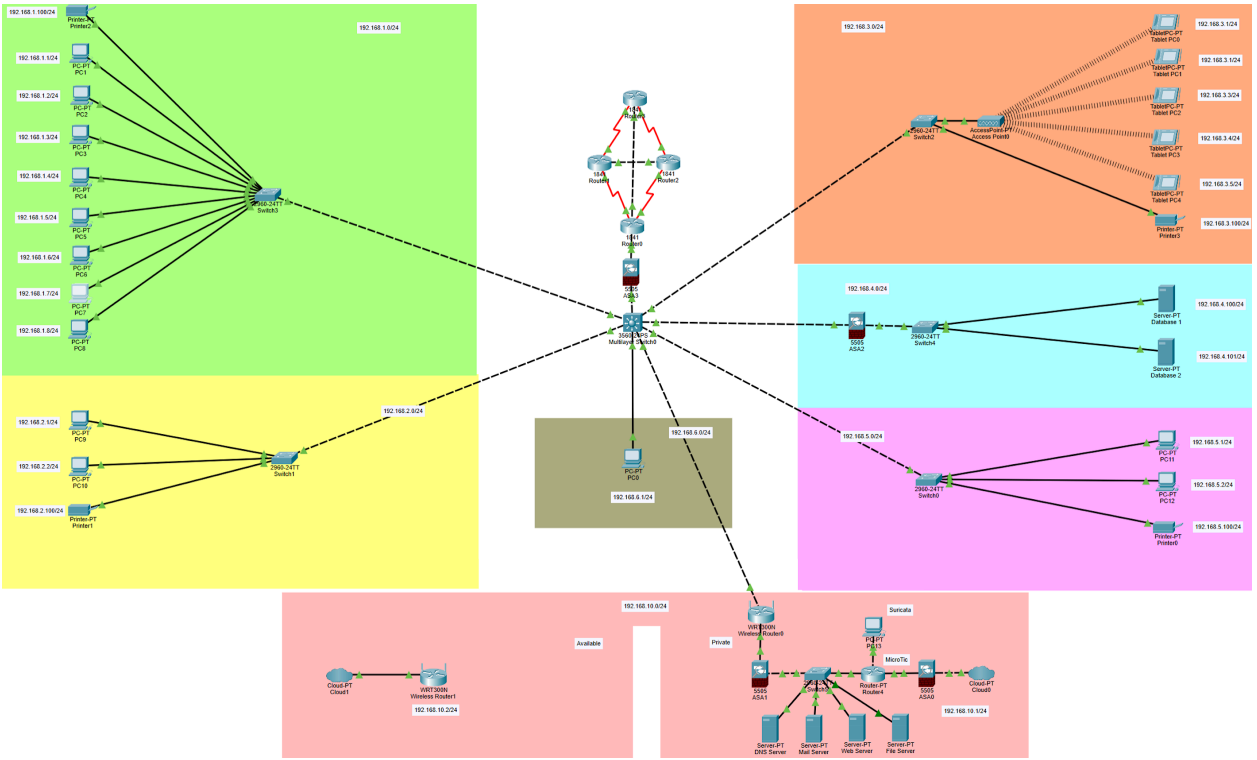

Рисунок 3.58 Захищена мережева інфраструктура банкового відділення

Відповідно до реалізованої моделі захисту мережевої інфраструктури, зобразимо схему моделі захисту (Рис. 59).

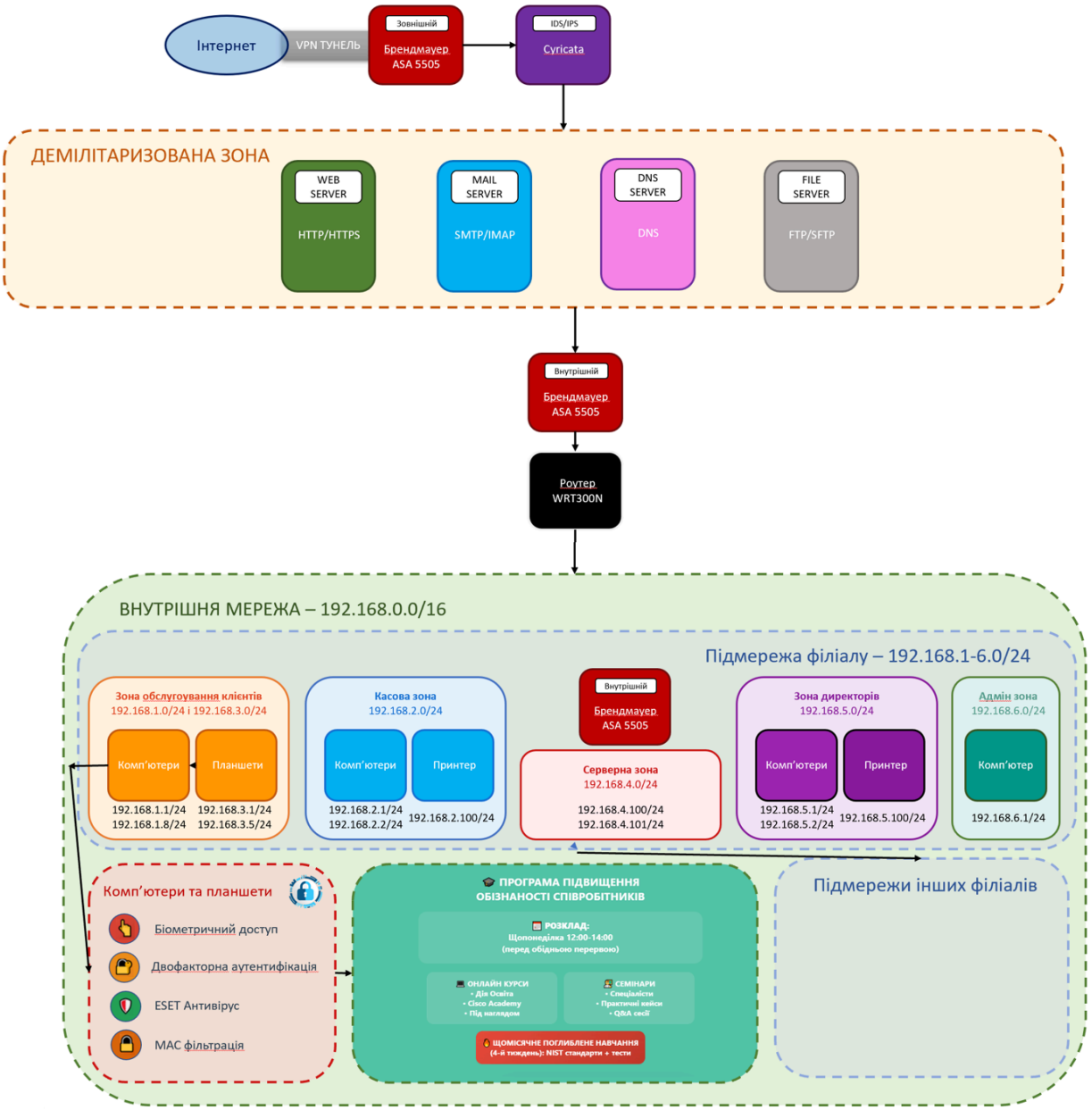

Рисунок 3.59 Схема моделі захисту мережі

3.6 Адаптація комплексної моделі захисту для різних галузей

У підрозділі 3.1 було детально розроблено та впроваджено комплексну модель захисту мережевої інфраструктури на прикладі банківського відділення ПриватБанку №91. Вибір банківської сфери як базового об'єкта дослідження був обумовлений кількома ключовими факторами, що роблять її ідеальним еталоном для розробки універсальної моделі кібербезпеки.

По-перше, банківський сектор характеризується найвищими вимогами до інформаційної безпеки серед усіх галузей. Фінансові установи обробляють критично важливу інформацію - персональні та фінансові дані клієнтів, здійснюють мільйони транзакцій щодня, та є постійною ціллю для кіберзлочинців через високу вартість інформаційних активів. Це змушує банки впроваджувати найсучасніші та найнадійніші засоби захисту.

По-друге, банківська галузь підлягає суворому державному регулюванню у сфері кібербезпеки. Вимоги Національного банку України.

По-третє, складність банківської IT-інфраструктури включає різноманітні типи пристроїв, мережевих сегментів, інтеграцій з зовнішніми системами та різні рівні доступу користувачів. Така багатокомпонентна архітектура дозволяє продемонструвати ефективність захисних механізмів в умовах максимальної складності.

Розроблена базова модель успішно інтегрує всі сучасні засоби кібербезпеки - від фізичного захисту до систем штучного інтелекту для виявлення загроз, створюючи комплексну, багаторівневу архітектуру захисту. Медичні установи працюють з персональними даними пацієнтів та потребують відповідності HIPAA стандартам [19] (Таб. 3.3, 3.4). Освітні заклади мають справу з захистом неповнолітніх та контролем контенту (Таб. 3.5, 3.6). Виробничі підприємства інтегрують IT та OT системи [20] (Таб. 3.7, 3.8), а телекомунікаційні компанії захищають критичну комунікаційну інфраструктуру (Таб. 3.9, 3.10). Юридичні фірми зберігають конфіденційну інформацію клієнтів, що потребує особливих засобів захисту професійної таємниці (Таб. 3.1, 3.2). Тому виникає необхідність адаптації універсальної моделі під специфічні потреби різних галузей, зберігаючи при цьому високий рівень захисту та ефективність базової архітектури.

Базова модель захисту (банківський сектор):

- Двофакторна аутентифікація на кожному ПК і планшеті мережі з біометричним доступом

- Антивірусне програмне забезпечення ESET на кожному ПК і планшеті мережі
- MAC-фільтрація на кожному комутаторі
- IP-сегментація всієї мережі
- Міжмережеві екрани на критичних точках
- Демілітаризована зона (ДМЗ)
- IPS і IDS системи
- VPN-тунелювання
- Структура підвищення обізнаності працівників

Таблиця № 3.1

Характеристика сфери юриспруденції

Характеристика	Опис
Специфіка галузі	Робота з конфіденційною інформацією клієнтів, договорами та правовими документами. Необхідність дотримання принципів *attorney-client privilege* та професійної таємниці.
Ключові активи	Юридичні документи, персональні дані клієнтів, договори, судові справи, інтелектуальна власність, конфіденційна ділова інформація.
Основні загрози	Витік конфіденційної інформації клієнтів, промислове шпигунство з боку конкурентів, порушення професійної етики, компрометація доказової бази.

Таблиця № 3.2

Додаткові компоненти захисту для сфери юриспруденції

Додаткові компоненти до базової моделі	Технічна реалізація	Обґрунтування
DLP (Data Loss Prevention) системи	• Встановлення DLP-агентів на всі робочі станції юристів • Налаштування правил класифікації документів за рівнем конфіденційності • Блокування передачі документів через неавторизовані канали (особисті email, USB) • Моніторинг друку конфіденційних документів • Контроль копіювання текстів у буфер обміну	Критично важливо для запобігання витоку конфіденційної правової інформації та персональних даних клієнтів. Забезпечує дотримання професійних етичних стандартів
Журналювання всіх дій з документами (Chain of Custody)	• Фіксація часу створення, редагування та доступу до документів • Ідентифікація користувача, що здійснював дії з документом • Збереження контрольних сум файлів для виявлення несанкціонованих змін • Автоматичне створення аудиторського сліду для судових справ • Цифрові підписи для критичних документів	Забезпечує юридичну достовірність документів та можливість відстеження історії змін. Необхідно для підтримання доказової бази в судових процесах

Таблиця № 3.3

Характеристика сфери охорони здоров'я

Характеристика	Опис
Специфіка галузі	Обробка персональних даних пацієнтів та критично важливої медичної інформації. Необхідність забезпечення безперервності роботи медичних систем
Ключові активи	Електронні медичні карти, результати аналізів, медичні зображення, персональні дані пацієнтів, дослідницькі дані, системи життєзабезпечення
Основні загрози	Компрометація медичних даних пацієнтів, порушення конфіденційності, атаки на системи життєзабезпечення, медичне шахрайство

Таблиця № 3.4

Додаткові компоненти захисту для сфери охорони здоров'я

Додаткові компоненти до базової моделі	Технічна реалізація	Обґрунтування
HIPAA-сумісні системи захисту медичних даних	• Шифрування всіх медичних баз даних стандартом AES-256 • Рольова модель доступу (лікар/медсестра/адміністратор/пацієнт) • Автоматичне логування доступу до електронних медичних карт • Анонімізація даних для дослідницьких цілей	Відповідність вимогам Health Insurance Portability and Accountability Act (HIPAA) для забезпечення конфіденційності

	• Резервування критичних медичних систем	медичної інформації пацієнтів.

Таблиця № 3.5

Характеристика сфери освіти

Характеристика	Опис
Специфіка галузі	Робота з персональними даними студентів та потреба у безпечному навчальному середовищі з контролем доступу до цифрових ресурсів
Ключові активи	Персональні дані студентів, академічні записи, результати іспитів, дослідницькі дані, освітній контент, системи дистанційного навчання
Основні загрози	Доступ до неприйнятного контенту, кібербулінг, порушення академічної доброчесності, витік персональних даних студентів

Таблиця № 3.6

Додаткові компоненти захисту для сфери освіти

Категорія компонента	Технічна реалізація	Обґрунтування
1	2	3
Контент-фільтрація	Блокування сайтів з неприйнятним контентом (насильство, порнографія) • Фільтрація за категоріями контенту • Білі списки освітніх ресурсів • Батьківський контроль для молодших класів	Забезпечення безпечного освітнього середовища та відповідність віковим обмеженням. Захист неповнолітніх від

	• AI-аналіз контенту в реальному часі	шкідливого контенту

Продовження табл. 3.6

1	2	3
Часові обмеження доступу	• Обмеження доступу до соціальних мереж під час занять • Різні права доступу для навчального та позанавчального часу • Автоматичне блокування доступу в неробочі години • Персоналізовані профілі для різних груп користувачів • Інтеграція з розкладом занять	Підвищення ефективності навчального процесу та контроль використання мережевих ресурсів відповідно до розкладу навчального закладу

Таблиця № 3.7

Характеристика сфери виробництва

Характеристика	Опис
Специфіка галузі	Інтеграція IT і OT систем, захист виробничих процесів, забезпечення безперервності виробництва

Ключові активи	Промислові системи управління (SCADA, PLC), IoT датчики, виробничі дані, технологічні процеси, інтелектуальна власність
Основні загрози	Промисловий саботаж, зупинка виробництва, крадіжка технологій, атаки на критичну інфраструктуру

Таблиця № 3.8

Додаткові компоненти захисту для сфери виробництва

Додаткові компоненти до базової моделі	Технічна реалізація	Обґрунтування
1	2	3
Моніторинг IoT пристроїв та датчиків	• Виявлення аномальної поведінки датчиків та контролерів • Моніторинг мережевого трафіку промислових протоколів • Автоматична ізоляція скомпрометованих пристроїв • Оновлення прошивок IoT пристроїв через безпечні канали • Інвентаризація всіх підключених пристроїв	Захист промислових IoT пристроїв на виробничих лініях від кіберзагроз та забезпечення стабільності виробничих процесів
OT (Operational Technology) захист	• Промислові міжмережеві екрани для OT мереж	Спеціалізований захист

	• Deep Packet Inspection для промислових протоколів (Modbus, DNP3) • Моніторинг цілісності конфігурацій промислового обладнання • Резервування критичних систем управління • Антивірусний захист для промислових систем	промислових систем управління (SCADA, PLC, HMI) від цільових атак на виробничу інфраструктуру

Продовження табл. 3.8

1	2	3
Air Gap ізоляція	• Окрема мережева інфраструктура для критичних процесів • Захищені шлюзи для обміну даними між IT та OT • Процедури безпечного оновлення ізольованих систем • Контроль знімних носіїв інформації • Фізична ізоляція критичних систем	Фізичне відокремлення критичних виробничих систем від корпоративної мережі для максимального захисту від зовнішніх атак

Таблиця № 3.9

Характеристика сфери телекомунікацій

Характеристика	Опис

Специфіка галузі	Захист телекомунікаційної сигналізації та абонентських даних від специфічних атак на телекомунікаційну інфраструктуру
Ключові активи	Телекомунікаційна інфраструктура, абонентські дані, сигналізація SS7/Diameter, біллінгові системи, мережеве обладнання
Основні загрози	Перехоплення комунікацій, SS7 атаки, SIM-swapping, DDoS на мережеву інфраструктуру, порушення конфіденційності зв'язку

Таблиця № 3.10

Додаткові компоненти захисту для сфери телекомунікацій

Додаткові компоненти до базової моделі	Технічна реалізація	Обґрунтуванн
SS7/Diameter Firewall	• Фільтрація сигнальних повідомлень SS7 та Diameter Виявлення аномальних сигнальних потоків • Блокування спроб перехоплення SMS та дзвінків • Захист від атак на роумінгову сигналізацію	Спеціалізований захист телекомунікаційної сигналізації від атак на протоколи SS7 та Diameter, що використовуються для перехоплення комунікацій

	• Моніторинг міжнародного трафіку	
Захист від SIM-swapping та SS7 атак	• Моніторинг геолокації абонентів для виявлення аномалій • Додаткова автентифікація при критичних операціях • Блокування несанкціонованих location update запитів • Система сповіщень про підозрілу активність • Виявлення підозрілих запитів на зміну SIM-карти	Комплексна система виявлення та запобігання атакам на SIM-карти абонентів та експлуатації вразливостей протоколу SS7

Висновки за розділом №3

У третьому розділі було успішно розроблено та впроваджено комплексну модель захисту мережевої інфраструктури для організації підприємств на прикладі банківського відділення, а також здійснено її адаптацію для різних галузей.

Було здійнено проектування та впровадження комплексної моделі захисту мережевої інфраструктури" реалізовано повний цикл створення захищеної мережевої архітектури банківського відділення ПриватБанку №91. Здійснено детальну сегментацію мережі з розподілом на сім функціональних зон: касова зона (192.168.2.0/24), зона обслуговування юридичних та фізичних осіб (192.168.1.0/24), зона обслуговування фізичних осіб з планшетами (192.168.3.0/24), серверна зона (192.168.4.0/24), зона директорів

(192.168.5.0/24), адміністративна зона (192.168.6.0/24) та зона підключення до інтернету (192.168.10.0/24).

Впроваджено багаторівневу систему захисту за принципом "defense in depth", що включає три рівні безпеки. На третьому рівні (маршрутизатори та міжмережевий обмін) встановлено периметрові, внутрішні та сегментні міжмережеві екрани, створено демілітаризовану зону з публічними сервісами, інтегровано систему SELKS з підтримкою IPS/IDS функціональності Suricata та налаштовано VPN-тунелювання з шифруванням AES-256. На другому рівні (комутатори та мережева інфраструктура) реалізовано MAC-фільтрацію на всіх комутаторах з обмеженням доступу за унікальними ідентифікаторами пристроїв та політики контролю доступу з диференційованими правами для різних категорій користувачів. На першому рівні (кінцеві пристрої) впроваджено антивірусний захист ESET Endpoint Protection Advanced, двофакторну аутентифікацію з біометричним доступом та програму підвищення кібер-обізнаності працівників.

А також здійснено. Адаптацію комплексної моделі захисту для різних галузей" проведено комплексний аналіз специфічних потреб п'яти ключових галузей та розроблено відповідні модифікації базової моделі. Для юридичної сфери додано DLP-системи для запобігання витоку конфіденційної інформації клієнтів та системи журналювання дій з документами для забезпечення chain of custody. У сфері охорони здоров'я інтегровано HIPAA-сумісні системи захисту медичних даних з шифруванням AES-256 та рольовою моделлю доступу. Для освітньої галузі впроваджено контент-фільтрацію та часові обмеження доступу для забезпечення безпечного навчального середовища. У виробничій сфері додано моніторинг IoT пристроїв, OT-захист промислових систем управління та Air Gap ізоляцію критичних процесів. Для телекомунікаційної галузі розроблено SS7/Diameter Firewall та системи захисту від SIM-swapping атак.

Створено систему кількісних метрик для оцінки ефективності галузевих адаптацій, що показала варіацію загальної вартості впровадження від 115% (освіта) до 140% (виробництво) відносно базової моделі при забезпеченні рівня

захисту даних від 85% до 98% залежно від галузевої специфіки. Час виявлення інцидентів варіюється від 3 хвилин (телекомунікації) до 15 хвилин (освіта), а вплив на продуктивність становить від -1% до -7%.

Розроблена методологія адаптації базової моделі забезпечує гнучкість архітектури безпеки та можливість масштабування для будь-якої галузі з урахуванням специфічних регуляторних вимог, унікальних загроз та обмежених ресурсів на кібербезпеку. Практична значущість результатів полягає у створенні універсального підходу до проектування захищеної мережевої інфраструктури, який може бути адаптований та впроваджений в організаціях різного профілю з мінімальними модифікаціями та максимальною ефективністю захисту.

ВИСНОВОК

У результаті виконання кваліфікаційної роботи досягнуто поставленої мети підвищення ефективності захисту мережевої інфраструктури підприємства шляхом розробки та впровадження комплексної моделі захисту з інтеграцією технічних і програмних засобів кібербезпеки.

Перше завдання щодо аналізу сучасних засобів та методів забезпечення кібербезпеки мережевої інфраструктури повністю реалізовано. Проведено системний огляд технічних рішень та програмних засобів захисту з практичною демонстрацією їх функціоналу на прикладі банківського відділення ПриватБанк №91. Систематизовано засоби захисту за трирівневою моделлю безпеки: першого рівня (антивірусні рішення ESET, двофакторна аутентифікація з біометричним захистом, програми підвищення кібер-обізнаності), другого рівня (MAC-фільтрація, IP-сегментація мережі) та третього рівня (міжмережеві екрани, ДМЗ, системи IDS/IPS, VPN-технології), що забезпечило науково-обґрунтовану основу для подальшого проектування комплексної моделі захисту.

Друге завдання з оцінки ризиків та розробки моделі загроз інформаційної безпеки успішно виконано через створення комплексної системи оцінки ризиків із побудовою трьох матриць безпеки (уразливостей, загроз та контролю) з використанням 4-бальної шкали взаємозв'язку. Розроблено детальну модель загроз за чотирма категоріями (загальні, мережеві, загрози прикладного ПЗ та ОС) із класифікацією за тріадою CIA та модель порушника з класифікацією 16 типів потенційних атакуючих, що охоплює як внутрішні (9 категорій), так і зовнішні загрози (7 категорій).

Третє завдання щодо розробки комплексної моделі захисту мережевої інфраструктури реалізовано через створення структурованої топології з 7 функціональними сегментами (касова зона, зони обслуговування юридичних та фізичних осіб, серверна зона, зона директорів, адміністративна зона, зона підключення до інтернету) та впровадження багаторівневої системи захисту з інтеграцією технічних і програмних засобів безпеки, включаючи периметрові та

внутрішні міжмережеві екрани, систему SELKS з IPS/IDS функціональністю Suricata, VPN-тунелювання з AES-256 шифруванням та комплексну програму підвищення обізнаності працівників.

Розроблена комплексна модель захисту забезпечує багаторівневий захист інформаційних активів через логічну сегментацію мережі, диференційований контроль доступу та централізований моніторинг подій безпеки, що демонструє ефективність інтегрованого підходу до кібербезпеки. Додатково здійснено адаптацію базової моделі для п'яти ключових галузей (юриспруденція, охорона здоров'я, освіта, виробництво, телекомунікації) з розробкою галузево-специфічних компонентів захисту від DLP-систем до SS7/Diameter Firewall.

Практична реалізація моделі на прикладі банківського відділення ПриватБанк №91 підтверджує можливість адаптації розроблених рішень до реальних умов функціонування фінансових установ з урахуванням специфічних вимог до безпеки та регуляторних стандартів НБУ. Запропонована методологія матричного аналізу "актив-уразливість-загроза-контроль" дозволяє здійснювати кількісну оцінку рівня ризику та ефективності заходів захисту.

Р езультати дослідження розширюють науково-методичну базу проектування захищених мережевих інфраструктур підприємств та можуть бути використані для розробки стандартів захисту критично важливої інформації у фінансовому секторі та інших галузях. Створено універсальний підхід до проектування захищеної мережевої інфраструктури, який може бути адаптований в організаціях різного профілю з мінімальними модифікаціями та максимальною ефективністю захисту.

Розроблена модель відповідає сучасним викликам кібербезпеки та забезпечує необхідний рівень захисту для протидії еволюціонуючим кіберзагрозам, що підтверджує актуальність та своєчасність проведеного дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Cybersecurity Ventures. (2024). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

2 IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation. https://www.ibm.com/reports/data-breach

3 Check Point Research. (2024). Cyber Security Report 2024: Global threat landscape analysis. Check Point Software Technologies Ltd.

4 Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Communications Inc.

5 Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Communications Inc. https://www.verizon.com/business/resources/reports/dbir/

6 Cybersecurity Ventures. (2023). 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. `https://cybersecurityventures.com/cybersecurity-almanac-2024/

7 IBM. (2024). What is a Data Breach? Security incident analysis and prevention strategies. https://www.ibm.com/think/topics/data-breach

8 Kaspersky Lab. (2023). How Antivirus Software Works: Detection methods and behavioral analysis. https://www.kaspersky.com/resource-center/definitions/antivirus

9 Fortinet. (2024). Network Segmentation Best Practices: Implementation guide for enterprise security. https://www.fortinet.com/resources/cyberglossary/network-segmentation

10 Palo Alto Networks. (2023). Next-Generation Firewall Technology: Advanced threat protection strategies. Palo Alto Networks Inc.

11 Cisco Systems. (2023). DMZ Network Design: Creating secure buffer zones for enterprise networks. Cisco Systems Inc.

12 International Organization for Standardization. (2022). Information security management systems — Requirements (ISO Standard No. 27001:2022). https://www.iso.org/standard/73906.html

13 Державна служба спеціального зв'язку та захисту інформації України. (2023). Нормативні документи у сфері технічного захисту інформації: НД ТЗІ 1.1-002-99, ТЗІ 2.5-004-99. https://cip.gov.ua/

14 Suricata Community. (2024). Intrusion Detection and Prevention Systems: Real-time network monitoring documentation. Open Information Security Foundation.

15 SELKS Project. (2024). Suricata Elasticsearch Logstash Kibana Scirius: Integrated security platform. https://www.stamus-networks.com/open-source

16 Гнатюк, С. О., & Мохор, В. В. (2022). VPN-технології та шифрування трафіку в корпоративних мережах. Захист інформації, 24(3), 78-92.

17 ESET. (2024). ESET Endpoint Protection Advanced: Enterprise cybersecurity solution documentation. ESET, spol. s r.o.

18 Шестак, Я. В., & Щебланін, Ю. М. (2023). Біометричні системи аутентифікації: сучасні технології та методи. Інформаційні технології та кібербезпека, 5(2), 34-48.

19 U.S. Department of Health and Human Services. (2023). HIPAA Security Rule: Technical safeguards for protected health information. https://www.hhs.gov/hipaa/for-professionals/security/

20 Anderson, R., Bond, M., & Clayton, R. (2024). Cross-Industry Cybersecurity Framework: Sector-specific implementation strategies. Journal of Computer Security, 32(1), 112-138.

ДОДАТОК А

МОДЕЛЬ ЗАГРОЗ ІНФОРМАЦІЇ

1 Класифікація загроз

Згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, ТЗІ 2.5-004-99 за результатом впливу на інформацію та систему її обробки загрози поділяються на чотири класи [13]:

1. Порушення конфіденційності («К») інформації (отримання доступу до інформації з обмеженим доступом);

2. Порушення цілісності («Ц») інформації (повне або часткове знищення, викривлення, модифікація, нав’язування хибної інформації);

3. Порушення доступності («Д») інформації (часткова або повна втрата працездатності системи, блокування доступу до інформації);

4. Втрата спостереженості («С») або керованості системи обробки (порушення процедур ідентифікації та автентифікації користувачів та процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

За джерелом впливу загрози поділяються на:

- Загрози, обумовлені діями людини (викрадення, підміна, пошкодження інформації, паролів і атрибутів доступу, технічних та програмних засобів її обробки);
- Загрози, обумовлені технічними засобами (неякісні технічні та програмні засоби обробки інформації);
- Загрози, обумовлені стихійними факторами (пожежа, землетрус, повінь та ін.)

За характером впливу на ЗВІД загрози поділяються на:

- Активні;
- Пасивні.

За способом впливу на об’єкт атаки загрози поділяються на:

- Загрози з безпосереднім впливом на об’єкт атаки;
- Загрози з впливом на систему прав доступу;
- Загрози з опосередкованим впливом.

За використовуваним для атаки компонентом ЗВІД загрози поділяються на:

- Загрози, які використовують технічні засоби ЗВІД;
- Загрози, які використовують технологічну інформацію ЗВІД;
- Загрози, які використовують програмні засоби ЗВІД.

За засобами атаки загрози поділяються на:

- Загрози з використанням стандартного програмного забезпечення або технічних засобів;
- Загрози з використанням спеціально розробленого програмного забезпечення або технічних засобів.

За станом об’єкту атаки загрози поділяються на:

- Загрози на об’єкт атаки, який знаходиться в стані зберігання;
- Загрози на об’єкт атаки, який знаходиться в стані обробки.

2 Модель загальних загроз

Таблиця № А.1

Модель загальних загроз

Назва загрози	Опис загрози та можливі наслідки реалізації	Об’єкти загрози	Суб’єкти загрози	Можлива атака	Дестабілізуючі фактори	Вразливість, що може використовуватися	Тип загрози
1	2	3	4	5	6	7	8
Несанкціонований доступ до банківських даних клієнтів	Отримання зловмисниками доступу до персональних даних, фінансової інформації та алгоритмів аналізу, що може призвести до витоку, фінансових збитків та юридичних наслідків.	Бази даних клієнтів, касові системи, банківські термінали	Зловмисники, недобросовісні касири, банківські консультанти	Використання викрадених паролів, соціальна інженерія, маніпуляції з касовими системами	Недостатній контроль доступу, використання слабких паролів	Відсутність двофакторної автентифікації, недостатня сегментація мережі	Порушення конфіденційності («К»), Втрата спостереженості («С»)

Продовження табл. А.1

1	2	3	4	5	6	7	8
Шкідливе програмне забезпечення (віруси, трояни, шпигунські програми)	Інфікування інформаційної системи, що може призвести до втрати або зміни даних, витоку інформації, віддаленого контролю над системою	Касові та робочі станції, сервери, планшети консультантів, комп’ютери директорів та адміна	Хакери, внутрішні користувачі (недбалість)	Впровадження шкідливого ПЗ через електронну пошту, флеш-накопичувачі, вразливі веб-сайти	Відсутність оновлень, недбале ставлення працівників	Використання старих версій ПЗ, відсутність антивірусного захисту	Порушення конфіденційності («К»), Порушення цілісності («Ц»), Втрата спостережності («С»)
Викрадення або пошкодження обладнання	Фізичне знищення або крадіжка серверів, робочих станцій, носіїв даних, що може призвести до витоку конфіденційної інформації листів	Серверна, касова зона, зона обслуговування клієнтів	Зловмисники, недобросовісні працівники	Фізичний доступ до приміщень, крадіжка, вандалізм	Відсутність відеоспостереження, слабка охорона	Відсутність контролю фізичного доступу, недостатній рівень безпеки	Порушення конфіденційності («К»), Порушення доступності («Д»)

Продовження табл. А.1

1	2	3	4	5	6	7	8
Інсайдерська загроза	Несанкціоноване розголошення або передача конфіденційної інформації працівниками	Бази даних, алгоритми, комерційна таємниця	Власні працівники	Копіювання інформації, передача конкурентам	Низький рівень контролю персоналу, відсутність моніторингу активності	Відсутність політик безпеки, недостатній контроль за діяльністю персоналу	Порушення конфіденційності («К»), Втрата спостережності («С»)
Аварійні ситуації (пожежа, затоплення, збої електромережі)	Фізичне пошкодження серверного обладнання, втрата даних	Серверна, офісне приміщення	Природні фактори	Виникнення пожежі, затоплення, перебої електроживлення	Відсутність системи резервного живлення, пожежної безпеки	Відсутність бекапів, недостатній рівень фізичного захист	Порушення доступності («Д»), Порушення цілісності («Ц»)

Продовження табл. А.1

1	2	3	4	5	6	7	8
Шахрайські фінансові операції	Несанкціоновані фінансові транзакції, підробка платіжних документів, маніпуляції з готівкою	Касові системи, банківські термінали	Клієнти-шахраї, недобросовісні касири, зовнішні зловмисники	Підробка документів, клонування платіжних карток, фіктивні переказі	Недостатній контроль касових операцій, слабка перевірка документів	Відсутність двофакторної автентифікації, недостатній контроль за касирами	Порушення конфіденційності («К»), Порушення цілісності («Ц»)

3 Модель мережевих загроз

Таблиця № А.2

Модель мережевих загроз

Назва загрози	Опис загрози та можливі наслідки реалізації	Об’єкти загрози	Суб’єкти загрози	Можлива атака	Дестабілізуючі фактори	Вразливість, що може використовуватися	Тип загрози
1	2	3	4	5	6	7	8

Продовження табл. А.2

1	2	3	4	5	6	7	8
Перехоплення мережевого трафіку (Sniffing)	Зловмисники можуть перехоплювати пакети даних, що передаються мережею, отримуючи доступ до конфіденційної інформації (паролі, фінансові дані)	Мережеві пристрої, сервери, робочі станції	Хакери, внутрішні зловмисники	Використання пакетних аналізаторів (Wireshark, tcpdump)	Відсутність шифрування трафіку	Використання незашифрованих протоколів (HTTP, FTP, Telnet)	Порушення конфіденційності («К»), Втрата спостережності («С»)
Атака "Людина посередині" (MITM)	Зловмисник вставляється між клієнтом і сервером, модифікує або записує дані	Сервери, мережеві пристрої	Хакери, співробітники	DNS Spoofing, ARP Spoofing, SSL Stripping	Відсутність перевірки сертифікатів, слабкі налаштування безпеки	Відсутність шифрування, використання підроблених сертифікатів	Порушення конфіденційності («К»), Порушення цілісності («Ц»)
DDoS-атака	Масове перевантаження мережевих ресурсів, що призводить до недоступності системи	Сервери, маршрутизатори, брандмауери	Хакерські угруповання, конкуренти	Використання ботнетів, SYN Flood, UDP Flood	Відсутність системи захисту від DDoS	Відсутність балансувальників навантаження, низька пропускна здатність мережі	Порушення доступності («Д»)

Продовження табл. А.2

1	2	3	4	5	6	7	8
Несанкціонований доступ до мережі	Злом локальної або Wi-Fi-мережі з подальшим викраденням даних або зміною конфігурації систем	Wi-Fi-роутери, комутатори, сервери	Зловмисники, недобросовісні співробітники	Використання вразливих протоколів безпеки (WEP, WPA), підбір паролів	Використання слабких паролів, відсутність сегментації мережі	Відсутність VLAN, використання дефолтних паролів	Порушення конфіденційності («К»), Втрата спостережності («С»)
DNS-спуфінг (підробка DNS)	Зловмисник підміняє DNS-записи, перенаправляючи жертву на шкідливі веб-сайти для крадіжки даних або зараження пристрою	DNS-сервери, клієнтські пристрої	Хакери, інсайдери	Впровадження підроблених DNS-записів, кеш-poisoning	Відсутність механізмів захисту DNS, використання незахищених мереж	Відсутність DNSSEC, довірливе використання DNS-записів	Порушення конфіденційності («К»), Порушення цілісності («Ц»)

4 Модель загроз прикладного ПЗ

Таблиця № А.3

Модель загроз прикладного ПЗ

Назва загрози	Опис загрози та можливі наслідки реалізації	Об’єкти загрози	Суб’єкти загрози	Можлива атака	Дестабілізуючі фактори	Вразливість, що може використовуватися	Тип загрози
SQL-ін'єкція	Впровадження SQL-коду через введення користувача, що може призвести до витоку даних	Веб-додатки, бази даних	Хакери, конкуренти	Використання некоректних запитів SQL	Відсутність перевірки введених даних	Відсутність механізмів захисту від SQL-ін'єкцій (Prepared Statements)	Порушення конфіденційності («К»), Порушення цілісності («Ц»)
XSS-атака (міжсайтовий скриптинг)	Вставка шкідливого JavaScript-коду в веб-сторінки, що може призвести до крадіжки сесій користувачів	Веб-додатки, браузери користувачів	Хакери	Вставка скриптів через форми введення	Відсутність фільтрації введених даних	Відсутність CSP (Content Security Policy), використання незахищених форм	Порушення конфіденційності («К»), Втрата спостереженості («С»)
Вразливість нульового дня	Використання невідомих розробникам вразливостей у ПЗ	Будь-яке прикладне ПЗ	Хакери, кіберзлочинці	Використання експлойтів	Відсутність оновлень	Відсутність системи моніторингу вразливостей	Порушення конфіденційності («К»), Порушення доступності («Д»)

5 Модель загроз ОС

Таблиця № А.4

Модель загроз ОС

Назва загрози	Опис загрози та можливі наслідки реалізації	Об’єкти загрози	Суб’єкти загрози	Можлива атака	Дестабілізуючі фактори	Вразливість, що може використовуватися	Тип загрози
1	2	3	4	5	6	7	8
Ескалація привілеїв	Зловмисник отримує підвищені права доступу в системі, що дозволяє йому змінювати налаштування та отримувати дані	Операційна система, сервери, робочі станції	Хакери, інсайдери	Використання експлойтів, вразливості в політиках доступу	Відсутність оновлень безпеки	Використання старих версій ОС, неправильні налаштування прав доступу	Втрата спостереженості («С»), Порушення цілісності («Ц»)
Віддалене виконання коду (RCE)	Зловмисник виконує шкідливий код на віддаленій системі, що дозволяє отримати контроль над нею	Операційна система, сервери	Хакери, зловмисники	Використання уразливостей ОС, виконання команд через мережу	Відсутність патчів безпеки, відкриті мережеві порти	Відсутність фаєрволів, використання застарілого ПЗ	Порушення конфіденційності («К»), Порушення доступності («Д»)

Продовження табл. А.4

1	2	3	4	5	6	7	8
Зловмисне програмне забезпечення	Встановлення вірусів, руткітів, троянів може призвести до крадіжки даних або порушення роботи ОС	Файлова система, процеси ОС	Кіберзлочинці, заражені файли	Впровадження шкідливого ПЗ, експлуатація уразливостей	Відсутність антивірусного захисту, використання ненадійних джерел ПЗ	Недостатній контроль за встановленням додатків, відсутність моніторингу поведінки процесів	Порушення конфіденційності («К»), Втрата спостереженості («С»), Порушення доступності («Д»)
Віруси та руткіти	Впровадження шкідливого ПЗ для прихованого управління системою або викрадення даних	Операційна система, робочі станції	Хакери, кіберзлочинці	Використання заражених файлів, соціальна інженерія	Відсутність антивірусного захисту, нехтування правилами кібергігієни	Відсутність моніторингу активності, слабкі політики безпеки	Порушення конфіденційності («К»), Порушення цілісності («Ц»), Втрата спостереженості («С»)

ДОДАТОК Б

МОДЕЛЬ ПОРУШНИКА ІНФОРМАЦІЇ

1. Перелік ділянок функціонування

Таблиця № Б.1

Перелік ділянок функціонування

Код ДФ	Назва ДФ	Опис
ДФ-01	Серверна	Місце розташування основних серверів, зберігання та обробка даних.
ДФ-02	Касова зона	Обслуговування клієнтів, проведення фінансових операцій, доступ до внутрішніх систем.
ДФ-03	Зона адміністратора	ІТ-адміністрування мережевої інфраструктури банку, управління серверами, моніторинг безпеки системи
ДФ-04	Кабінет директорів	Обробка вхідної та вихідної документації, доступ до внутрішніх систем, вирішення важливих питань.
ДФ-05	Клієнтська зона обслуговування	Робочі комп’ютери і планшети для виконання завдань, доступ до внутрішніх систем, консультування клієнтів.
ДФ-06	Конференц-зал	Використання для нарад, презентацій, відеоконференцій, обговорення конфіденційних питань.
ДФ-07	Кухня	Побутова зона, без зберігання конфіденційних даних.
ДФ-08	Вбиральня	Побутова зона, без зберігання конфіденційних даних.

2. Форми представлення інформації на функціональних ділянках ІТС.

Таблиця № Б.2

Форми представлення інформації на функціональних ділянках ІТС

Код форми	Форма представлення інформації
Ф-01	Електронна (цифрові дані на серверах, робочих станціях).
Ф-02	Паперова (друкована документація, звіти, договори).
Ф-03	Візуальна (відображення на екранах, презентаціях).
Ф-04	Аудіо/відео (записи нарад, телефонні розмови).

3. Модель використання інформації функціональними ділянками

Таблиця № Б.3

Модель використання інформації функціональними ділянками

Код ДФ	Форми, в яких інформація передається на вхід ДФ	Форми, в яких інформація знаходиться на ДФ під час обробки	Форми, в яких інформація передається на вихід ДФ
ДФ-01	Ф-01 (Електронна), Ф-02 (Паперова)	Ф-01 (Електронна)	Ф-01 (Електронна), Ф-02 (Паперова)
ДФ-02	Ф-01 (Електронна), Ф-02 (Паперова), Ф-03 (Візуальна)	Ф-01 (Електронна), Ф-03 (Візуальна)	Ф-01 (Електронна), Ф-02 (Паперова), Ф-03 (Візуальна)
ДФ-03	Ф-01 (Електронна), Ф-02 (Паперова)	Ф-01 (Електронна)	Ф-01 (Електронна), Ф-02 (Паперова), Ф-03 (Візуальна)
ДФ-04	Ф-01 (Електронна), Ф-02 (Паперова), Ф-03 (Візуальна), Ф-04 (Аудіо/відео)	Ф-01 (Електронна), Ф-02 (Паперова)	Ф-01 (Електронна), Ф-02 (Паперова), Ф-03 (Візуальна)

Продовження табл. Б.3

ДФ-05	Ф-01 (Електронна), Ф-02 (Паперова), Ф-03 (Візуальна)	Ф-01 (Електронна), Ф-03 (Візуальна)	Ф-01 (Електронна), Ф-02 (Паперова), Ф-03 (Візуальна)
ДФ-06	Ф-01 (Електронна), Ф-02 (Паперова), Ф-03 (Візуальна), Ф-04 (Аудіо/відео)	Ф-03 (Візуальна), Ф-04 (Візуальна)	Ф-04 (Аудіо/відео)
ДФ-07	Не застосовується	Не застосовується	Не застосовується
ДФ-08	Не застосовується	Не застосовується	Не застосовується

4. Рівні обізнаності потенційних порушників та рівні їх навичок

Таблиця № Б.4

Рівні обізнаності потенційних порушників та рівні їх навичок

Код	Назва
РО-01	Випадковий порушник (низький рівень навичок)
РО-02	Внутрішній інсайдер (середній рівень навичок)
РО-03	Досвідчений хакер (високий рівень навичок)
РО-04	Організована група (дуже високий рівень навичок)

5. Методи, які можуть бути використаними порушниками політики безпеки

Таблиця № Б.5

Методи, які можуть бути використаними порушниками політики безпеки

Код	Назва
М-01	Фішинг (соціальна інженерія)
М-02	Злом паролів та облікових записів
М-03	Використання шкідливого програмного забезпечення (віруси, трояни)

Продовження табл. Б.5

М-04	Перехоплення трафіку
М-05	Фізичний доступ до обладнання
М-06	Підробка документів
М-07	Внутрішні витоки інформації (інсайдерські атаки)

6. Період часу дії потенційних порушників політики безпеки

Таблиця № Б.6

Період часу дії потенційних порушників політики безпеки

Код	Назва
ПД-01	Короткострокова (разова атака)
ПД-02	Середньострокова (від кількох тижнів до місяців)
ПД-03	Довгострокова (більше 6 місяців)

1. Місце дії потенційних порушників політики безпеки

Таблиця № Б.7

Місце дії потенційних порушників політики безпеки

Код	Назва
МД-01	Внутрішнє (з приміщення компанії)
МД-02	Зовнішнє (через Інтернет)
МД-03	Змішане (поєднання фізичного та віддаленого доступу)

2. Перелік потенційних можливостей порушників політики безпеки

Таблиця № Б.8

Перелік потенційних можливостей порушників політики безпеки

№	Категорії потенційних порушників	Можливості	Методи	Час дії	Місце дії
1	2	3	4	5	6
Внутрішні потенційні порушники					
П1	Касири	Доступ до внутрішніх облікових систем, клієнтських рахунків, платіжних документів та касового програмного забезпечення	М-01, М-02, М-07	ПД-02, ПД-03	МД-01
П2	Колнсультанти з питань юридичних і фізичних осіб	Доступ до персональних даних клієнтів, фінансових документів, CRM-систем, електронного документообігу та сканованих копій документів	М-01, М-06, М-07	ПД-02, ПД-03	МД-01
П3	Адмін системи	Доступ до мережевих налаштувань, адміністрування серверів. Повний контроль над мережевою інфраструктурою, логами, системами доступу та привілеями користувачів	М-02, М-03, М-04, М-05, М-07	ПД-03	МД-03
П4	Директора та керівництво	Доступ до стратегічної, управлінської та фінансової інформації, внутрішніх звітів, документів, рішень	М-05, М-06, М-07	ПД-03	МД-01

Продовження табл. Б.8

1	2	3	4	5	6
П5	Технічний персонал	Фізичний доступ до обладнання, мережевих кабелів, комутаторів, електроживлення, іноді — до серверних приміщень	М-01, М-05, М-07	ПД-01, ПД-02	МД-01
П6	Охорона	Доступ до фізичних зон об'єкта в неробочий час, спостереження за персоналом, контроль відеоспостереження	М-05, М-07	ПД-01, ПД-02	МД-01
П7	Співробітники, що звільняються	Можуть мати залишкові облікові записи, знання внутрішніх процесів, паролі або копії даних	М-01, М-07	ПД-01	МД-03
П8	Віддалені працівники	Доступ до корпоративних систем через VPN або інші канали, робота з корпоративними файлами і базами поза межами офісу	М-01, М-03, М-04, М-07	ПД-02, ПД-03	МД-02
П9	Тимчасові працівники або стажери	Частковий або тимчасовий доступ до систем, недостатній рівень обізнаності щодо політик безпеки	М-01, М-02, М-03, М-05, М-06, М-07	ПД-01, ПД-02	МД-03
Зовнішні потенційні порушники					
П10	Конкуренти	Використання корпоративного шпигунства	М-01, М-06, М-07	ПД-02,	МД-03

				ПД-03	

Продовження табл. Б.8

1	2	3	4	5	6
П11	Кіберзлочинці	Хакерські атаки, злом систем	М-01, М-02, М-03, М-04	ПД-01, ПД-02, ПД-03	МД-02
П12	Випадкові відвідувачі	Випадковий доступ до інформації, прослуховування	М-05	ПД-01	МД-01
П13	Підрядники, обслуговуючий персонал	Доступ до приміщень та техніки	М-01, М-05, М-07	ПД-01, ПД-02	МД-01
П14	Зловмисники	Несанкціонований фізичний доступ, крадіжка даних	М-02, М-05, М-06	ПД-01, ПД-02	МД-01
П15	Спостерігачі (журналісти, активісти)	Спостереження, збір інформації	М-01, М-04	ПД-02	МД-01
П16	Незадоволені клієнти або партнери	Поширення дезінформації, витік даних	М-01, М-02	ПД-01, ПД-02	МД-01