ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

студента (ки) Парфьонова Р.Д.
(*прізвище та ініціали)*
представлену на здобуття освітнього ступеня «магістр»
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему Проект комп'ютерної мережі комерційного банку

2. Актуальність підтверджується постійним зростанням кількості хакерських атак на комп'ютерні мережі банку. Удосконалення методів та засобів побудови, а також технологій захисту інформаційно-комуніцікйаних систем є актуальною задачею сьогодення.

(зазначити, які питання теоретичного і практичного характеру визначають актуальність роботи)

3. Основний зміст роботи викладно у пояснювальній записці, яка виконана на належному рівня, містить достатню кількість ілюстративного матеріалу. Список літератури є достатнім для аналізу та виконання поставлених задач.

4. Зміст розділів роботи *(зазначити за кожним розділом, які питання досліджені та з якою метою)*

Перший розділ пояснювальної записки направлений на проведення аналізу методів та засобів захисту інформації комерційного банку, визначення особливостей проблем захисту та канали витоку нформації. Проведено аналіз інформаційної безпеки комерційного банку.

У другому розділі проведені дослідження щодо модернізації комп'ютерної мережі комерційного банку. Представлено модернізовану топологію, вибір обладнання, та основні налаштування технологій захисту.

Третій розділ присвячено тестуванню запропонованої топології та проведених налаштувань захисту.

У четвертому розглядаються питання з охорони праці, безпеки роботи та визнкачено вимоги до приміщень.

5. Висновки обгрунтовані, повністю відповідають поставленим завданням, мають теоретичне та практичне значення. .

(обґрунтованість, теоретичне і практичне значення)

6. Список використаних літературних джерел. Джерела опрацьовані у повному обсязі, відповідають змісту роботи.

(обсяг і повнота опрацювання за змістом роботи)

7. Додатки містять технічні характеристик та налаштування вибраного обладнання

(перелік додатків та повнота їх опрацювання за змістом роботи)

8. Таблиці та ілюстрації Ілюстрації носять інформаційний характер, є доповненням до змісту роботи.

(призначення таблиць та їх використання для підтвердження досліджень в роботі)

9. Якість оформлення роботи на достатньому рівні

10. Ставлення студента (ки) до виконання кваліфікаційної магістерської роботи відповідально

11. Висновок

В цілому при написанні кваліфікаційної роботи бакалавра студент (ка) Парфьонов Р.Д.

(*прізвище та ініціали)*

вміння /невміння/ підібрати необхідну літературу, інформаційну базу, проаналізувати їх, зробити відповідні висновки і оформити свої дослідження у атестаційній магістерській роботі.

Кваліфікаційна бакалаврська робота студента (ки) Парфьонова Р.Д.

(*прізвище та ініціали)*

написана на достатньо /недостатньо/ високому рівні та може /не може/ бути допущена до захисту в Екзаменаційній комісії.

Науковий керівник _канд. техн. наук, доцент, декан ФІКТ, доцент кафедри КІтаКБ
(*вчений ступінь, звання, посада)*



Надія ЛОБАНЧИКОВА
(підпис) *(прізвище та ініціали)*
«16 » червня 2020 р.

РЕЦЕНЗІЯ

на випускну кваліфікаційну роботу студента денної форми навчання

спеціальності 123 «Комп'ютерна інженерія»

(шифр та назва спеціальності)

Парфьонова Руслана Дмитровича

(прізвище, ім'я, по-батькові)

1. Тема: Проект комп'ютерної мережі комерційного банку

2. Актуальність теми випускної кваліфікаційної роботи Комп'ютеризація банківської діяльності дозволила значно підвищити продуктивність праці працівників банку, впровадити нові фінансові продукти та технології. Однак прогрес в техніці злочинів здійснювався не меншим повільними темпами, ніж розвиток банківських технологій. В даний час більше 90 % всіх злочинів пов'язаних з використанням інформаційно-комунікаційних систем (ІКС) банку. Відповідно, при створенні та модернізації ІКС банкам необхідно приділяти особливу увагу забезпеченню її безпеки. Саме цій проблемі присвячується більша частина дипломної роботи.

(зазначити ступінь актуальності теми)

3. Наукова та практична цінність роботи полягає в тому, що було здійснено модернізацію комп'ютерної мережі відділення банку «Райффайзен Банк Аваль».

4. Недоліки: 1) Список використаних джерел містить 22 джерела, з яких усі є Інтернет-джерелами. Тому автору варто було б звернути увагу на друковані видання

5. Загальний висновок:

Вважаємо, що випускна кваліфікаційна робота студента Парфьонова Р.Д.

(ПІБ студента)

на тему: Модернізація комп'ютерної мережі відділення банку «Райффайзен Банк Аваль»

Відповідає / не відповідає профілю підготовки бакалавра,

(«бакалавра», «магістра» – вказати потрібне)

Написана на **достатньо** / недостатньо високому рівні, а її автор заслуговує на **присвоєння** / неприсвоєння освітнього ступеня бакалавр

(«бакалавр», «магістр» – вказати потрібне)

Рецензент

д.п.н., доц., проф.каф.ІПЗ		Вакалюк Т. А.
(посада)	*(підпис, печатка)*	*(ПІБ)*

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему:

«Проект комп'ютерної мережі комерційного банку»

Виконав студент 4-го курсу, групи КІ-2
спеціальності 123 «Комп'ютерна інженерія»
_____ Парфьонов Р.Д.
Керівник, декан ФІКТ, канд. техн. наук, доцент
_____ Лобанчикова Н.М.
Завідувач кафедри КІ та КБ, канд.техн.наук.
_____ Єфіменко А.А.
Рецензент, професор кафедри ІПЗ, д-р пед. наук, доцент
_____ Вакалюк Т.А.

Житомир 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки, канд. техн. наук
Єфіменко А. А.
«06» квітня 2020 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу

Студента **Парфьонова Руслана Дмитровича**

Тема роботи: **Проект комп'ютерної мережі комерційного банку**
затверджена Наказом по університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи – **1 червня 2020 р.**
Вихідні дані для роботи:

1. Опис комп'ютерної мережі відділення банку.
2. Перелік та характеристики апаратного забезпечення, що використовується у функціонуванні комп'ютерної мережі
3. Нормативно-правові вимоги щодо функціонування та захисту комп'ютерної мережі банків від Національного Банку України
4. Інші нормативні положення, що регламентують побудову та захист комп'ютерної мережі комерційного банку.
5. Перелік програмного забезпечення, що використовується в діяльності банку.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Лобанчикова Н.М.	06.04.20	06.04.20
2	Лобанчикова Н.М.	20.04.20	20.04.20
3	Лобанчикова Н.М.	11.05.20	11.05.20

Керівник _____ Лобанчикова Н.М.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2020 – 7 квітня 2020	Виконано
2	Аналіз наявної комп'ютерної мережі	8 квітня 2020 – 11 квітня 2020	Виконано
3	Виявлення недоліків та аналіз методів покращення та модифікації мережі	12 квітня 2020 – 16 квітня 2020	Виконано
4	Аналіз та вибір обладнання	17 квітня 2020 – 19 квітня 2020	Виконано
5	Проектування захищеної мережі	20 квітня 2020 – 30 квітня 2020	Виконано
6	Розробка комп'ютерної мережі	1 травня 2020 – 18 травня 2020	Виконано
7	Тестування мережі	19 травня 2020 – 22 травня 2020	Виконано
8	Аналіз результатів тестування	23 травня 2020 – 24 травня 2020	Виконано
9	Написання пояснювальної записки	25 травня 2020 – 29 травня 2020	Виконано
10	Підготовка презентації та виступу	30 травня 2020 – 31 травня 2020	Виконано
11	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2020 – 8 червня 2020	Виконано
12	Захист кваліфікаційної роботи	13 червня 2020	Виконано

Студент _____ Парфьонов Р.Д.

Керівник _____ Лобанчикова Н.М.

РЕФЕРАТ

Пояснювальна записка до дипломного проекту випускника освітньо-кваліфікаційного рівня бакалавр на тему «Проект комп'ютерної мережі комерційного банку» викладена на 71 с., містить 15 рисунків, 8 таблиць, 22 літературних джерел.

Об'єкт дослідження – технології побудови комп'ютерних мереж банків.

Предмет дослідження – методи, засоби та технології побудови комп'ютерної мережі відділення банку «Райффайзен Банк Аваль».

Мета дослідження – розробка проекту модернізації комп'ютерної мережі Житомирського відділення № 1 АТ «Райффайзен Банк Аваль».

У першому розділі дипломного проекту представлено результати аналізу методів та засобів захисту інформації комерційного банку. На основі аналізу було виявлено недоліки в існуючій системі захисту інформації комерційного банку «Райффайзен Банк Аваль». У другому розділі дипломного проекту проведено модернізацію підсистеми захисту комп'ютерної (інформаційно-комунікаційної) мережі шляхом вдосконалення кабельної системи, топології та технології побудови. Проведено вибір та обґрунтування мережевого обладнання та здійснено його налаштування. В третьому розділі було проведено тестування працездатності запропонованої комп'ютерної мережі шляхом комп'ютерного моделювання.

Ключові слова: СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, КОМЕРЦІЙНИЙ БАНК, МЕРЕЖА.

ABSTRACT

The explanatory note to the diploma project of the graduate of the educational qualification level bachelor on the topic "Project of the computer network of a commercial bank" is set out on the 78 pages, contains 15 drawings, 8 tables, 22 literary sources.

The object of research - technologies for building computer networks of banks.

The subject of the research is methods, means and technologies of building a computer network of Raiffeisen Bank Aval branch.

The purpose of the study is to develop a project to modernize the computer network of the Zhytomyr branch № 1 of JSC "Raiffeisen Bank Aval".

The first section of the diploma project presents the results of the analysis of methods and means of information protection of a commercial bank. Based on the analysis, shortcomings in the existing information protection system of Raiffeisen Bank Aval were identified. In the second section of the diploma project the modernization of the subsystem of protection of the computer (information and communication) network was carried out by improving the cable system, topology and construction technology. The selection and substantiation of the network equipment was carried out and its adjustment was carried out. In the third section, the performance of the proposed computer network was tested by computer simulation.

Keywords: INFORMATION PROTECTION SYSTEM, INFORMATION AND COMMUNICATION SYSTEM, COMMERCIAL BANK, NETWORK.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АТ – Акціонерне товариство

НБУ – Національний Банк України

ІКС – Інформаційно-комп’ютерна система

CPT – Cisco Packet Tracer

VPN – Virtual Private Network

США – Сполучені Штати Америки

ЗМІ – Засоби Масової Інформації

IT -Information Technology

АЗЗ – Апаратні Засоби Захисту

АС – Апаратні Системи

ДСТУ – Державні Стандарти України

НДТЗІ – Нормативний Документ Технічного Захисту Інформації

ISO – International Standardization Organisation

СБ – Служба Безпеки

ОЗП – Операційно Запам’ятовуючий Пристрій

VLAN – Virtual Local Area Network

OSPF – Open Shortest Path First

IGP - Interior Gateway Protocol

AH - Authentication Header

ESP – Encapsulating Security Payload

ЗМІСТ

ВСТУП..... 9

1. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ КОМЕРЦІЙНОГО БАНКУ 11

1.1 Загальна характеристика комерційного банку «Райффайзен Банк Аваль» 11

1.2 Методи та засоби забезпечення інформаційної безпеки комерційного банку 14

1.2.1 Особливості проблем забезпечення інформаційної безпеки комерційних банків 14

1.2.2 Неправомірне отримання банківської інформації та захист від нього 17

1.3 Аналіз інформаційної безпеки комерційного банку «Райффайзен Банк Аваль»..... 23

Висновки до першого розділу 32

2. МОДЕРНІЗАЦІЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ ЖИТОМИРСЬКОГО ВІДДІЛЕННЯ АТ «Райффайзен Банк Аваль» 33

2.1 Аналіз інформаційно-комунікаційної системи відділення комерційного банку «Райффайзен Банк Аваль»..... 33

2.2 Аналіз топології та розробка системи адресації інформаційно-комунікаційної мережі 38

2.3 Обґрунтування вибору технології побудови інформаційно-комунікаційної системи комерційного банку..... 40

2.4 Обґрунтування вибору обладнання мережі 44

2.5 Налаштування захищеної інформаційно-комунікаційної мережі відділення комерційного банку «Райффайзен Банк Аваль» 45

3. ТЕСТУВАННЯ ЗАХИЩЕННОЇ МЕРЕЖІ КОМЕРЦІЙНОГО БАНКУ 50

3.1 Перевірка доступності вузлів мережі 50
3.2 Перевірка налаштованих параметрів\технологій захисту мережі. 53
4. ОХОРОНА ПРАЦІ В КОМЕРЦІЙНОМУ БАНКУ 56
4.1 Загальні вимоги до охорони праці в комерційному банку 56
4.2 Вимоги до виробничих приміщень 57
4.2.1 Фарбування і коефіцієнти віддзеркалення 57
4.2.2 Освітлення 58
4.2.3 Параметри мікроклімату 59
4.2.4 Шум і вібрація 61
4.2.5 Електромагнітне та іонізуюче випромінювання 62
4.3 Ергономічні вимоги до робочого місця 62
Висновки до четвертого розділу 66
ВИСНОВКИ 67
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 69
ДОДАТКИ 71
Додаток А 72

ВСТУП

Історія існування банків бере свій початок дуже давно. Кожна людина бажає захистити свої заощадження, але залишати коштовні речі вдома стало не зовсім безпечно, тому що завжди були люди які хотіли нажитися у злочинний спосіб. І цей інтерес був пов'язаний не лише із зберіганням в кредитних організаціях грошових засобів, але й з тим, що в банках зосереджувалась важлива і часто секретна інформація про фінансову та господарську діяльність багатьох людей, компаній, організацій і навіть цілих держав.

В даний час значення інформації, що зберігається в банках, значно збільшилося. Також у зв'язку із всезагальною інформатизацією та комп'ютеризацією банківської діяльності значення інформаційної безпеки банківських структур зросло в декілька разів. Ще 30 років тому об'єктом інформаційних атак були дані про клієнтів банків або про діяльність самого банку. Такі атаки були досить рідкісними, коло їх замовників був дуже вузький, а збиток міг бути значним лише в особливих випадках. Зараз, в результаті всезагального розповсюдження електронних платежів, банківських пластикових карт, комп'ютерних мереж, об'єктом інформаційних атак стали безпосередньо грошові кошти як банків, так і їх клієнтів. Здійснити злочинну спробу може будь-хто – необхідно лише наявність комп'ютера та підключення до Інтернету. При чому для цього не має необхідності фізично проникати в банк, можна «працювати» і за десятки кілометрів.

Комп'ютеризація банківської діяльності дозволила значно підвищити продуктивність праці працівників банку, впровадити нові фінансові продукти та технології. Однак прогрес в техніці злочинів здійснювався не меншим повільними темпами, ніж розвиток банківських технологій. В даний час більше 90 % всіх злочинів пов'язаних з використанням інформаційно-комунікаційних систем (ІКС) банку. Відповідно, при створенні та модернізації ІКС банкам необхідно приділяти особливу увагу забезпеченню її безпеки. Саме цій проблемі присвячується більша частина дипломної роботи.

Таким чином, метою даної роботи є розробка проекту модернізації комп'ютерної мережі Житомирського відділення АТ «Райффайзен Банк Аваль» та розробка ефективних засобів захисту, що дозволяють забезпечити необхідний рівень захисту інформаційних ресурсів комерційного банку.

Об'єкт дослідження – технології побудови комп'ютерних мереж банків.

Предмет дослідження – методи, засоби та технології побудови комп'ютерної мережі відділення банку «Райффайзен Банк Аваль».

Для досягнення вказаної мети необхідним є вирішення наступних задач:

1. Аналіз методів і засобів збереження та захисту інформаційних ресурсів в інформаційно-комунікаційній системі відділення банку «Райффайзен Банк Аваль».
2. Аналіз загальних вимог до захисту інформаційних ресурсів банку.
3. Аналіз погроз безпеці інформаційно-комунікаційної системи банку.
4. Визначення існуючого рівня інформаційної безпеки банку.
5. Дослідження технологій побудови інформаційно-комунікаційної системи відділу банку.
6. Модернізація комп'ютерної мережі відділення банку «Райффайзен Банк Аваль».
7. Вибір засобів збереження та захисту інформаційних ресурсів.

1. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ КОМЕРЦІЙНОГО БАНКУ

1.1 Загальна характеристика комерційного банку «Райффайзен Банк Аваль»

«Райффайзен Банк Аваль» - на даний час є один з найбільших австрійських банківських груп та також кооперативний банк. Штаб -квартира банку знаходиться у Відні.

Банківська група в Австрії була заснована в 1927 році під назвою Genossenschaftliche Zentralbank. Згодом кілька разів змінювала назву. Слово Райффайзен з'явилося в назві в 1989 році на честь Фрідріха Вільгельма Райффайзена, німецького громадського діяча і піонера кооперативного руху. У 1938 році, відразу після окупації Австрії Німеччиною, банківська група була націоналізована а в 1955 році була повернута колишнім власникам.

Перше дочірнє товариство Raiffeisen в Східній Європі було відкрито в 1987 році. Після 2000 року група розширила свою присутність в центральній і східній Європі, і в 2003 році дочірні суспільства в цих країнах були об'єднані в компанію Raiffeisen International. У 2017 році Raiffeisen International був об'єднаний з головним банком групи, Raiffeisen Zentralbank Österreich AG, новий банк отримав назву Raiffeisen Bank International, в свою чергу він входить до складу Raiffeisen Bank Group. З € 225 млрд активів групи € 140 млрд в 2018 році довелося на Raiffeisen Bank International.

Історія одного з найвідоміших австралійських банків бере свій початок з 28 березня 1992 року, коли НБУ зареєстрував АКБ «Аваль». На початку 1994 році Національний Банк України перереєстрував банк як АППБ «Аваль». Під також назвою він існував аж до 2006 року. «Райффайзен Банк Аваль» постачає допомогу клієнтам різних рівнів, МСБ та великі корпорації. Банк обслуговує та надає повний перелік банківських продуктів і послуг зокрема це кредити та депозити, фінансування проектів, поточні рахунки, зарплатні проекти, казначейські послуги розрахунково-касові та казначейські послуги, тощо.

Наприкінці жовтня 2005 року банк приєднується до банківської групи «Райффайзен Інтернаціональ Банк-Холдинг» АГ, Австрія. На початку 2010 року – Райффайзен Банк Інтернаціональ АГ. 1 січня 2015 року РБІ захоплює 96,4% акцій українського банку. І от вже наразі «Райффайзен Банк Аваль» стає найбільшим українським банком із іноземним капіталом.

Широку варіацію звичайних та сучасних послуг отримує більше аніж 3 мільйони відвідувачів Райффайзен Банку Аваль за допомогою загальнонаціональної мережі, до якої можна віднести 674 відділення у великих містечках, обласних та районних центрах, окремих селищах по всій території нашої держави.

Організаційною моделлю банку є 26 відділів департаменту, 14 відділів та управлінь, підгрупи та групи менеджменту по інформаційним технологіям, служби які співпрацюють з недержавним пенсійним забезпеченням, казначейства, виконавчого секретаріату тощо.

Не менш важливою ознакою банку є ефективна структура управління, що має чіткий розподіл: бізнес-лінії та вертикалі підтримки, що працюють на рівні Центрального офісу та дирекцій обласних центрів. Банк має чітко прописане розмежування функціонування офісу, що дає змогу підвищити рівень обслуговування та якість надання послуг. Не секрет, що це значно зменшує ризики та контролює процес. Якщо говорити про організаційну структуру, то доречно буде додати, що вона постійно вдосконалюється для того щоб поліпшити рівень прийняття важливих рішень, забезпечувати якість обслуговування серед клієнтів на всій території України.

Неабиякі досягнення Банку Аваль традиційно визнають також і в Україні, і за її межами відомі люди, партнери, експерти, рейтингові компанії, та клієнти. Наведемо приклад, що у 2012 році Райффайзен Банк Аваль вже вдруге визнано як найкращий банк в Україні, зокрема у межах дослідження Eurasian Bank Survey 2012, що проводилося відомим культовим виданням Business New Europe.

Доречно буде додати, що Банк Аваль прийнято вважати найкращим стабільним недержавним банком України дотримуючи рейтингу «30 най

надійніших банківських секторів» та публікації в журналі «Кореспондент» й інвестиційною компанією Dragon Capital.

Сфера відвідувань мереж банків 2018 року нараховувала неабияку кількість відвідувачів. Серед них: 504 відділення по всій території, 2525 банкоматів та 413 платіжних терміналів. Банк вже емітував 4,9 млн. платіжних карток, що позиціонує Райффайзен Банк Аваль як надійного партнера. Зокрема, Райффайзен Банк Аваль володіє наймасштабнішою мережею торговельних POS-терміналів чисельністю понад 24 тисячі одиниць.

Зважаючи на інформацію, що контрольними пакетами акційного банку «Райффайзен Банк Аваль» є АТ «Райффайзен Централбанк», буде влучно, навести декілька цікавих фактів і про нього. Райффайзен Центральбанк Остеррайх АГ (РЦБ) - головний банк найбільшої австрійської банківської сфери групи Райффайзен. Він виступає - провідним корпоративним та інвестиційним банком в Австрії, який розглядає Центральну і Східну Європу як свій домашній ринок. РЦБ відносить себе до єдиного австрійського банку, що має глобальну мережу відділень, що охоплюють та працюють майже у всіх найвпливовіших фінансових центрах світу. Групи, відділення та представництва даного банку також розташовані в Азії. Якщо брати до уваги дочірню компанію, Райффайзен Інтернаціональ Банк-Холдинг АГ, РЦБ керує одним із найбільших банківських мереж розташованих в Центральній та Східній Європі. Понад 16 ринків у поданому регіоні мають як лізингові компанії, дочірні банки та також два представництва й декілька фінансових інститутів. Більше ніж 14,5 млн користувачів обирають послуги у більшості ніж 3200 мереж банку.

Головна мета діяльності Банку Аваль є отримання прибутку в інтересах його власних та акціонерів. На сьогодні Райффайзен є провідним банком, який надає послуги кредитування та максимально повний список банківських опцій, з них грошові перекази та споживче кредитування.

Отже, «Райффайзен Банк Аваль» розвивається як роздрібний універсальний банк з потужною корпоративною вертикаллю, здатною ефективно обслуговувати підприємства великого, малого та середнього бізнесу.

1.2 Методи та засоби забезпечення інформаційної безпеки комерційного банку

1.2.1 Особливості проблем забезпечення інформаційної безпеки комерційних банків

Актуальність проблеми інформаційної безпеки комерційних банків визначається рядом взаємозв'язаних факторів, більшість з яких є наслідком процесу інформатизації сучасного суспільства.

Серед таких факторів, з одного боку, – формування правових засад інформатизації, поширення застосування сучасних інформаційних технологій у підприємницькій діяльності, а з іншого – висока уразливість інформаційних систем, стрімкий прогрес розвитку так званої «інформаційної зброї».

Особливості соціально-економічної ситуації, відсутність реальних обмежень щодо доступу до засобів інформаційного нападу призводять до численних фактів їх застосування конкурентами, кримінальними елементами, іншими суб'єктами проти комерційних структур.

Крім того, в умовах жорстокої конкурентної боротьби, проведення суб'єктами економічних ринків актів недобросовісної конкуренції та дій, пов'язаних із промисловим шпигунством, виникла нагальна потреба в розмежуванні доступу до носіїв інформації безпосередньо на підприємствах та у банках, виокремлення інформації з обмеженим доступом і визначення порядку її отримання та використання.

Наша банківська система є першою в Україні по використанню новітніх інформаційних технологій для того, щоб діяльність банків була автоматизованою. Теперішній банк користується чималою кількістю високо-технологічних рішень, також використовує платіжні системи та системи переказів грошей – як особистих так і державних і міжнародних. Варто сказати, що всі ці системи були створенні у різні часи та різними людьми, тому мають різний ступінь захищеності та взагалі рівень безпеки.

Ці рішення в більшості використовуються різними підрозділами банку і нерідко не мають потрібного супроводу.

Відношення людей, які займають керівні посади в банках, до інформаційних технологій різне: перші ставляться до впровадження такої системи дуже добре, оскільки розуміють, що це призведе до першості на ринку та допоможе залучити більше клієнтів; других зупиняє думка про те, що вартість таких змін дуже висока і супроводження такої системи також коштує чимало грошей.

Існує ще одна проблема – потрібно витрачати багато грошей на систему захисту інформацію. Керівництво банків часто думають, що використання коштів в такий вигляд є недоцільним, та не приносять прибутку, тому вирішують не впроваджувати таку систему. Внаслідок цього, за статтею «Захист інформації» витрати зменшуються весь час, також економляться чималі кошти на спеціалістів, котрі повинні супроводжувати й контролювати банківську інформаційну безпеку. І доти, доки установа не почне зазнавати значних збитків, втрату клієнтів, погіршення репутації та інших фінансових або соціальних впливів, ситуація не зміниться, але вже втрати не повернути.

Можна навести велику кількість прикладів, коли банки втрачали неймовірні суми грошей через порушення інформаційної безпеки. За даними Програми зі стану інформаційної безпеки Форуму з питань інформаційної безпеки (ISF`s Information Security Status Survey), збитки від злодіїв, які використовують хакерські атаки, що призвели до порушення цілісності інформації та компрометації становлять близько 1.5 мільйона доларів США щороку, від помилок та незаконних дій персоналу - близько 1.2 мільйона доларів, від інших порушень – 3.2 мільйона доларів США за рік.

Кожний такий випадок рано чи пізно стане відомий суспільству і довіра та повага до такої банківської установи різко впаде. Завдяки ЗМІ, ця інформація поширюється з неймовірною швидкістю і кожна людина, яка має інтернет може побачити цю інформацію і розповсюдити серед своїх знайомих, родичів, друзів, колег та просто випадкових людей. І зазвичай нікого не хвилює чия це була провина чи хто був винуватцем, але згідно статистики, у 95% випадків,

працівники організації приймали участь у злочині, що робить цей процес набагато легшим. І не дивлячись на статистичні дані, не варто виключати з списку злочинців таких людей, як хакери, особливо в тих банках, де до питань інформаційної безпеки ставляться зі знехтуванням.

Використання цих технологій захисту інформації також наражає на певну небезпеку, оскільки потрібно весь час відстежувати кожний крок та кожний байт даних, який був втрачений чи міг бути модифікований для того, щоб мінімізувати фінансові втрати. Саме таку вимогу встановлює до банків Базельський комітет – проводити оцінку операційних ризиків.

До операційних ризиків можна віднести все, що виникає у банківському процесі, тобто все, що було перелічене в минулому абзаці(надалі – IT ризики). На даний момент, є декілька класифікацій, для яких основою є причини, місце або джерела виникнення ризиків.

Найчастіше виникають та призводять до найбільших втрат такі IT-ризики: отримання несанкціонованого доступу до інформації, її несанкціоновані зміни, пошкодження та втрата [21]. Ці ризики мають різне походження, а саме:

– хакерські атаки;
– неправомірні дії персоналу;
– помилки та недостатня обізнаність персоналу;
– відсутність належної системи захисту;
– неправильна робота програмно-технічних комплексів;
– використання небезпечних інформаційних технологій$
– неправильне використання послуг третіх сторін;
– негативний вплив зовнішнього середовища, техногенні катастрофи тощо.

Якщо подивитись на приведені вище пункти і спробувати звести їх до спільного знаменника, можна буде виділити, що вони призводять до втрати конфіденційності, цілісності й доступності інформації. Згідно з цими судженнями, наступні задачі повинні бути виконаними для того, щоб надати стовідсоткову безпеку комерційного банку:

– ефективно виявляти найкритичніші ризики та забезпечувати їх усунення;

– знизити й оптимізувати вартість побудови та підтримки системи інформаційної безпеки;

– постійно відстежувати та оцінювати ризики з урахуванням завдань бізнесу;

– будувати політику інформаційної безпеки та забезпечити її виконання;

– ефективно розробляти, впроваджувати і тестувати плани відновлення бізнесу;

– забезпечувати розуміння питань ІБ з боку керівництва банку;

– забезпечувати підвищення репутації та ринкової привабливості банків;

– забезпечувати захист від рейдерських атак тощо

Аналізуючи особливості забезпечення інформаційної безпеки в комерційних банках, стає очевидно, що ера впровадження «точкових» або локальних рішень безпеки підійшла до кінця. На порядку денному – побудова комплексних масштабованих систем з єдиним центром управління, що відповідають світовим стандартам. Внаслідок цього відбувається прийняття того факту, що захист банківської інформації, будучи надзвичайно складним і дорогим процесом, вимагає відпрацьованих методик щодо її забезпечення, які негайно перетворюються в один з найбільш значущих активів організації. І щоб бути впевненим, що всі внески, які потрібні для того, щоб забезпечити найкращий захист даних, потрібно гарно проаналізувати ринок пропозицій захисту ,та відшукати найкращий зі сторони фінансів і що більш важливе, зі сторони якості послуг та рівня безпеки.

1.2.2 Неправомірне отримання банківської інформації та захист від нього

Банківська діяльність досить насичена не тільки діловими відносинами, їй значною мірою притаманні тісні інформаційні відносини партнерів та конкурентів. Останні ж регулюються відповідними законодавчими та нормативними актами держави, а також нормативними документами підприємницьких структур.

Що ж до банківської інформації, то, відповідно до положень Законів України «Про інформацію»[22], «Про підприємства в Україні»[22], «Про банки і банківську діяльність» [22] та інших законодавчих актів, її структура може мати вигляд, що показано на рисунку 1.1.



Рисунок 1.1 – Структура банківської інформації

Спираючись на статтю 60 Закону України « Про банки і банківську систему», інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку, є банківською таємницею.

Банківською таємницею, зокрема, є:

1)відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

3) фінансово-економічний стан клієнтів;

4) системи охорони банку та клієнтів;

На жаль, банк не може гарантувати 100% безпечність даних, тому що кожний працівник банку – людина, і неможливо бути впевненим до кінця, що жодні ваші дані не будуть втрачені, перехоплені, передані якимось іншим способом третім особам, не дивлячись на те, що всі банки це гарантують. Також, гарантії, що інформаційна система ніколи не дасть збій, чи не зможе бути зламаною впевненості немає, але якщо банк не хоче втрачати свою репутацію та

своїх клієнтів, потрібно витратити чималі кошти на захищеність мережі, даних та доступу кожного співробітника банку до системи. Для того, щоб максимально уникнути цих випадків, існують обов'язкові заходи щодо забезпечення захисту банківської таємниці. Наведемо декілька прикладів:

- обмеження кількості людей, які мають доступ до інформації, що належить до банківської таємниці;

- створення спеціального підрозділу, який займається документами, що містять згадувану інформацію;

- налагодження спеціальної системи захисту, яка буде запобігати несанкціонованому доступу з будь-яких носіїв;

- вказування кожного пункту захисту інформації під час підписання договорів, а точніше – про її нерозголошення в межах банку і поза ним як клієнтами так і співробітниками.

У загальному випадку оволодіння інформацією комерційного банку, щодо якої встановлено обмежений доступ, може здійснюватись шляхом:

– мимовільної втрати;

– розголошення;

– несанкціонованого доступу до неї.

Під витоком інформації варто розуміти мимовільне поширення її через технічні або експлуатаційні особливості певних пристроїв, втрати, пошкодження, знищення всіх носіїв інформації в випадку стихійного лиха, розповсюдження даних через потрапляння комп’ютерних вірусів у систему, а також всі інші випадки, які не мають навмисного характеру.

Під розголошенням інформації, слід розуміти навмисну або необережну передачу повідомлень, опублікувань, оголошень, передань, наданні для ознайомлення, пересиланні, неможливості зберегти інформацію людьми, які мали до неї доступ через службові обов’язки і коли у цьому не було робочої необхідності.

Несанкціонований доступ до інформації розуміється як доступ до інформації, який здійснюється з порушенням установлених правил розмежування

доступу, тобто людьми, які не повинні були мати доступ до такої інформації, що призвело до небезпеки поширення, тому саме розмежуванню доступу та створення відповідних підрозділів з певним рівнем доступу до інформації та захищеними паролями є важливою частиною при створенні мережі.

В таблиці 1.1 наведено фактори, які створюють умови витоку (передання) банківської інформації, за дослідженнями спецслужб[].

Таблиця 1.1

Фактори витоку інформації

Фактори	%
Надмірна балакучість співробітників банків	32
Прагнення працівників банків заробляти гроші будь-яким способом і будь-якою ціною	24
Відсутність у банку системи заходів, спрямованих на захист інформації	14
Звичка співробітників банків ділитись один з одним почутими новинами, чутками, інформацією	12
Безконтрольне використання інформаційних систем	10
Наявність передумов для виникнення серед співробітників конфліктних ситуацій	8

Згідно даних наведених вище , можна зробити висновок, що здебільшого розповсюдження інформації третім особам відбувається саме від співробітників банку та через слабку чи взагалі відсутню систему захисту інформації. В зв’язку з цим, можна вивести два основні фактори, які повинний мати кожний банк для того, щоб зробити все можливе для захисту інформації в засобах і мережах її передачі та обробки, а також створення відповідної системи, яка б керувала порядком доступу, зберігання і використання не тільки конфіденційної а й будь-якої банківської інформації.

Для захисту, обробки, зберігання, передачу та інших видів маніпуляцій з даними в основному використовують апаратні, програмні та криптографічні

засоби. У свою чергу, апаратні засоби захисту (АЗЗ) застосовуються для вирішення таких завдань:

–перешкодження візуальному спостереженню та дистанційно-керованому підслуховуванню;

– нейтралізація паразитних електромагнітних випромінювань і наводок;

– виявлення технічних засобів підслуховування і магнітного запису, не санкціоновано встановлених в приміщенні банку;

– захист інформації, що передається засобами зв'язку та міститься в системах автоматизованої обробки даних.

На практиці всі заходи щодо використання АЗЗ в комерційного банку поділяються на три групи: організаційні, організаційно-технічні, технічні.

Організаційні засоби захисту:

Розробка організаційних засобів повинна належати до компетенції служби безпеки. Найчастіше експерти з безпеки:

- Розроблюють внутрішню документацію, яка визначає правила роботи з комп'ютерною технікою та конфіденційною інформацією.
- Забезпечують інструктаж та періодичні перевірки персоналу; ініціюють підписання додаткових угод до трудових договорів, які визначають відповідальність за розголошення або неправомірне використання інформації, пов'язаної з роботою.
- Розмежують обов'язки, щоб уникнути ситуацій, коли один працівник має в розпорядженні найважливіші файли даних; організовують роботу зі звичайними програмами робочого процесу та забезпечують збереження критичних файлів на мережевих накопичувачах.
- Інтегрують програмні продукти, що захищають дані від копіювання чи знищення будь-яким користувачем, включаючи вищий менеджмент компанії.
- Розроблюють плани відновлення системи у разі збоїв з будь-якої причини.

Технічні засоби захисту. Група технічних засобів поєднує апаратні та програмні засоби. Ось основні з них:

- Регулярне резервне копіювання та віддалене зберігання найважливіших файлів даних в комп'ютерній системі.
- Копіювання та резервне копіювання всіх мережевих підсистем, важливих для безпеки даних.
- Можливість перерозподілу мережевих ресурсів у разі несправності окремих елементів.
- Можливість використання резервних систем живлення.
- Забезпечення безпеки від пожежі чи пошкодження води.
- Встановлення вдосконалених продуктів, що захищають бази даних та іншу інформацію від несанкціонованого доступу.
- Комплекс технічних заходів включає заходи, які роблять засоби фізичної мережі фізично недоступними, наприклад, обладнання кімнат з камерами та сигналізацією.

Також, дуже важливим пунктом є захист інформації від копіювання і це виконується наступними функціями:

– ідентифікація середовища, з якого буде запускатись програма;
– аутентифікація середовища, із якого запущена програма;
– реакція на запуск із несанкціонованого середовища;
– реєстрація санкціонованого копіювання;
– протидія вивченню алгоритмів роботи системи.

Сьогодні на ринку послуг існують продукти, за допомогою яких будь-який банк може організувати надійну систему захисту інформації від несанкціонованого доступу та її неправомірного використання. Досить проаналізувати перераховані вище критерії та уважно вивчити ринок систем безпеки.

1.3 Аналіз інформаційної безпеки комерційного банку «Райффайзен Банк Аваль»

Аналіз існуючого стану інформаційної безпеки комерційного банку включає в себе низку складових, що так чи інакше впливають на інформаційну діяльність банку, забезпечення безпеки банківської інформації, капіталів, конфіденційних відомостей клієнтів, працівників тощо.

Тому можна виділити коло питань, які підлягають аналізу для побудови комплексної оцінки про стан захищеності інформації банківської структури, яка буде враховуватися під час розробки проекту модернізації підсистеми захисту інформаційно-комунікаційної мережі відділення комерційного банку та підсистеми захисту приміщення відділення банку від несанкціонованого доступу. До них відносяться:

– визначення джерел небезпеки (суб'єктів погроз);

– визначення потенційних об'єктів ураження та ресурсів їх захисту;

– оцінка ступеня ризику для різних категорій користувачів в банківській системі;

– аналіз складових забезпечення захисту банківської інформації.

Аналіз інформаційної безпеки комерційного банку «Райффайзен Банк Аваль» буде проводитися на прикладі Житомирського відділення № 1.

До суб'єктів погроз Житомирського відділення № 1 АТ «Райффайзен Банк Аваль» (P) відносяться:

– кримінальники або кримінальні групи, які з корисних міркувань можуть стати виконавцями незаконного втручання в діяльність банку(P_1);

– представники основного, допоміжного та технічного персоналу банку, які з корисних міркувань або під впливом погроз (вбивства, викрадення членів сімей, насильства), шантажу, залякування, чи винагороди можуть стати виконавцями незаконного втручання в діяльність банку(P_2);

– члени сімей або родичі працівників банку, які, використовуючи можливість доступу своїх близьких до цінностей банку, спроможні на підготовку та здійснення актів незаконного втручання в діяльність банку(P_3);

– хакери, крекери та інші комп'ютерні злодії, які з корисних міркувань або за для розваги можуть здійснювати незаконне втручання в діяльність банку, а саме в його інформаційно-телекомунікаційну складову(P_4);

– недобросовісні партнери(P_5);

– банки-конкуренти(P_6);

– колишні або дійсні працівники банку, які, на їхню думку, були звільнені або покарані безпідставно(P_7);

– представники наглядових організацій, аварійних служб та силових структур(P_8).

Їх можна представити у вигляді відкритого класифікаційного угрупування суб'єктів погроз (множини суб'єктів погроз):

$$P = \bigcup_{\eta} P_{\eta}, \tag{1.1}$$

де η – кількість категорій суб'єків погроз.

Побудуємо модель прояву суб'єктів погроз та представимо її на рисунку 1.2. Множину персоналу (N), який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність банку складають:

– працівники, що займають керівні посади в банку (N_1);

– працівники служби безпеки банку (N_2);

– працівники обслуговуючого персоналу банку (прибиральники, тощо) (N_3);

– працівники касового вузла, що мають безпосередній доступ до готівки та/або інших цінностей (N_4);

– представники технічного персоналу, що займаються життєзабезпеченням та обслуговуванням техніки (N_5);

– інші співробітники банку (N_6).

Множину потоку клієнтів банку (Z) складають:

– клієнти банку, що постійно користуються його послугами (Z_1);

– потенційні клієнти банку (Z_2) (особи, які цікавилися інформацією про банк та послуги, що він надає та ін.);

– контактні особи (Z_3) (особи, які співпрацюють зі структурними відділами банку: інкасатори, служба безпеки інкасаторів, представники КРУ та ін.);

– особи, що супроводжують клієнтів (потенційних клієнтів) на території банку (Z_4).

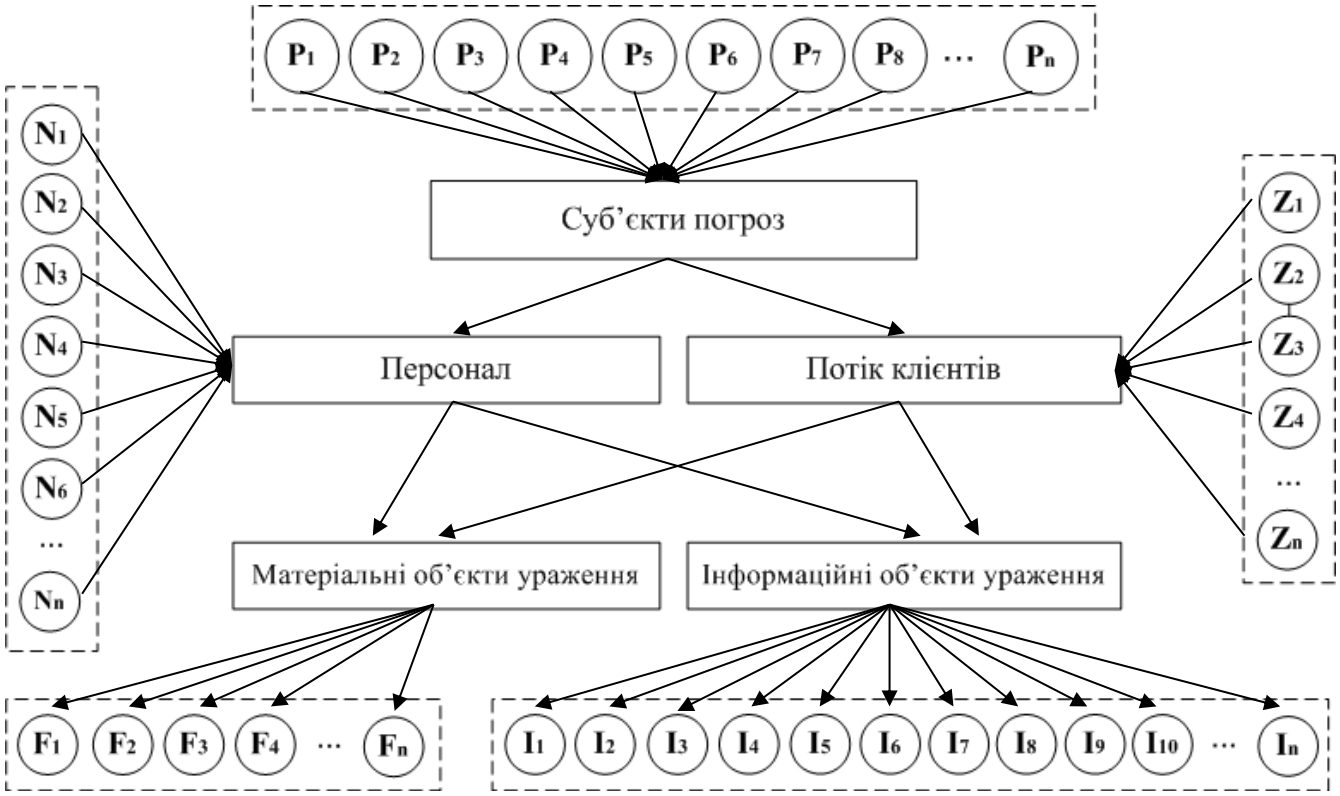


Рисунок 1.2 – Модель прояву суб'єктів погроз виникнення надзвичайних ситуацій на території банку

Отже, отримано наступні відкриті класифікаційні угрупування:

1. Множина персоналу (працівників банку), який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність банку:

$$N = \bigcup_{\gamma} N_{\gamma}\,, \tag{1.2}$$

де γ – кількість категорій персоналу.

2. Множина потоку клієнтів, який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність банку:

$$Z = \bigcup_{j} Z_j\,, \tag{1.3}$$

де j – кількість категорій клієнтів.

Потенційні об’єкти ураження можна поділити на два класифікаційні угрупування (групи):

1) об’єкти фізичного (матеріального) ураження;

2) об’єкти інформаційного ураження (інформаційні ресурси, засоби та системи інформатизації).

Множину об’єктів (F^P)фізичного ураження складають:

– матеріальні засоби (F_1^P) (споруди, будівлі банку, сховища, технічне обладнання, транспорт);

– фінансові кошти, валюта, цінності (F_2^P);

– персонал банку (F_3^P) (керуючі працівники, виробничий персонал, що має безпосередній доступ до фінансів, валюти, цінностям, сховищам, обізнані у відомостях, що становлять банківську та комерційну таємницю, працівники зовнішньоекономічних служб та ін.);

– технічні засоби та системи охорони та захисту матеріальних та інформаційних ресурсів (F_4^P).

Множину об’єктів інформаційного (I^P) ураження складають:

– інформаційні ресурси з обмеженим доступом, що становлять службову і комерційну таємницю (I_1^P);

– інша конфіденційна інформація на паперовій, магнітній, оптичної основі (I_2^P);

– інформаційні масиви та бази даних (I_3^P);

– програмне забезпечення (I_4^P);

– інформативні фізичні поля різного характеру (I_5^P);

– автоматизовані системи різного рівня та призначення (I_6^P);

– обчислювальні мережі різного рівня та призначення (I_7^P);

– лінії телеграфного, телефонного, факсимільного, радіо і оптичного зв'язку (I_8^P);

– технічні засоби передачі інформації (I_9^P);

– засоби розмноження і відображення інформації (I_{10}^P).

На підставі визначених суб’єктів та об’єктів погроз ресурси захисту умовно можна поділити на:

– нормативно-правові;

– людські (працівники банку, організаційне та управлінське забезпечення тощо);

– програмні;

– інженерно-технічні.

Ресурси захисту тісно переплітаються зі складовими забезпечення захисту інформації, що будуть розглянуті трохи нижче.

При створенні моделі порушника й оцінки ризику втрат від дій персоналу було проведено диференціювання всіх співробітників по їх можливостях доступу до системи і, отже, по потенційному збитку від кожної категорії користувачів.

Таким чином, кожен користувач у відповідності зі своєю категорією ризику може завдати більший або менший збиток системі. Крім того, було враховано, що користувачі різних категорій розрізняються не тільки за ступенем ризику, а й по тому, якому елементу системи вони загрожують найбільше. У результаті було оцінено ступінь ризику даної категорії користувачів щодо даного елемента

системи і представлено результати аналізу у вигляді таблиці відповідностей (див. табл.1.2).

У якості варіанту градації ризику було використано наступний:

- найвищий ризик (5);
- підвищений ризик (4);
- середній ризик (3);
- обмежений ризик (2);
- низький ризик (1);
- відсутність ризику (0).

Таблиця 1.2 – Ступінь ризику для різних категорій користувачів

	Елементи АС																	
	I			II			III			IV			V			VI		
Види погроз / Категорії користувачів	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
Начальник відділення банку	5	5	5		3	3		3	3	5	5	5		4	4	4	5	5
Начальник IT-сектору	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Системний адміністратор	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Спеціаліст по мережевому забезпеченню	4	5	5				4	5	5	5	5	5	5	5	5	3	4	4
Інженер-програміст	3	4	4	2	3	3				2	3	3				4	5	5
Спеціаліст по підтримці користувачів													4	5	5	5	5	5
Прикладний програміст	2	2	2	2	2	3							2	3	3			
Завідуючий касового вузла	5	5	5		2	2				1	2	2	5	5	5			
Рядовий касир	4	4	5		1	1				1	1	1	3	4	5			
Менеджер	4	4	4		1	1							4	4	4			
Начальник відділу безпеки	5	5	5	5	5	5	5	5	5	5	5	5	3	4	4	5	5	5
Адміністратор безпеки	5	5	5	5	5	5	5	5	5	2	3	4	3	4	4	5	5	5
Спеціаліст по периферійним пристроям											2	2	1	4	4		2	2

У якості вразливих елементів систем було використано:

– внутрішні дані (I);
– внутрішні прикладні програми (II);

– внутрішні системні модулі (III);

– зовнішні дані (IV);

– зовнішні системні модулі (V);

– елементи комп’ютера та інша апаратура (VI).

У якості видів погроз було використано:

– модифікація (A);

– руйнування (B);

– компрометація (розкриття) даних (C).

Як видно з таблиці, різні категорії користувачів можуть по-різному впливати на різні частини АС комерційного банку. Ці тонкощі будуть враховані як при проектуванні підсистем захисту, так і при її експлуатації.

Тепер перейдемо до аналізу моделі порушника. Модель порушника будуємо з урахуванням часу та місця виникнення надзвичайної ситуації, особливостей конкретної предметної області та технології обробки інформації.

Побудована модель порушника наведена в додатку __. В якості типів порушника були використані:

– основний персонал (ПЕРС);

– системні та програмні адміністратори (АДМ);

– керівники банку (КЕР);

– технічний персонал (ТЕХ);

– програмісти (ПРОГ);

– представники служби безпеки банку (СББ);

– хакери, крекери (ХАК);

– зовнішні порушники (ЗОВН).

Серед точок банківської системи, що піддаються атаці було виділено:

– комп’ютери користувачів (КомпКОР);

– база даних банку (БД);

– сервери (СЕРВ);

– комунікаційна мережа та мережеве устаткування (МЕРЕЖА);

– електромережа напругою 220 В (ЕлМер);

– банківські рахунки (БанкРах);

– платіжні картки (ПлКарт);

– носії інформації та місця їх зберігання.

Останнім етапом оцінки інформаційної безпеки банку є аналіз складових забезпечення захисту банківської інформації. Першою складовою захисту інформації, її теоретичною базою, є нормативно-правове забезпечення. До нього входять нормативні акти, закони та положення, встановленні як на державному рівні, так і безпосередньо правлінням банку.

Всі нормативно-правові документи, на які посилається діяльність Житомирського відділення АТ «Райффайзен Банк Аваль» можна поділити на дві групи:

– Закони України, постанови Національного Банку України та міжнародні стандарти в сфері інформаційної безпеки;

– постанови правління АТ «Райффайзен Банк Аваль» щодо захисту інформації.

Розглянемо детальніше кожну групу документів. Для початку проаналізуємо нормативно-правові документи на державному рівні.

До даної групи документів входять Закони України [22]:

– «Про інформацію»;

– «Про телекомунікації»;

– «Про захист інформації в інформаційно-телекомунікаційних системах»;

– «Про електронний цифровий підпис»;

– «Про банки і банківську діяльність»;

– «Про Національний банк України»;

– «Про платіжні системи та переказ коштів в Україні»;

Також до даної групи входять:

– Державний стандарт захисту інформації ДСТУ 3396;

– нормативний документ НДТЗІ 2.5-004;

– Міжнародний стандарт захисту інформації ISO/IEC 17799:2005;

– Указ Президента України «Про Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99»;

– Постанова Правління Національного Банку України «Про затвердження Правил технічного захисту інформації для приміщень банків, в яких обробляються електронні банківські документи» від 17 серпня 2007 року за №955/144222.

Вищеперераховані документи закріплюють права банку на інформацію, закладають правові основи інформаційної діяльності банку, встановлюють правову основу діяльності банку у сфері телекомунікацій та визначають повноваження держави щодо управління та регулювання зазначеною діяльністю.

Останні документи встановлюють вимоги та правила технічного захисту для приміщень з обмеженим доступом, комутаційних кімнат, серверних приміщень і приміщень електронних архівів, а також екранованих приміщень та систем електроживлення банків тощо.

Найголовнішим нормативним документом щодо захисту інформації другої групи є Постанова Правління АТ «Райффайзен Банк Аваль» «Про політику інформаційної безпеки АТ «Райффайзен Банк Аваль»» від 06.10.2009 № П-282/09.

Другим важливим нормативним документом є постанова Правління АТ «Райффайзен Банк Аваль» «Про правила роботи в інформаційно-обчислювальній системі АТ «Райффайзен Банк Аваль». Вимоги щодо інформаційної безпеки» від 13.07.2010 № П-196/10. Даний нормативний документ розроблений у відповідності до Політики інформаційної безпеки АТ «Райффайзен Банк Аваль» та Стандартів безпеки «Raiffaisen Group».

До організаційного забезпечення захисту інформації Житомирського відділення №1 АТ «Райффайзен Банк Аваль» відносяться:

– вимоги з інформаційної безпеки на робочих місцях;

– вимоги з інформаційної безпеки при роботі в локальній мережі;

– правила роботи з ресурсами Інтернет та електронною поштою;

– вимоги з інформаційної безпеки при роботі з платіжними та інформаційними системами;

– порядок дотримання внутрішньобанківського режиму.

Третьою складовою забезпечення захисту інформації є програмне забезпечення. В Житомирському відділенні як програмний засіб парольної ідентифікації обраний програмний продукт Access Denied 3.40. Як засіб шифрування інформації в Житомирському відділенні АТ «Райффайзен Банк Аваль» встановлена програма Secret Agent Pro 3.1.54. Secret Agent – засіб шифрування промислового рівня. У якості антивірусного програмного забезпечення використовується NOD 32, захищений паролем від відключення та зміни налаштувань.

Останнім і чи не найсуттєвішим елементом забезпечення захисту інформації є система технічного захисту, яка встановлена у відділенні банку. Основою даної складової є існуюча підсистема захисту приміщення відділення банку від несанкціонованого доступу , що буде розглянута в третьому розділі.

Висновки до першого розділу

1. Проведений аналіз роботи АТ «Райффайзен Банк Аваль» виявив основні напрямки діяльності банку та особливостей структури.

2. Аналіз методів та засобів забезпечення інформаційної безпеки комерційного банку виявив особливості проблем забезпечення, ризики, що призводять до втрати цілісності, конфіденційності й доступності. Виявлені ризики дозволили визначити задачі систем захисту інформації комерційних банків.

3. За допомогою аналізу банківської інформації та на підставі нормативно-правового забезпечення визначено обов’язкові заходи, що мають здійснювати банки щодо забезпечення захисту банківської таємниці. Визначено канали витоку інформації та заходи її захисту.

4. Проведений аналіз інформаційної безпеки комерційного банку дозволив сформувати множину суб’єктів погроз, визначити множину об’єктів ураження.

5. Проведено оцінку ступеню ризику для різних категорій користувачів.

2. МОДЕРНІЗАЦІЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ ЖИТОМИРСЬКОГО ВІДДІЛЕННЯ АТ «Райффайзен Банк Аваль»

2.1 Аналіз інформаційно-комунікаційної системи відділення комерційного банку «Райффайзен Банк Аваль»

Аналіз банківської інформаційно-комунікаційної системи включає в себе:

– дослідження приміщення, в якому знаходиться відділення банку;

– аналіз існуючої кабельної системи банку в тому числі комунікаційного та апаратного забезпечення;

– дослідження та аналіз існуючої топології інформаційно-комунікаційної мережі;

– дослідження та аналіз підсистеми захисту інформаційно-комунікаційної мережі.

Житомирське відділення «Райффайзен Банк Аваль» знаходиться за адресою м.Житомир, пл. Перемоги 10

Для даної організації характерними є те, що подібні організації обробляють великий об'єм коштів, тобто оперують конфіденційними відомостями, у тому числі персональними даними.

Відділення розташоване в центрі міста. З боку вулиці наявна автомобільна стоянка. З обох боків від відділення знаходяться бізнес-центри. Вікна виходять на дорогу та на обидві будівлі з правої та лівої сторони.

В кімнаті служби безпеки банку розташовано дві робочі станції, контролер сповіщувачів несанкціонованого доступу та відео-регістратор. Кабінет начальника банку розташований по праву сторону від кімнати СБ банку та має в наявності також дві робочі станції.

Приміщення операційно-касового вузла включає в себе відокремлені одна від одної каси №1 та № 2. В приміщенні розташовано по одній робочій станції на касу.

В серверному приміщенні розташований сервер та комутатор. Через службове приміщення здійснюється вихід з відділення банку через аварійний (запасний) вихід.

Кабінет для нарад служить для проведення переговорів з потенційними клієнтами, проведення закритих внутрішньобанківських нарад та для проведення переговорів з представниками сторонніх організацій, в тому числі і банків-конкурентів.

З кімнати ІТ-відділу відбувається адміністрування інформаційно-комунікаційною системою банку. Також ІТ-відділ забезпечує програмування, системний аналіз, мережеве забезпечення та технічну підтримку системи банку.

Хол займає найбільшу площу. В холі зосереджені корпоративний відділ та відділ роздрібної торгівлі відділення банку.

В мережі використовується кабель типу UTP категорії 5е. Це неекранована вита пара, специфікація 10Base-T, 100Base-TX. Швидкість передачі даних 100 Мбіт/с. Максимальна довжина сегменту 100 м. Кількість станцій в мережі: до 1024.

У якості серверу використовується HP NetServer LH 6000r D9114AV с одним процессором Pentium III Xeon 550 МГц /2 Мб.

Комутаційне обладнання являє собою комутатор та маршрутизатор. Як модель маршрутизатора використовується Cisco 3640. В якості комутатора використовується Cisco Linksys SRW2016-EU.

Загалом в Житомирському відділенні використовуються 20 персональних комп'ютерів. Персональні комп'ютери є двох конфігурацій. Перший вид робочих машин для звичайних працівників банку, другий – для керівного складу філіалу. Далі наведено конфігурації кожного типу:

Перший тип:

- Процесор: Core™ i3 8100
- Сімейство процесору: Intel Core i3
- Кількість ядер: 4 ядра
- Тактова частота ядру: 3,6 ГГц

- Графічне ядро: Intel HD Graphics 630
- ОЗП: 8 Гбайт
- Тип відеокарти: Інтегрована
- Відеокарта: Intel HD Graphics 630
- Об’єм HDD: 1000 Гб SATA III
- Операційна система: Windows 10

Другий тип:

- Процесор: Ryzen™ 5 3400G
- Сімейство процесору: AMD Ryzen 5
- Кількість ядер: 4 ядра
- Тактова частота ядру: 3.7 ГГц в режимі Boost 4.2 ГГц
- Графічне ядро: Intel HD Graphics 630
- ОЗП: 16 Гбайт
- Тип відеокарти: Інтегрована
- Відеокарта: AMD Radeon RX Vega
- Об’єм SSD 960 Гб
- Операційна система: Windows 10

Пристрої для вводу та виведенню інформації у всіх робочих машин однакові, а саме:

- Клавіатура та мишка фірми Logitech серії MX
- Монітор 24" Samsung S24R350 Dark Silver (LS24R350FHIXCI)
- Веб-камера Logitech C270 HD (960-001063)

Дані машини використовуються як офісні для обміну даними, формування звітності, здійснення банківських операцій, тощо.

Для виведення інформації працівники операційного залу використовують лазерні чорно-білі принтери Samsung SCX-3200. В касовому блоці для друку використовується термопринтер чеків Sprinter POS58Z. Також на касах використовуються POS-термінали (платіжні термінали) Hypercom Ice 5500Plus.

Для внутрішнього зв’язку та обміну документами у банку використовують електронну пошту та факси. Процес обміну (пересилки) інформацією

відбувається з відділень банку та мережі банкоматів до центрального офісу та навпаки, під час якого відбувається щоденна пересилка звітів та повідомлень до головного офісу в місті Києві. Зв'язок з головним офісом забезпечується за допомогою окремо прокладених волоконно-оптичних ліній між маршрутизаторами.

Після того, як наведено основне апаратне та комунікаційне забезпечення, зокрема локальна обчислювальна мережа, що побудована у відділенні банку, можна перейти до розгляду та аналізу принципу роботи самої мережі.

В даній мережі використовується шинна топологія. Типова шинна топологія має просту структуру кабельної системи з короткими відрізками кабелів. Тому в порівнянні з іншими топологіями вартість її реалізації невелика. Однак низька вартість реалізації компенсується високою вартістю управління. Фактично, найбільшим недоліком шинної топології є те, що діагностика помилок та ізолювання мережевих проблем можуть бути досить складними, оскільки тут є кілька точок концентрації.

Так як середовище передачі даних не проходить через вузли, підключені до мережі, втрата працездатності одного з пристроїв ніяк не позначається на інших пристроях. Хоча використання всього лише одного кабелю може розглядатися як перевага шинної топології, однак вона компенсується тим фактом, що кабель, який використовується в цьому типі топології, може стати критичною точкою відмови. Іншими словами, якщо шина обривається, то жодне з підключених до неї пристроїв не зможе передавати сигнали.

До серверу підключений комутатор рівня доступу. Сервер знаходиться в комутаційній (серверному приміщенні). Він збирає сигнали з усіх комп'ютерів, відеокамер та аудіо пристроїв запису. Важливим моментом є те, що інформація з серверів, які розташовані у кожному відділені, зчитується головним сервером, який знаходиться в Австрії, у Відні, в центральному банку «Raiffeisen Bank Group».

Останнім етапом дослідження існуючого стану інформаційно-комунікаційної системи Житомирського відділення «Райффайзен Банк Аваль» є аналіз підсистеми захисту.

Для повноцінного, ефективного та швидкого функціонування відділень і філій комерційного банку необхідна наявність оперативного доступу до серверу, бази даних та центрального офісу. Також має бути забезпечений постійний взаємозв'язок між центральним офісом та банкоматами. Для цього використання власної корпоративної мережі недоцільне, особливо зважаючи на кількість та місця розташування відділень банку на території країни. Більш розумно використовувати вже існуючу глобальну мережу Internet. Однак постає питання захисту даних, що передаються через незахищене середовище. Саме тому на даний момент основу підсистеми захисту мережі відділення банку складає використання віртуальної приватної мережі VPN.

Суть цієї технології VPN в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже встановленому з'єднанні організується зашифрований канал, що забезпечує високий рівень захисту інформації, що передається з цього каналу, за рахунок застосування спеціальних алгоритмів шифрування.

Віртуальні приватні мережі, що створюються на базі орендованих і комутованих каналів зв'язку, мереж загального користування (Internet), є чудовою альтернативою ізольованим корпоративним мережам, причому, альтернативою, що володіє рядом безсумнівних переваг:

– низька вартість орендованих каналів і комунікаційного обладнання розвинена топологія мережі;

– висока надійність;

– легкість масштабування (залучення нових мереж або користувачів);

– легкість зміни конфігурації;

– контроль подій і дій користувачів.

Існує багато варіантів віртуальних приватних мереж і яка саме була обрана буде наведено в розділі 2.3.

2.2 Аналіз топології та розробка системи адресації інформаційно-комунікаційної мережі

В даний момент у відділенні комерційного банку «Райффайзен Банк Аваль», як вже зазначалося, використовується шинна топологія. Дана топологія була проаналізована, були визначено її переваги та недоліки. Тому було вирішено модернізувати її на основі кабельної системи відділення банку.

Проектом модернізації кабельної системи передбачається використання зіркоподібної топології. Так як в Центральному відділенні АТ «Райффайзен Банк Аваль» є сервер, який контролює циркулювання інформації у всій мережі, до якої входять в тому числі і робочі станції операторів, банкомати та каси, то він буде виступати центральним вузлом в зіркоподібній топології (hub-маршрутизатором), яка є оптимальною для даного випадку.

Перевагами топології «зірка» є:

– підвищена стійкість мережі;

– легкість додавання/видалення нового комп'ютера в мережі, що є досить важливим, оскільки мережа банку постійно розширюється;

– простота діагностики і усунення неполадок (швидкість здійснення банківських операцій).

Проте є і деякі недоліки даної топології, такі як:

– підвищена витрата кабелю при прокладці мережі;

– необхідність придбання дорогого устаткування.

Але ці недоліки є незначними, оскільки рівень матеріальних затрат для організації, що представляє собою філію інтернаціонального банку досить

незначні. Використовуючи топологію «зірка», досить легко здійснювати підключення всіх робочих станцій до глобальної мережі Internet.

При побудові модернізованої мережі за основу було взято інформаційно-комунікаційну мережу європейських банків з представництвом в Україні АТ «Райффайзен Банк Аваль». Тобто, розробка мережі була зосереджена саме на філіалі то доступу до головного офісу. Маршрутизатори мережі, що проектується, будуть з'єднуватися між собою через певне незахищене середовище, а саме мережу Інтернет. Умовно мережу Інтернет буде представляти маршрутизатор , за допомогою якого буде реалізовано обрану топологію інформаційно-комунікаційної мережі.

Як вже зазначалося, за основу розрахунку адресації майбутньої мережі було взято інформаційно-комунікаційну мережу банків АТ «Райффайзен Банк Аваль».

Розрахунки мережі були зроблені для прикладу, для реального налаштування та створення мережі потрібно мати дані про кількість філіалів, відділів та робочих машин.

В нашому випадку, локальна мережа філіалу буде використовувати діапазон: 18.10.1.0 - 18.10.6.0. Кожний відділ має власну мережу та відокремлений у свій VLAN. Третій байт мережі відповідає номеру VLANy.

Таблиця 2.1 - Розрахунок адресації локальної мережі

Маска підмережі	11111111.11111111.11111111.00000000 255.255.255.0
Інвертована маска мережі	00000000.00000000.00000000.11111111 0.0.0.255
Адреса мережі	00010010.00001010.00000001.00000000 18.10.1.0
Мінімальна IP-адреса	00010010.00001010.00000001.00000001 18.10.1.1
Максимальна IP-адреса	00010010.00001010.00000110.11111110 18.10.6.254
Широкомовна IP-адреса	00001010.01010011.00001010.11111111 190.168.11.255

В нашому філіалі кожний відділ має по 5 робочих машин та у 6 VLANi знаходяться сервери та точка доступу. Номер адреси IP-вузла для мережі

становить 5 бітів, а з врахуванням майбутнього розширення обираємо 6 біт. Маска мережі: (32-6) = 26 біт.

Для прикладу наведено розрахунок IP-адресації для однієї внутрішньої підмережі офісу банку. Для адресації робочих станцій використовуємо діапазон: 18.10.2.2 – 18.10.2.100. З них 5 IP-адрес застосовуються для реальних робочих станцій, а інші зарезервовані для подальшого використання.

Для адресації комутатора використовуємо IP-адресу 18.10.2.1. Адресації всіх інших внутрішніх підмереж відділення банку розраховуються аналогічним чином. В таблиці 2.2 наведено приклад розрахунку IP-адресації.

Таблиця 2.2 – Розрахунок IP-адресації внутрішньої мережі регіонального офісу банку

Маска підмережі	11111111.11111111.11111111.00000000 255.255.255.0
Інвертована маска мережі	00000000.00000000.00000000.11111111 0.0.0.255
Адреса мережі	00010010.00001010.00000010.00000000 18.10.2.0
Мінімальна IP-адреса	00010010.00001010.00000010.00000001 18.10.2.1
Максимальна IP-адреса	00010010.00001010.00000010.01100100 18.10.2.100
Широкомовна IP-адреса	00010010.00001010.00000010.01100101 18.10.2.101

2.3 Обґрунтування вибору технології побудови інформаційно-комунікаційної системи комерційного банку

Як вже зазначалось в розділі 2.1 для забезпечення захищеного доступу до центрального офісу, потрібно налаштувати VPN. Для нашої мережі було обрано налаштувати IPsec VPN tunnel та OSPF для динамічної маршрутизації.

OSPF (Open Shortest Path First) — протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), що

використовує для знаходження найкоротшого шляху Алгоритм Дейкстри (Dijkstra's algorithm).

Протокол OSPF був розроблений IETF в 1988 році. Остання версія протоколу представлена в RFC 2328. Протокол OSPF являє собою протокол внутрішнього шлюзу (Interior Gateway Protocol — IGP). Протокол OSPF поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи.

OSPF був створений:

- Відкритим;
- Динамічним;
- Протоколом з врахуванням стану каналу;
- Внутрішньо шлюзовим протоколом;
- Ієрархічним;
- Наявна можливість забезпечити розподіл навантаження по каналам передачі з однаковою вартістю (метрикою);
- Має засоби захисту;
- Підтримує мереж різних типів;
- Підтримка VLSM та CIDR.
- Підтримка інкапсуляції IP.
- Підтримка передачі по всіх фізичних середовищах.
- Передача між маршрутизаторами не всієї таблиці, а лише їх зміни.
- Потребує меншого об’єму трафіку.
- Велика масштабованість.
- Ієрархія маршрутизації OSPF:
- Внутрішньо обласна маршрутизація – якщо адреса відправника і отримувача в пакеті знаходяться в межах однієї і тієї ж області.
- Міжобласна маршрутизація – якщо адреса відправника і отримувача в пакеті знаходяться в різних областях, але все ще відносяться до однієї і тієї ж автономної системи.

– Зовнішня маршрутизація – якщо адрес отримувача в пакеті знаходиться за межами автономної системи.

В OSPF використовується неструктурована метрика, яка представлена двійковим числом довжиною 16 біт, тому лежить в діапазоні 0…65535.

Дуже важливим є розуміння розрахунку ціни маршруту, оскільки за допомогою розрахунку, протокол знаходить найкоротший маршрут:

– cost = reference bandwidth / link bandwidth

Reference bandwidth це пропускна здатність, щодо якої вираховується, за замовчуванням вартість інтерфейсу. Вона дорівнює 100Mb, але може бути змінена.

Сумарна вартість маршруту вважається підсумовуванням вартості вихідних інтерфейсів шляхом передачі LSA. Для того щоб позначити недоступну мережу, OSPF використовує метрику рівну 16777215 (224 -1), яка вважається недосяжною метрикою для OSPF.

Отож, загальна інформація, історія створення, розрахунок маршрутів, це все зрозуміло, але для побудови якісної мережі, потрібно розуміти як працює протокол.

Опис роботи протоколу:

– Маршрутизатори обмінюються hello-пакетами через всі інтерфейси, на яких активований OSPF. Маршрутизатори, що розділяють загальний канал передачі даних, стають сусідами, коли вони приходять до домовленості при певних параметрах, зазначених в їх hello-пакетах.

– На наступному етапі роботи протоколу маршрутизатори будуть намагатися перейти в стан суміжності зі своїми сусідами. Перехід у стан суміжності визначається типом маршрутизаторів, які обмінюються hello-пакетами, і типом мережі, по якій передаються hello-пакети. OSPF визначає кілька типів мереж і кілька типів маршрутизаторів. Пара маршрутизаторів, що знаходяться в стані суміжності, синхронізує між собою базу даних стану каналів.

– Кожен маршрутизатор посилає оголошення про стан каналу маршрутизаторам, з якими він знаходиться в стані суміжності.

– Кожен маршрутизатор, який отримав оголошення від суміжного маршрутизатора, записує передану в ньому інформацію в базу даних стану каналів маршрутизатора і розсилає копію оголошення всім іншим суміжним з ним маршрутизаторам.

IPsec використовує два протокола для забезпечення безпечності трафіку – Authentication Header(AH) та Encapsulating Security Payload (ESP).

IP AH забезпечує цілісність без встановлення з'єднання, автентифікацію джерела даних та додаткову службу захисту від повтору. Він використовує хеш-алгоритм для вирахування значення хеша як для корисного навантаження так і для заголовку пакету, забезпечуючи цілісність пакету. Але, це викликає дуже специфічну проблему. Він не буде працювати через NAT-пристрій, тому що він змінює IP-заголовок пакета під час перекладу але значення хешу не змінюється. Таким чином, пристрій на іншій стороні буде думати, що пакет був змінений під час передачі і відхилить пакет.

Протокол ESP може забезпечувати конфіденційність та обмежену конфіденційність трафіку. Він також може забезпечувати підключення та цілісність без встановлення з'єднання, автентифікацію джерела даних та службу захисту від повтору. (Один чи інший набір цих служб безпеки повинен працювати кожний раз, коли викликається ESP.) Він виконує функції конфіденційності, автентифікації та цілісності. Таким чином, ESP виконує шифрування і по своїй суті більш безпечніший ніж AH. ESP вводить в пакет як додатковий заголовок так і трейлер.

Обидва протоколи є транспортними можливостями для контролю доступу на основі розподілення криптографічних ключей та управління потоками трафіку по відношенню до цих протоколів безпеки.

Вибір технологій був зроблений, перейдемо до наступного етапу проектування захищеної комп'ютерної мережі.

2.4 Обґрунтування вибору обладнання мережі

У даній мережі всі маршрутизатори було обрано фірми Cisco, серії 2900. Вони призначені для організацій, діяльність яких заснована на використанні передових технологій. Маршрутизатори Cisco серії 2900 з інтегрованими мережевими сервісами (ISR) забезпечують захищене високошвидкісне підключення робочих місць до мультисервісної мережі підтримку мультимедійних даних і відмінні експлуатаційні характеристики.

Маршрутизатори Cisco серії 2900 забезпечують:

1. Безперервне підключення до мережі: високий рівень доступності і тривалий час безвідмовної роботи за рахунок застосування ПО Cisco IOS апаратного резервування і засобів аварійного перемикання.

2. Універсальний набір сервісів: модульна підтримка щонайширшого набору мережевих і захисних сервісів Cisco, а також віртуальних сервісів, що настроюються, з доступом за запитом.

3. Колективна робота з високим рівнем безпеки: архітектура, підготовлена до передачі відео, підтримує мультимедійні можливості уніфікованих комунікацій.

4. Безпечний мобільний доступ: високошвидкісний безпровідний доступ дозволяє підвищити продуктивність праці співробітників, працюючих далеко від свого робочого місця.

5. Вбудовані засоби мережевої безпеки.

6. Гнучка підтримка мереж VPN: надання мобільному персоналу і віддаленим співробітникам безпечного доступу до ресурсів компанії по захищеному з'єднанню.

Всі маршрутизатори було обрано однакової моделі: Cisco 2911- VSEC-SRE/K9.

Швидкість фільтрації та просування кадрів – дві основні характеристики продуктивності комутатора. Ці характеристики є інтегральними показниками, вони не залежать від того, яким чином технічно реалізований комутатор.

Швидкість фільтрації визначає швидкість, з якою комутатор виконує перераховані нижче етапи обробки кадрів.

Основним критерієм вибору моделей комутаторів є кількість портів. Також враховується швидкість передачі цих портів. Моделі комутаторів, які були обрані для даної мережі:

В якості 24-портових комутаторів оберемо модель Cisco 2960 24 10/100 + 2 1000BT LAN Base Image (WS-C2960-24TT-L) та Cisco Catalyst 3560 24 10/100/1000T (WS-C3560G-24PS-S)

2.5 Налаштування захищеної інформаційно-комунікаційної мережі відділення комерційного банку «Райффайзен Банк Аваль»

В результаті проведених досліджень було запропоновано проект комп'ютерної мережі комерційного банку, яка представлена на рис.2.1.

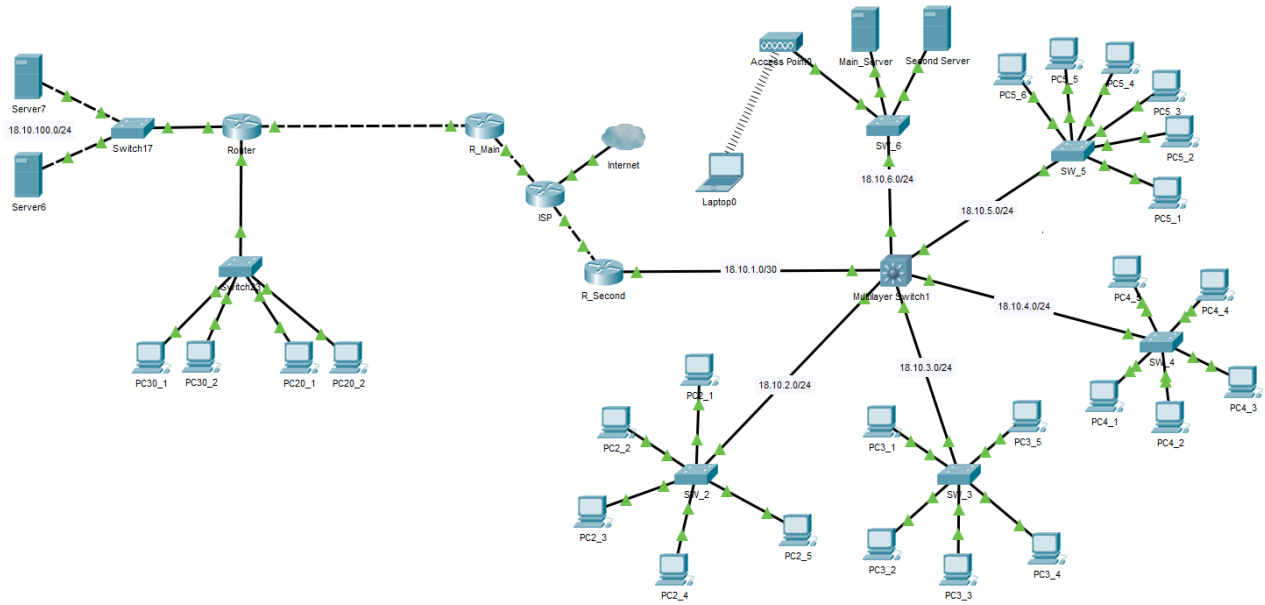


Рисунок 2.1 – Схема мережі побудованої в середовищі CPT

Базове налагодження захищеної інформаційно-комунікаційної мережі складатися з:

- налаштування інтерфейсів маршрутизаторів;
- налаштування маршрутизації мережі;
- налаштування IP-адресації робочих станцій.

У якості протоколу маршрутизації було обрано OSPF.

Файли конфігурації для всіх маршрутизаторів після базового налагодження наведено в додатку _.

В якості робочих станцій, як вже зазначалося, використовуються станції PC. Для генерації IP адрес було використано DHCP сервер, коректність роботи якої показана на рисунку 2.

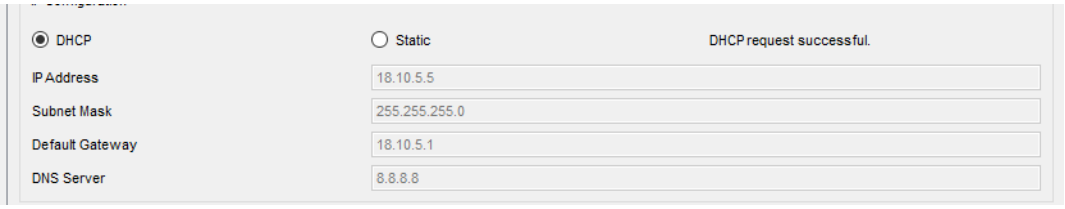


Рисунок 2.2 – Перевірка роботи DHCP

Після базових налаштувань було перевірено доступність вузлів мережі за допомогою команди: ping [address]. На рисунку __ наведено перевірку зв’язку між маршрутизатором R_Main та іншими маршрутизаторами (перевірка роботи зовнішньої мережі).

Як видно з рисунку 2.6, мережа функціонує правильно. Наступним завданням є створення шифрованої віртуальної приватної мережі між внутрішніми мережами. Більш детально цей етап розглянуто нижче.

```
R_Erste_1#ping 10.83.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.83.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 368/552/740 ms
R_Erste_1#ping 10.83.10.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.83.10.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 208/659/1012 ms
R_Erste_1#ping 10.83.10.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.83.10.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 560/920/1452 ms
```

Рисунок 2.3 – Перевірка роботи зовнішньої мережі

Далі безпосередньо перейдемо до налаштування захисту мережі. Як вже зазначалося, налаштування віртуальної приватної мережі складається з наступних кроків:

налаштування протоколу IPSec;

налаштування динамічної маршрутизації.

Налаштування протоколу IPSec відбувається в два етапи. Перший етап – це налаштування IKE, тобто створення політики безпеки isakmp. Другий етап – це налаштування IPSec-профілю.

Так як налаштування протоколу IPSec на всіх маршрутизаторах ідентичні, то розглянемо команди даних налаштувань на прикладі маршрутизатора головного офісу R_Main.

R_MAIN>#crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

crypto isakmp key secretkey address 210.210.200.1

crypto ipsec transform-set Main-Second esp-aes 256 esp-sha-hmac

crypto map IPSEC-MAP 10 ipsec-isakmp

set peer 210.210.200.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set Main-Second

match address 100

interface GigabitEthernet0/0

crypto map IPSEC-MAP

access-list 100 permit ip 18.10.10.0 0.0.0.255 18.10.1.0 0.0.0.255

Після успішного налаштування тунелю віртуальної приватної мережі, дуже важливо також налаштувати зашифрований доступ по ключу SSH. Для прикладу, він налаштований на нашому маршрутизаторі головного офісу R_Main, але за таким самим принципом налаштовується і на решті пристроїв.

hostname cisco-ssh

ip domain-name https://www.aval.ua/ru

crypto key generate rsa

line vty 0 4

access-class 18 in

exec-timeout 60 0

logging synchronous

transport input ssh

privilege level 15

ip ssh time-out 45

Однією з головних налаштувань також є динамічна маршрутизація. В даній мережі було обрано налаштовувати OSPF, опис якого був приведений на початку другого розділу. Нижче наведені налаштування для маршрутизатору R_Main, але ідентичні налаштування були проведені і на решті в нульовій зоні.

router ospf 1

log-adjacency-changes

network 210.210.100.0 0.0.0.255 area 0

network 18.10.10.0 0.0.0.3 area 0

Основні налаштування захисту мережі проведені і тепер перейдемо до тестування мережі. Але перед цим слід зазначити що також буде доцільно зазначити що одним важливим налаштуванням є RADIUS. Він допомогає налаштувати автентифікацію всіх користувачів, Але при обраному та вже налаштованому обладнанні, таке налаштування є неможливим. В майбутньому ці налаштування також будуть проведені.

Висновки до другого розділу

1. Було проаналізовано існуючу інформаційно-комунікаційну систему. Наведено її переваги та недоліки. У якості існуючої топології кабельної системи (горизонтальна підсистема) та мережі, що на її базі побудована, визначено топологію типу «шина».

2. Проведений аналіз дозволив розробити проект модернізованої кабельної системи та обрати у якості типу топології «зірку».

3. Було проаналізовано та обґрунтовано рішення щодо вибору технології побудови мережі, а саме віртуальної приватної мережі, наведено її переваги та недоліки.

4. Було розроблено схему IP-адресації модернізованої інформаційно-комунікаційної мережі.

5. Проведено налаштування захищеної інформаційно-комунікаційної мережі, включаючи базове налаштування та підсистему захисту мережі.

3. ТЕСТУВАННЯ ЗАХИЩЕННОЇ МЕРЕЖІ КОМЕРЦІЙНОГО БАНКУ

3.1 Перевірка доступності вузлів мережі

Перевірка доступності вузлів мережі здійснювалася за допомогою команд ping[address] та tracert/traceroute[address].

На рисунку 3.1 наведено результат роботи команди tracert до різних робочих станцій.

```
C:\>tracert 18.10.6.2

Tracing route to 18.10.6.2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      18.10.30.1
  2    0 ms      0 ms      0 ms      18.10.10.1
  3    1 ms      0 ms      0 ms      210.210.100.2
  4    0 ms      0 ms      11 ms     210.210.200.1
  5    1 ms      0 ms      13 ms     18.10.1.2
  6    0 ms      0 ms      11 ms     18.10.6.2

Trace complete.

C:\>tracert 18.10.2.5

Tracing route to 18.10.2.5 over a maximum of 30 hops:

  1    4294967293 ms0 ms       0 ms      18.10.30.1
  2    0 ms      0 ms      0 ms      18.10.10.1
  3    1 ms      0 ms      0 ms      210.210.100.2
  4    0 ms      0 ms      19 ms     210.210.200.1
  5    1 ms      0 ms      0 ms      18.10.1.2
  6    *         0 ms      0 ms      18.10.2.5

Trace complete.

C:\>tracert 18.10.1.1

Tracing route to 18.10.1.1 over a maximum of 30 hops:

  1    0 ms      0 ms      2 ms      18.10.30.1
  2    0 ms      10 ms     1 ms      18.10.10.1
  3    0 ms      0 ms      0 ms      210.210.100.2
  4    0 ms      12 ms     0 ms      18.10.1.1

Trace complete.

C:\>
```

Рисунок 3.1 – Перевірка доступності робочих станцій мережі

На рисунку 3.2 та 3.3 наведено результат роботи команди ping до різних робочих станцій.

```
C:\>ping 18.10.2.2

Pinging 18.10.2.2 with 32 bytes of data:

Request timed out.
Reply from 18.10.2.2: bytes=32 time=11ms TTL=123
Reply from 18.10.2.2: bytes=32 time=2ms TTL=123
Reply from 18.10.2.2: bytes=32 time=1ms TTL=123

Ping statistics for 18.10.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 4ms

C:\>ping 18.10.3.2

Pinging 18.10.3.2 with 32 bytes of data:

Request timed out.
Reply from 18.10.3.2: bytes=32 time<1ms TTL=123
Reply from 18.10.3.2: bytes=32 time=2ms TTL=123
Reply from 18.10.3.2: bytes=32 time=1ms TTL=123

Ping statistics for 18.10.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\>ping 18.10.4.2

Pinging 18.10.4.2 with 32 bytes of data:

Request timed out.
Reply from 18.10.4.2: bytes=32 time=11ms TTL=123
Reply from 18.10.4.2: bytes=32 time=12ms TTL=123
Reply from 18.10.4.2: bytes=32 time<1ms TTL=123

Ping statistics for 18.10.4.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
```

Рисунок 3.2 – Перевірка доступності робочих станцій мережі

```
C:\>ping 18.10.5.2

Pinging 18.10.5.2 with 32 bytes of data:

Request timed out.
Reply from 18.10.5.2: bytes=32 time<1ms TTL=123
Reply from 18.10.5.2: bytes=32 time=11ms TTL=123
Reply from 18.10.5.2: bytes=32 time=11ms TTL=123

Ping statistics for 18.10.5.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 7ms

C:\>ping 18.10.1.2

Pinging 18.10.1.2 with 32 bytes of data:

Reply from 18.10.1.2: bytes=32 time=5ms TTL=251
Reply from 18.10.1.2: bytes=32 time=1ms TTL=251
Reply from 18.10.1.2: bytes=32 time=12ms TTL=251
Reply from 18.10.1.2: bytes=32 time<1ms TTL=251

Ping statistics for 18.10.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 4ms

C:\>
```

Рисунок 3.2 – Перевірка доступності робочих станцій мережі

Для виводу інформації про налаштовану політику ISAKMP було використано команду show crypto isakmp policy (див. рис.3.3). Даною командою виводиться інформація про алгоритм шифрування, хеш-алгоритм, групу Diffie-Hellman, час життя політики безпеки та метод, що використовується для аутентифікації.

```
R_Main#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption
Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #5 (1536 bit)
        lifetime:                86400 seconds, no volume limit
```

Рисунок 3.3 – Вивід інформації про політику isakmp

За допомогою команди show crypto map та на прикладі маршрутизатора R_Main, виводяться всі криптографічні карти для інтерфейсів (див. рис. 3.3).

```
R_Main#show crypto map
Crypto Map IPSEC-MAP 10 ipsec-isakmp
        Peer = 210.210.200.1
        Extended IP access list 100
            access-list 100 permit ip 18.10.10.0 0.0.0.3
18.10.1.0 0.0.0.3
        Current peer: 210.210.200.1
        Security association lifetime: 4608000 kilobytes/86400
seconds
        PFS (Y/N): Y
        Transform sets={
                Main-Second,
        }
        Interfaces using crypto map IPSEC-MAP:
                GigabitEthernet0/0
```

Рисунок 3.3 – Вивід інформації про криптографічні карти

За допомогою команди show ip route було виведено таблицю маршрутизації центрального маршрутизатора (рис. 3.4).

```
R_Main#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 210.210.100.2 to network 0.0.0.0

     18.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
O       18.10.1.0/30 [110/3] via 210.210.100.2, 00:24:26, GigabitEthernet0/0
O IA    18.10.2.0/24 [110/4] via 210.210.100.2, 00:24:26, GigabitEthernet0/0
O IA    18.10.3.0/24 [110/4] via 210.210.100.2, 00:24:26, GigabitEthernet0/0
O IA    18.10.4.0/24 [110/4] via 210.210.100.2, 00:24:26, GigabitEthernet0/0
O IA    18.10.5.0/24 [110/4] via 210.210.100.2, 00:24:26, GigabitEthernet0/0
O IA    18.10.6.0/24 [110/4] via 210.210.100.2, 00:24:26, GigabitEthernet0/0
C       18.10.10.0/30 is directly connected, GigabitEthernet0/2
L       18.10.10.1/32 is directly connected, GigabitEthernet0/2
O IA    18.10.20.0/24 [110/2] via 18.10.10.2, 00:24:26, GigabitEthernet0/2
O IA    18.10.30.0/24 [110/2] via 18.10.10.2, 00:24:26, GigabitEthernet0/2
O IA    18.10.100.0/24 [110/2] via 18.10.10.2, 00:24:26, GigabitEthernet0/2
     210.210.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       210.210.100.0/24 is directly connected, GigabitEthernet0/0
L       210.210.100.1/32 is directly connected, GigabitEthernet0/0
S    210.210.200.0/24 [1/0] via 210.210.100.2
S*   0.0.0.0/0 [1/0] via 210.210.100.2
```

Рисунок 3.4 – Вивід таблиці маршрутизації для R_Main

3.2 Перевірка налаштованих параметрів\технологій захисту мережі.

Тепер можна перейти до тестування та перевірки технологій захисту та інших функцій нашої мережі. На рисунку 3.5 продемонстровано підключення по ключу SSH.

```
C:\>ssh -l admin 18.10.10.2

Password:
cisco-ssh#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cisco-ssh(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 18.10.10.1 to network 0.0.0.0

     18.0.0.0/8 is variably subnetted, 14 subnets, 3 masks
O       18.10.1.0/30 [110/4] via 18.10.10.1, 02:03:21,
```

Рисунок 3.5 – Підключення на маршрутизатор по SSH ключу

Як ми бачимо на рисунку, підключення з будь-якої робочої машини нашої мережі при наявності пароля надає всі можливості. На рисунку 3.6 зображено налаштований NTP та Syslog. Оскільки для коректної взаємодії системних повідомлень, нам потрібно бачити правильну та головне одну й ту саму дату та час, ці функції дуже тісно пов'язані між собою.

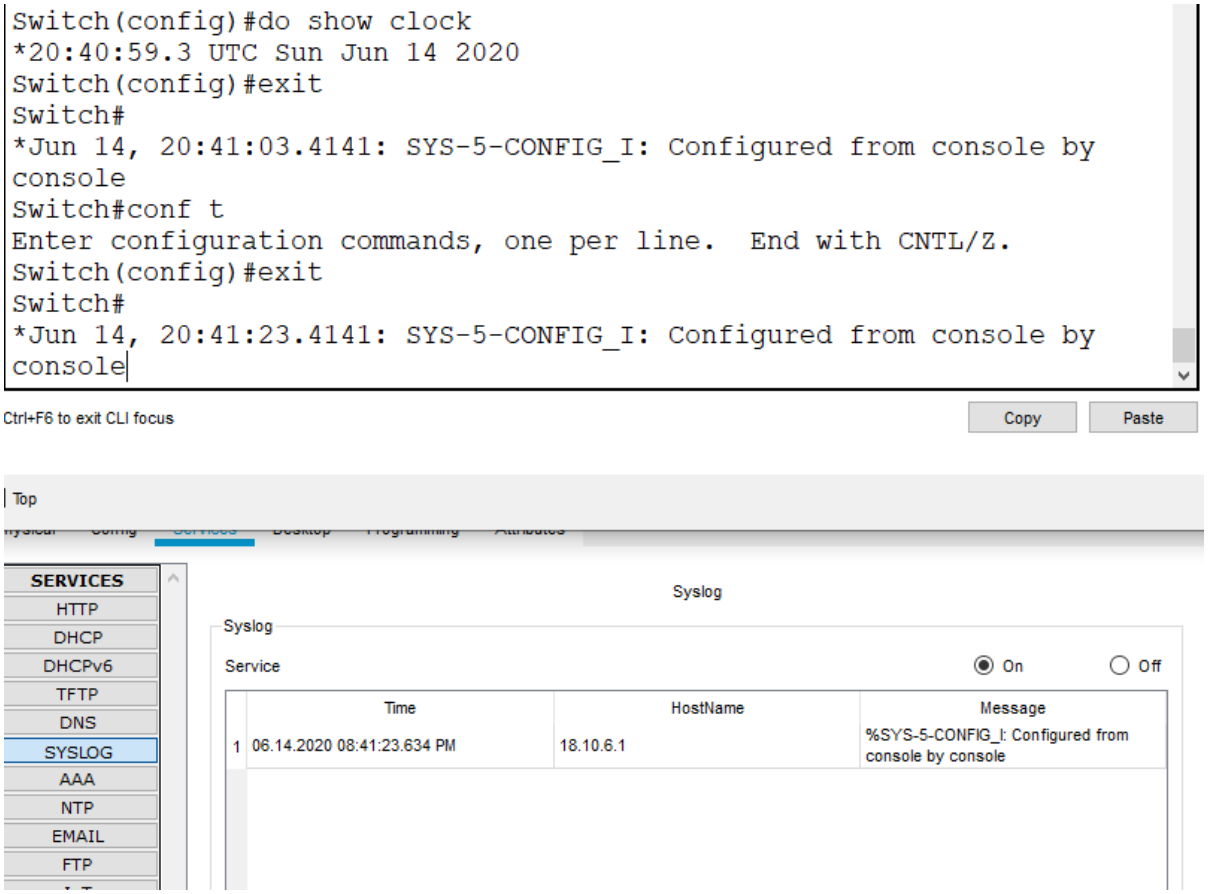


Рисунок 3.6 – Коректна робота NTP та Syslog

Звісно, жодна комерційна установа не може обійтись без бездротового підключення. В нашій мережі також була налаштована точка доступу, підключитись до якої може будь який пристрій з підтримкою даного підключення. На Рис. 3.7 зображено підключення умовного ноутбуку до нашої точки доступу за допомогою паролю.

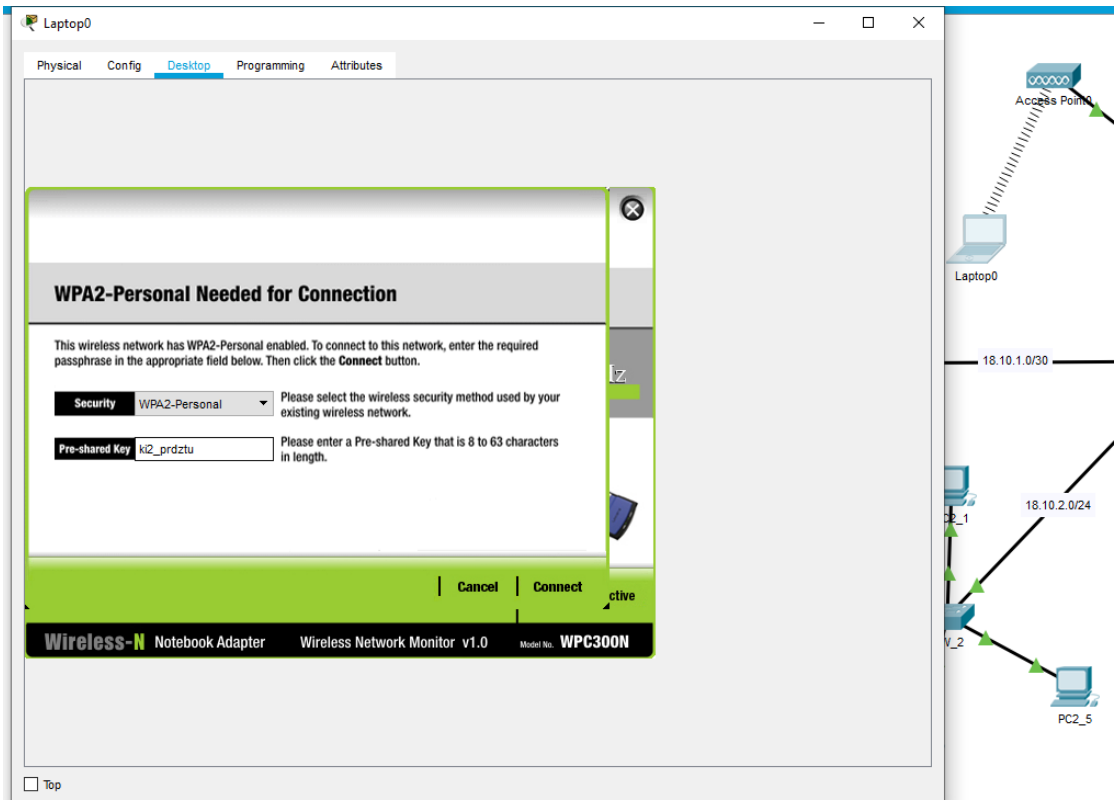


Рисунок 3.7 – Підключення до бездротової мережі

Висновки до третього розділу

1. В результаті проведених досліджень було запропоновано топологію комп'ютерної мережі та здійснено перевірку її працездатності шляхом перевірки доступності всіх елементів мережі.

2. Проведено перевірку налаштувань запропонованої комп'ютерної мережі комерційного банку.

4. ОХОРОНА ПРАЦІ В КОМЕРЦІЙНОМУ БАНКУ

4.1 Загальні вимоги до охорони праці в комерційному банку

Питання наукової організації праці, культури виробництва, ефективності праці нерозривно пов’язані з умовами й охороною праці. Правовою основою законодавства щодо охорони праці є Конституція України, Закони України: «Про охорону праці», «Про охорону здоров’я», «Про пожежну безпеку», «Про забезпечення санітарного та епідеміологічного благополуччя населення», а також кодекс законів про працю України.

Науково-технічний прогрес вніс серйозні зміни в умови виробничої діяльності працівників розумової праці. Їх праця стала більш інтенсивною, напруженою, яка вимагає значних витрат розумової, емоційної і фізичної енергії. Це потребує комплексного вирішення проблем ергономіки, гігієні і організації праці, регламентації режимів праці та відпочинку.

В даний час комп'ютерна техніка широко застосовується у всіх областях діяльності людини. При роботі з комп'ютером людина піддається дії ряду небезпечних і шкідливих виробничих факторів: електромагнітних полів (діапазонов радіочастот: ВЧ, УВЧ і СВЧ), інфрачервоного та іонізуючого випромінювань, шуму і вібрації, статичної електрики та ін.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням користувача, високою напруженістю зорової роботи і досить великим навантаженням на м'язи рук при роботі з клавіатурою ПЕОМ.

Велике значення має раціональна конструкція і розташування елементів робочого місця, що важливо для підтримки оптимальної робочої пози людини-користувача ПЕОМ.

У процесі роботи з комп'ютером необхідно дотримуватись правильного режиму роботи і відпочинку. В іншому випадку в персоналу, в даному випадку у всіх працівників банку, спостерігається значна напруга на зоровий апарат з появою скарг на незадоволеність роботою, головний біль, дратівливість,

порушення сну, втому і хворобливі відчуття в очах, в поясниці, в області шиї і руках.

4.2 Вимоги до виробничих приміщень

4.2.1 Фарбування і коефіцієнти віддзеркалення

Кольори приміщень і меблів повинні сприяти створенню сприятливих умов для зорового сприйняття, гарного настрою. Джерела світла, такі як світильники і вікна, які дають віддзеркалення від поверхні екрану, значно погіршують точність знаків і тягнуть за собою перешкоди фізіологічного характеру, які можуть виразитися в значній напрузі, особливо при тривалій роботі. Віддзеркалення, включаючи віддзеркалення від вторинних джерел світла, повинне бути зведено до мінімуму. Для захисту від надмірної яскравості вікон можуть бути застосовані штори та жалюзі.

В залежності від орієнтації вікон рекомендується наступне фарбування стін і підлоги:

1. Вікна орієнтовані на південь: стіни зеленувато-блакитного або світло-блакитного кольору, підлога – зеленого.

2. Вікна орієнтовані на північ: стіни світло-оранжевого або оранжево-жовтого кольору, підлога – червонувато-оранжевого.

3. Вікна орієнтовані на схід: стіни жовто-зеленого кольору, підлога – зеленого або червонувато-оранжевого.

4. Вікна орієнтовані на захід: стіни жовто-зеленого або голубувато-зеленого кольору, підлога – зеленого або червоно-оранжевого.

У приміщеннях, де знаходиться комп'ютер, необхідно забезпечити такі величини коефіцієнта віддзеркалення:

– для стелі: 60...70%;
– для стін: 40...50%;
– для підлоги: близько 30%;
– для інших поверхонь і робочих меблів: 30...40%.

4.2.2 Освітлення

Правильно спроектоване і виконане виробниче освітлення покращує умови зорової роботи, знижує стомлюваність, сприяє підвищенню продуктивності праці, благотворно впливає на виробниче середовище, створюючи позитивний психологічний вплив на працюючого, підвищує безпеку праці і знижує травматизм.

Недостатність освітлення приводить до напруги зору, ослаблює увагу, призводить до настання передчасної стомлюваності. Надмірно яскраве освітлення викликає осліплення, роздратування і різь в очах. Неправильний напрямок світла на робочому місці може створювати різкі тіні, відблиски, дезорієнтувати працівника. Всі ці причини можуть призвести до нещасного випадку або профзахворювання. Тому дуже важливо правильно розраховувати освітленість.

Існує три види освітлення: природне, штучне і поєднане (природне і штучне разом). Природне освітлення – освітлення приміщень денним світлом, що потрапляє через світлові прорізи в зовнішніх огороджуючих конструкціях приміщення. Природне освітлення характеризується тим, що змінюється в широких межах в залежності від часу дня, пори року, характеру області і ряду інших чинників. Штучне освітлення застосовується при роботі в темний час доби і вдень, коли не вдається забезпечити нормовані значення коефіцієнта природного освітлення (похмура погода, короткий світловий день). Освітлення, при якому недостатнє за нормативами природне освітлення доповнюється штучним, називається суміщеним освітленням.

Штучне освітлення поділяється на робоче, аварійне, евакуаційне, охоронне. Робоче освітлення, у свою чергу, може бути загальним або комбінованим. Загальне – освітлення, при якому світильники розміщуються у верхній зоні приміщення рівномірно, або, як розташоване устаткування. Комбіноване – освітлення, при якому до загального додається місцеве освітлення.

При виконанні робіт категорії високої зорової точності (найменший розмір об'єкта розрізнення 0,3...0,5 мм) величина коефіцієнта природного освітлення

(КПО) повинна бути не нижче 1,5%, а при зоровій роботі середньої точності (найменший розмір об'єкта розрізнення 0,5...1,0 мм) КПО повинен бути не нижче 1,0%. В якості джерела природного освітлення звичайно використовуються люмінісцентні лампи типу ЛБ, або ДРЛ, які попарно об'єднуються в світильники, які повинні розташовуватися над робочими поверхнями рівномірно.

Вимоги до освітленості в приміщеннях, де встановлені комп'ютери, наступні:

– при виконанні зорових робіт високої точності загальна освітленість повинна складати 300лк, а комбінована – 750лк;

– при виконанні робіт середньої точності – 200 і 300лк відповідно.

Крім того все поле зору повинне бути освітлено достатньо рівномірно – це основна гігієнічна вимога. Іншими словами, ступінь освітлення приміщення і яскравість екрану компьютера повинні бути приблизно однаковими, оскільки яскраве світло в районі периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності.

4.2.3 Параметри мікроклімату

Параметри мікроклімату можуть мінятися в широких межах, у той час як необхідною умовою життєдіяльності людини є підтримка постійності температури тіла завдяки терморегуляції, тобто здатності організму регулювати віддачу тепла в навколишнє середовище. Принцип нормування мікроклімату – це створення оптимальних умов для теплообміну тіла людини з навколишнім середовищем.

Обчислювальна техніка є джерелом істотних тепловиділень, що може привести до підвищення температури і зниження відносної вологості в приміщенні. У приміщеннях, де встановлені комп'ютери, повинні дотримуватися конкретні параметри мікроклімату. У санітарних нормах встановлені величини параметрів мікроклімату, що створюють комфортні умови. Ці норми встановлюються в залежності від пори року, характеру трудового процесу і характеру виробничого приміщення (див. табл. 4.1).

Рухливість повітря ефективно сприяє тепловіддачі організму людини і позитивно проявляється при високих температурах, але негативно – при низьких.

Об'єм приміщень, в яких розміщені працівники обчислювальних центрів, не повинен бути меншим 19,5 м^3 на людину з урахуванням максимального числа одночасно працюючих у зміну. Норми подачі свіжого повітря в приміщення, де розташовані комп'ютери, наведені в таблиці 4.2.

Таблиця 4.1 – Параметри мікроклімату для приміщень, де встановлені комп'ютери

Період року	Параметр мікроклімата	Величина
Холодний	Температура повітря в приміщенні	22…24 °С
	Відносна вологість	40…60 %
	Швидкість руху повітря	до 0,1 м/с
Теплий	Температура повітря в приміщенні	23…25 °С
	Відносна вологість	40…60 %
	Швидкість руху повітря	0,1…0,2 м/с

Таблиця 4.2 – Норми подачі свіжого повітря в приміщення, де розташовані комп'ютери

Характеристика приміщення	Об’ємний розхід свіжого повітря, що подається в приміщення, м^3 на одну людину за годину
Об’є м до 20 м^3 на людину	Не менше 30
20…40 м^3 на людину	Не менше 20
Більше 40 м^3 на людину	Природна вентиляція

Для забезпечення комфортних умов використовують як організаційні методи (раціональна організація проведення робіт залежно від пори року і доби,

чергування праці і відпочинку), так і технічні засоби (вентиляція, кондиціонування повітря, опалювальна система).

4.2.4 Шум і вібрація

Шум погіршує умови праці надаючи шкідливу дію на організм людини. Працівники, що працюють в умовах тривалого шумового впливу відчувають роздратованість, головні болі, запаморочення, зниження пам'яті, підвищену стомленість, зниження апетиту, біль у вухах і т.д. Такі порушення в роботі ряду органів і систем організму людини можуть викликати негативні зміни в емоційному стані людини до стресових.

Під впливом шуму знижується концентрація уваги, порушуються фізіологічні функції, з’являється втома у зв'язку з підвищеними енергетичними витратами і нервово-психічною напругою, погіршується мовна комутація. Все це знижує працездатність людини та її продуктивність, якість і безпеку праці. Тривалий вплив інтенсивного шуму (вище 80 дБ) на слух людини призводить до його часткової або повної втрати.

В таблиці 4.3 вказані граничні рівні звуку залежно від категорії тяжкості і напруженості праці, що є безпечними відносно збереження здоров'я і працездатності.

Таблиця 4.3 – Граничні рівні звуку на робочих місцях (дБ)

Категорія Напруженості праці	Категорія тяжкості праці			
	I. Легка	II. Середня	III. Тяжка	IV. Дуже тяжка
I. Мало напружена	80	80	75	75
II. Помірно напружена	70	70	65	65
III. Напружена	60	60	-	-
IV. Дуже напружена	50	50	-	-

Таким чином визначено основні обмеження щодо рівня звуку та вібрації на робочому місці, які дозволяють забезпечити належний рівень продуктивності праці.

4.2.5 Електромагнітне та іонізуюче випромінювання

Більшість вчених вважають, що як короткочасний, так і тривалий вплив всіх видів випромінювання від екрану монітора не небезпечно для здоров'я користувача, що працює з цими комп'ютерами. Проте вичерпних даних щодо небезпечності впливу випромінювання від моніторів на працюючих з комп'ютером не існує і дослідження спрямувані в цьому напрямку тривають.

Допустимі значення параметрів неіонізуючих електромагнітних випромінювань від монітора комп'ютера представлені в табл. 4. Максимальний рівень рентгенівського випромінювання на робочому місці користувача ПЕОМ зазвичай не перевищує 10мкбер / ч, а інтенсивність ультрафіолетового і інфрачервоного випромінювання від екрану монітора лежить в межах 10 ... 100мВт/м2.

Таблиця 4.4 – Допустимі значення параметрів неіонізуючих електромагнітних випромінювань

Назва параметра	Допустимі
Напруженість електричної складової электромагнітного поля на відстані 50 см від поверхні відеомонітора	10 В/м
Напруженість магнітної складової электромагнітного поля на відстані 50 см від поверхні відеомонітора	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати: 1) для дорослих користувачів; 2) для дітей дошкільного закладу і школярів середніх спеціальних і вищих учбових закладів.	 20 кВ/м 15 кВ/м

Для зниження дії цих видів випромінювання рекомендується застосовувати моніторинри зі зниженим рівнем випромінювання, встановлювати ззахисні екрани, а також регламентовані режими праці та відпочинку.

4.3 Ергономічні вимоги до робочого місця

Проектування робочих місць, забезпечених ЕОМ, відноситься до числа важливих проблем ергономічного проектування в області обчислювальної техніки. Робоче місце і взаємне розташування всіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи. Зокрема, при організації робочого місця співробітника комп'ютерного відділу повинні бути дотримані наступні основні умови:

– оптимальне розміщення обладнання, що входить до складу робочого місця;

– достатній робочий простір, що дозволяє здійснювати всі необхідні рухи і переміщення.

Ергономічними аспектами проектування комп'ютеризованих робочих місць, зокрема, є: висота робочої поверхні, розміри простору для ніг, вимоги до розташування документів на робочому місці (наявність і розміри підставки для документів, можливість різного розміщення документів, відстань від очей користувача до екрану, документа, клавіатури і т.д.), характеристики робочого крісла, вимоги до поверхні робочого столу, регульованість елементів робочого місця.

Головними елементами робочого місця співробітника є стіл і крісло. Робоча поза сидячи викликає мінімальне стомлення. Раціональне планування робочого місця передбачає чіткий порядок і сталість розміщення предметів, засобів праці і документації. Те, що потрібно для виконання роботи частіше, розташоване в зоні легкої досяжності робочого простору.

Моторне поле – простір робочого місця, в якому можуть здійснюватися рухливі дії людини.

Максимальна зона досяжності рук – це частина моторного поля робочого місця, обмеженого дугами, описуваними максимально витягнутими руками при русі в плечовому суглобі.

Оптимальна зона – частина моторного поля робочого місця, обмеженого дугами, описуваними передпліччями при русі в ліктьових суглобах з опорою в

точці ліктя і з відносно нерухомим плечом. На рис. 1 показаний приклад розміщення основних і периферійних складових ПК на робочому столі співробітника банку.

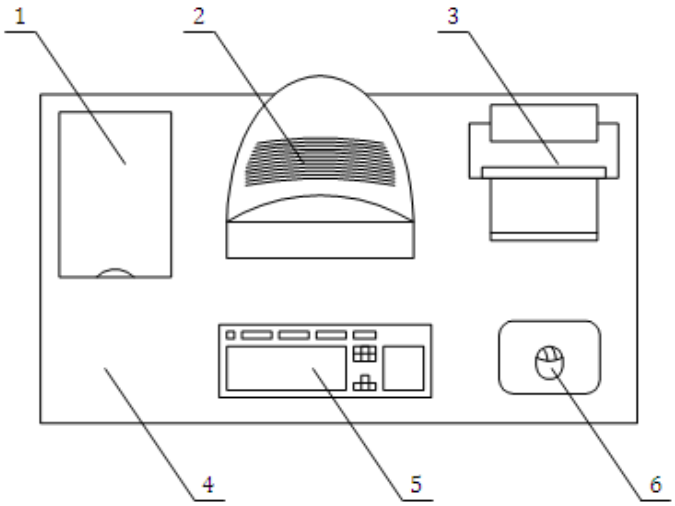


Рисунок 4.1 – Розміщення основних і периферійних компонентів ПК (1 – сканер, 2 – монітор, 3 – принтер, 4 – поверхня робочого столу, 5 – клавіатура, 6 – маніпулятор типу «мишка»)

Для комфортної роботи стіл повинен задовольняти наступним умовам:

1. Висота столу повинна бути вибрана з урахуванням можливості сидіти вільно, в зручній позі, при необхідності спираючись на підлокітники.

2. Нижня частина столу повинна бути сконструйована так, щоб працівник міг зручно сидіти, не був змушений підбирати ноги.

3. Поверхня столу повинна мати властивості, що виключають появу відблисків.

4. Конструкція столу повинна передбачати наявність висувних ящиків (не менше 3 для зберігання документації, лістингів, канцелярського приладдя).

5. Висота робочої поверхні рекомендується в межах 680-760 мм. Висота поверхні, на яку встановлюється клавіатура, повинна бути близько 650 мм.

Велике значення надається характеристикам робочого крісла. Так, рекомендована висота сидіння над рівнем підлоги перебуває в межах 420-550 мм.

Поверхня сидіння м'яка, передній край закруглений, а кут нахилу спинки – регульований.

Необхідно передбачати при проектуванні можливість різного розміщення документів: збоку від комп'ютера між монітором і клавіатурою і т.п. Крім того, у випадках, коли комп'ютер має низьку якість зображення, наприклад помітні блимання, відстань від очей до екрану роблять більше (біля 700 мм), ніж відстань від ока до документа (300-450 мм). Взагалі при високій якості зображення на моніторі комп'ютера відстань від очей користувача до екрану, документа і клавіатури може бути рівною.

Положення екрану визначається:

– відстанню зчитування (0,6 ... 0,7 м);

– кутом зчитування, напрямком погляду на 20° нижче горизонталі до центру екрану, при чому екран перпендикулярний цьому напрямку.

Повинна також передбачатися можливість регулювання екрану:

– по висоті: + 3 см;

– по нахилу від (-10°) до +20° відносно вертикалі;

– у лівому і правому напрямках.

Велике значення також надається правильній робочій позі користувача. При незручній робочій позі можуть з'явитися болі в м'язах, суглобах і сухожиллях. Вимоги до робочої пози користувача ПЕОМ наступні:

– голова не повинна бути нахилена більш ніж на 20°;

– плечі повинні бути розслаблені;

– лікті розташовуються під кутом 80°...100°;

– передпліччя і кисті рук розташовуються в горизонтальному положенні.

Причина неправильної пози користувачів обумовлена наступними чинниками:

– немає хорошої підставки для документів;

– клавіатура знаходиться дуже високо, а документи – низько;

– нікуди покласти руки і кисті;

– недостатньо простору для ніг.

Істотний вплив для продуктивної і якісної роботи на комп'ютері мають розміри знаків, густина їх розміщення, контраст і співвідношення яскравостей символів і фону екрану. Якщо відстань від очей користувача до екрану монітора складає 60 ... 80 см, то висота знака повинна бути не менше 3 мм. Оптимальне співвідношення ширини і висоти знака становить 3:4, а відстань між знакам – 15-20 % їх висоти. Співвідношення яскравості фону екрану і символів – від 1:2 до 1:15.

Під час користування комп'ютером медики радять встановлювати монітор на відстані 50-60 см від очей. Фахівці також вважають, що верхня частина комп'ютера повинна бути на рівні очей або трохи нижче. Коли людина дивиться прямо перед собою, його очі відкриваються ширше, ніж коли він дивиться вниз. За рахунок цього площа огляду значно збільшується, викликаючи обезводнення очей. До того ж якщо екран встановлено високо, а очі широко відкриті, порушується функція моргання. Це значить, що очі не закриваються повністю, не омиваються слізною рідиною, не отримують достатньо зволоження, що приводить до їх швидкого стомлювання.

Створення сприятливих умов праці і правильне естетичне оформлення робочих місць має велике значення як для полегшення праці, так і для підвищення його привабливості, позитивно впливає на продуктивність праці.

Висновки до четвертого розділу

1. Проведено аналіз загальних вимог щодо охорони праці в комерційному банку.

2. Визначено основні вимоги до виробничих приміщень щодо фарбування і віддзеркалення, освітлення, рівнів шуму та вібрації, параметрів мікроклімату, рівнів електромагнітного та іонізуючого випромінювань.

3. Визначено ергономічні вимоги щодо робочого місця.

ВИСНОВКИ

1. Проведений аналіз роботи АТ «Райффайзен Банк Аваль» виявив основні напрямки діяльності банку та особливості організаційної структури, особливості проблем забезпечення захисту інформації, ризики, що призводять до втрати цілісності, конфіденційності й доступності. Виявлені ризики дозволили визначити задачі систем захисту інформації комерційних банків.

2. За допомогою аналізу банківської інформації та на підставі нормативно-правового забезпечення визначено обов'язкові заходи, що мають здійснювати банки щодо забезпечення захисту банківської таємниці. Визначено канали витоку інформації та заходи її захисту.

3. Проведений аналіз інформаційної безпеки комерційного банку дозволив сформувати множину суб'єктів погроз, визначити множину об'єктів ураження. Проведено оцінку ступеню ризику для різних категорій користувачів.

4. Було проаналізовано існуючу інформаційно-комунікаційну систему відділення житомирської філії банку, визначено її переваги та недоліки. У якості існуючої топології кабельної системи (горизонтальна підсистема) та мережі, що на її базі побудована, визначено топологію типу «шина».

5. Проведений аналіз дозволив розробити проект модернізованої кабельної системи та обрати у якості типу топології «зірку». Проаналізовано та обґрунтовано рішення щодо вибору технології побудови мережі, а саме віртуальної приватної мережі, наведено її переваги та недоліки.

6. Було розроблено схему IP-адресації модернізованої інформаційно-комунікаційної мережі. Проведено налаштування захищеної інформаційно-комунікаційної мережі, включаючи базове налаштування та підсистему захисту мережі.

7. В результаті проведених досліджень було запропоновано топологію комп'ютерної мережі та здійснено перевірку її працездатності шляхом перевірки доступності всіх елементів мережі. Проведено перевірку налаштувань запропонованої комп'ютерної мережі комерційного банку.

8. Проведено аналіз загальних вимог щодо охорони праці в комерційному банку. Визначено основні вимоги до виробничих приміщень щодо фарбування і віддзеркалення, освітлення, рівнів шуму та вібрації, параметрів мікроклімату, рівнів електромагнітного та іонізуючого випромінювань. Визначено ергономічні вимоги щодо робочого місця.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Електронні ресурси

1. Райффайзен Банк Аваль. Режим доступу до ресурсу: https://www.aval.ua/about/info
2. Райффайзен Банк Аваль. Режим доступу до ресурсу: https://latifundist.com/kompanii/412-rajffajzen-bank-aval
3. ISP. Режим доступу до ресурсу: https://www.opennet.ru/base/cisco/2isp_link.txt.html
4. Radius. Режим доступу до ресурсу: https://www.packettracernetwork.com/tutorials/radiusconfiguration.html
5. Tacacs. Режим доступу до ресурсу: https://skeletor.org.ua/?p=225
6. Практична мережева безпека. Режим доступу до ресурсу: http://blog.netskills.ru/2017/01/network-security15.html
7. Create an IPsec VPN tunnel using Packet Tracer - CCNA Security. Режим доступу до ресурсу: https://www.youtube.com/watch?v=Z7LwU6H5IGE&t=378s
8. Create an IPsec VPN tunnel using Packet Tracer - CCNA Security. Режим доступу до ресурсу: https://www.youtube.com/watch?v=WkFCUa5b9-g
9. Видео уроки Cisco Packet Tracer. Курс молодого бойца. Syslog, NTP. Режим доступу до ресурсу: https://www.youtube.com/watch?v=LDGBT8dPalg&list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9&index=20
10. Видео уроки Cisco Packet Tracer. Курс молодого бойца. AAA. Режим доступу до ресурсу: https://www.youtube.com/watch?v=sltiryUaLhQ&list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9&index=21
11. OSPF. Режим доступу до ресурсу: http://xgu.ru/wiki/OSPF_в_Cisco
12. Настройка Site-To-Site IPSec VPN на Cisco. Режим доступу до ресурсу: https://wiki.merionet.ru/seti/20/nastrojka-site-to-site-ipsec-vpn-na-cisco/
13. Что такое IPsec - энциклопедия lanmarket.ua. Режим доступу до ресурсу: https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/ipsec.html
14. Настройка SSH в Cisco. Режим доступу до ресурсу: https://habr.com/ru/post/68262/
15. Доступ по протоколу SSH к оборудованию Cisco. Режим доступу до ресурсу: https://netclo.ru/dostup-po-protokolu-ssh-k-oborudovaniyu-cisco/

16. IP Калькулятор подсетей Онлайн. Режим доступу до ресурсу: http://infocisco.ru/ip_calculator.php
17. Cisco Packet Tracer – Cisco. Режим доступу до ресурсу: https://www.cisco.com/c/ru_ua/training-events/netacad/training-courses/cisco-packet-tracer.html
18. Packet Tracer – Configuring VPNs (Optional). Режим доступу до ресурсу: https://courses.cs.ut.ee/MTAT.08.004/2014_spring/uploads/Main/37_1.pdf
19. IPSec VPN Setup in Packet Tracer 7.1. Режим доступу до ресурсу: https://community.cisco.com/t5/vpn/ipsec-vpn-setup-in-packet-tracer-7-1/td-p/3212515
20. Національний Банк України. Режим доступу до ресурсу: https://bank.gov.ua/
21. Захист інформації в локальних мережах. Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97_%D0%B2_%D0%BB%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0%D1%85
22. Законодавство України. Режим доступу до ресурсу: https://www.rada.gov.ua/news/zak

ДОДАТКИ

Додаток А

ISP:

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn
FTX1524YR3L-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 210.210.100.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 210.210.200.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0/0
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/0/1
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/0/2
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/0/3
switchport mode access
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 210.210.200.0 0.0.0.255 area 0
network 210.210.100.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
!
line aux 0
!
```

```
line vty 0 4
login
!
!
!
End
```

R_Second:

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable secret 5
$1$mERr$a3YsdVsums0IOTq29pL.r1
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn
FTX1524T550-
license boot module c2900 technology-package
securityk9
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key secretkey address
210.210.100.1
!
!
!
crypto ipsec transform-set Second-Main esp-
aes 256 esp-sha-hmac
!
crypto map IPSEC-MAP 10 ipsec-isakmp
set peer 210.210.100.1
set pfs group5
set security-association lifetime seconds 86400
set transform-set Second-Main
match address 100
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 210.210.200.1 255.255.255.0
duplex auto
speed auto
crypto map IPSEC-MAP
!
interface GigabitEthernet0/1
ip address 18.10.1.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 18.10.1.0 0.0.0.3 area 0
network 210.210.200.0 0.0.0.255 area 0
!
ip classless
ip route 210.210.100.0 255.255.255.0
210.210.200.2
ip route 0.0.0.0 0.0.0.0 210.210.200.2
!
ip flow-export version 9
!
!
```

```
access-list 100 permit ip 18.10.1.0 0.0.0.3
18.10.10.0 0.0.0.3
!
no cdp run
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
End
```

R_Main:

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R_Main
!
!
!
enable secret 5
$1$mERr$a3YsdVsums0IOTq29pL.r1
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn
FTX1524L6IB-
license boot module c2900 technology-package
securityk9
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key secretkey address
210.210.200.1
!
!
!
crypto ipsec transform-set Main-Second esp-
aes 256 esp-sha-hmac
!
crypto map IPSEC-MAP 10 ipsec-isakmp
set peer 210.210.200.1
set pfs group5
set security-association lifetime seconds 86400
set transform-set Main-Second
match address 100
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 210.210.100.1 255.255.255.0
duplex auto
speed auto
crypto map IPSEC-MAP
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
ip address 18.10.10.1 255.255.255.252
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
```

```
!
router ospf 1
log-adjacency-changes
network 210.210.100.0 0.0.0.255 area 0
network 18.10.10.0 0.0.0.3 area 0
!
ip classless
ip route 210.210.200.0 255.255.255.0
210.210.100.2
ip route 0.0.0.0 0.0.0.0 210.210.100.2
!
ip flow-export version 9
!
!
access-list 100 permit ip 18.10.10.0 0.0.0.3
18.10.1.0 0.0.0.3
!
no cdp run
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
End
```

Multilayer Switch1:

```
version 12.2(37)SE1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
enable secret 5
$1$mERr$x7SYHiyAzJ8uzNVsfkVgY.
!
!
!
!
!
aaa new-model
!
aaa authentication login default group radius
local
!
!
!
!
!
!
ip routing
!
!
!
!
username ki2 privilege 15 secret 5
$1$mERr$MT2EIHydWsBHs/826Bj6w/
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/4
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/5
```

```
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/6
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
no switchport
ip address 18.10.1.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan2
mac-address 0090.2166.0801
ip address 18.10.2.1 255.255.255.0
ip helper-address 18.10.6.2
!
interface Vlan3
mac-address 0090.2166.0802
ip address 18.10.3.1 255.255.255.0
ip helper-address 18.10.6.2
!
interface Vlan4
mac-address 0090.2166.0803
ip address 18.10.4.1 255.255.255.0
ip helper-address 18.10.6.2
!
interface Vlan5
mac-address 0090.2166.0804
ip address 18.10.5.1 255.255.255.0
ip helper-address 18.10.6.2
!
interface Vlan6
mac-address 0090.2166.0805
ip address 18.10.6.1 255.255.255.0
!
router ospf 1
log-adjacency-changes
network 18.10.2.0 0.0.0.255 area 1
network 18.10.3.0 0.0.0.255 area 1
network 18.10.4.0 0.0.0.255 area 1
network 18.10.5.0 0.0.0.255 area 1
network 18.10.6.0 0.0.0.255 area 1
network 18.10.1.0 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 18.10.1.1
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
```

```
logging trap debugging
logging 18.10.6.2
line con 0
!
line aux 0
!
line vty 0 4
!
!
!
ntp server 18.10.6.2
!
End
```

Router:

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname cisco-ssh
!
!
!
enable secret 5
$1$mERr$Wvx.LTtFcAE2XceYvNFIH.
!
!
!
!
!
aaa new-model
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5
$1$mERr$Wvx.LTtFcAE2XceYvNFIH.
!
!
license udi pid CISCO2911/K9 sn
FTX1524SJHR-
!
!
!
!
!
!
!
!
!
ip ssh time-out 45
ip domain-name https://www.aval.ua/ru
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 18.10.10.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 18.10.100.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2.20
encapsulation dot1Q 20
ip address 18.10.20.1 255.255.255.0
!
interface GigabitEthernet0/2.30
encapsulation dot1Q 30
ip address 18.10.30.1 255.255.255.0
!
interface FastEthernet0/0/0
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/0/1
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/0/2
switchport mode access
```

```
switchport nonegotiate
!
interface FastEthernet0/0/3
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/1/0
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/1/1
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/1/2
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/1/3
switchport mode access
switchport nonegotiate
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 18.10.10.0 0.0.0.3 area 0
network 18.10.20.0 0.0.0.255 area 1
network 18.10.30.0 0.0.0.255 area 1
network 18.10.100.0 0.0.0.255 area 1
!
ip classless
ip route 0.0.0.0 0.0.0.0 18.10.10.1
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
access-class 18 in
exec-timeout 60 0
logging synchronous
transport input ssh
privilege level 15
!
!
ntp server 18.10.100.101
!
End
```

SW_2:

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk allowed vlan 2
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/7
!
```

```
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End
```

SW_3:

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk allowed vlan 3
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
```

```
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End
```

SW_4:

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk allowed vlan 4
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 4
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 4
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 4
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 4
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 4
switchport mode access
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
```

```
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End
```

SW_5:

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk allowed vlan 5
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 5
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 5
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 5
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 5
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 5
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 5
switchport mode access
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
```

```
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End
```

SW_6:

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk allowed vlan 6
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 6
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 6
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 6
switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
```

```
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
logging trap debugging
logging 18.10.6.2
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End
```

Switch17:

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
```

```
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End
```

Switch23:

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk allowed vlan 20,30
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
```

```
login
!
!
!
!
end
```