МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Кафедра електроніки і комп’ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи магістра на тему:

«Розподілена система маршрутизації даних»

Завідувач кафедрою	А.С. Опанасюк
Керівник роботи	О.В. Бережна
Консультант з техніко-економічної частини	О.М. Маценко
Проектував студент	П.В. Клець

Суми
2020 р.

Сумський державний університет

Факультет Заочний **Кафедра** Електроніки і КТ
Спеціальність Електронні системи та компоненти

ЗАТВЕРДЖУЮ:
Зав. кафедри Опанасюк А.С.
«____» _____ 20__ г.

ЗАВДАННЯ

ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ МАГІСТРА СТУДЕНТУ

Клець Павел Володимирович

1. Тема роботи «Розподілена система маршрутизації даних»

затверджено наказом від «06» листопада 2020 р. № 1727-III

2. Термін здачі студентом закінченого проекту 15.12.20

3. Вихідні дані до роботи Розробити пристрій, який буде задовольняти наступні вимоги: кількість портів – 4; тип мережі – Ethernet; реалізувати алгоритм захисту від несанкціонованого доступу.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які підлягають розробці) Вступ. Огляд літератури та постановка завдання. Науково-дослідна частина. Розробка алгоритму функціонування та структурної схеми системи. Розробка схеми електричної функціональної пристрою. Розробка та розрахунок принципових електричних схем вузлів та блоків пристрою. Техніко-економічна частина. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
1 Схема алгоритму.
2 Схема електрична структурна.
3Схема електрична функціональна.
4Схема електрична принципова.

6. Консультанти до проекту (работи), з зазначенням розділів проекту, що до них відносяться

Розділ	Консультант	Підпис, дата	
		Завдання надав	Завдання прийняв
Економіка	Маценко О.М.		

7. Дата надання завдання_____

Керівник_____
(підпис)

Завдання прийняв до виконання_____
(підпис)

Календарний план

№ п/п	Найменування етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1.	Огляд технічної літератури	10.10.20	
2.	Науково-дослідна частина	20.10.20	
3.	Розробка алгоритму функціонування та структурної схеми	30.10.20	
4.	Розробка схеми електричної функціональної	10.11.20	
5.	Розробка схеми електричної принципової	20.11.20	
6.	Розробка техніко-економічної частини	25.11.20	
7.	Оформлення графічної частини	05.12.20	
8.	Оформлення пояснювальної записки	10.12.20	
9.	Рецензування та підготовка до захисту	15.12.20	

Студент-дипломник _____

Керівник проекту _____

РЕФЕРАТ

Пояснювальна записка містить: 92 аркушів, 32 рисунків, 7 таблиць, 18 джерел літератури.

Графічна частина роботи містить: схеми алгоритму та схеми електричної структурної «маршрутизуючого сервісу», схеми алгоритму функціонування маршрутизатора, схеми електричної структурної, функціональної та принципової.

Пояснювальна записка містить шість розділів: огляд літератури та постановку завдання, науково-дослідну частину, розроблення алгоритму функціонування та структурної схеми системи передачі даних, розроблення схеми електричної функціональної пристрою кодування, розроблення схеми електричної принципової пристрою кодування та техніко-економічну частину.

Перший розділ містить огляд технічної літератури за обраним напрямом роботи, розглянуті питання, пов'язані з актуальністю використання безпровідних систем та захисту інформації.

У другому розділі наведені результати наукового дослідження. Розглянуто проблеми інформаційної безпеки бездротових мереж, основні підходи до вирішення цих проблем, а також наведений аналіз існуючих методів та алгоритмів виявлення мережевих атак. Розроблено схему-алгоритму та структурну схему «маршрутизуючого сервісу» на основі динамічної маршрутизації.

Третій розділ присвячений розробленню алгоритма функціонування та схеми електричної структурної системи.

У четвертому розділі розглядається розроблення схеми електричної функціональної маршрутизатора. маршрутизатора

П'ятий розділ містить розроблення схеми електричної принципової маршрутизатора, виконано розрахунок основних вузлів та блоків, розроблено програмне забезпечення.

Шостий розділ присвячений питанням економіки: розглядається оцінка ефективності інформаційних систем та приводиться розрахунок собівартості та оптової ціни пристрою, що розроблюється.

ЗМІСТ

ВСТУП

Сучасний рівень розвитку виробництва характеризується широким впровадженням перспективних комп'ютерних технологій в різних сферах людської діяльності. Нові інформаційні технології активно впроваджуються в усі сфери діяльності держави. Інформаційні мережі обслуговують та управляють банківськими системами, космічними об'єктами, контролюють роботу атомних електростанцій, а також розподіляють електроенергію [1].

Інформатизація технологічних процесів виробництва є характерною рисою існування сучасного суспільства. Інформаційно-комунікаційні системи передачі даних є основою обміну інформаційними ресурсами, завдяки яким здійснюється зберігання, передача й обробка інформації, а також надання послуг споживачам з умов впровадження найсучасніших технологій.

Широке впровадження інформаційно-комунікаційних систем і мереж є основою сучасного функціонування організацій та підприємств. Такий підхід відкриває можливість підвищити ефективність діяльності компаній за рахунок використання більш оперативної й повної інформації, а також розширяє нові можливості для взаємодії з потенційними клієнтами за допомогою загальнодоступних глобальних інформаційних мереж [2].

Новітні інформаційно-комунікаційні технології відкрили можливість об'єднати корпоративні мережі в глобальне інформаційне середовище. Це призвело до появи такого унікального явища, як глобальні інформаційні системи та мережі передачі даних. Концепція організації інформаційно-комунікаційних мереж є логічним результатом розвитку інформаційних технологій та їх упровадження в усі сфери діяльності сучасного суспільства [2].

Основна функція інформаційно-комунікаційних систем та мереж в умовах функціонування інтегрованих інформаційних комплексів полягає в організації оперативного та надійного обміну інформацією між абонентами, а також у скороченні витрат на передачу даних. Разом з перевагами застосування глобальних інтегрованих інформаційних систем та мереж передачі даних з'явилися дуже небезпечні ризики, стосовно взаємодії з відкритим та неконтрольованим зовнішнім інформаційним середовищем. Стало очевидним, що надійність функціонування інтегрованих інформаційних комплексів залежить не тільки від рівня захисту інформаційних даних в системі від несанкціонованого доступу, а також характеризується рівнем застосування

сучасних технологій та методів захисту інформації від зовнішнього середовища та руйнівних програмних впливів [1, 2].

Досвід застосування комп’ютерних засобів і технологій управління виробництвом стимулював проведення нових наукових досліджень в сфері розробки нових принципів організації та методів синтезу систем комплексного захисту інформації. Важливість проблеми організації безпеки інформаційних технологій, обумовлені такими причинами [3]:

– різким збільшення обсягів інформаційних потоків даних, що обробляється і передається каналами зв’язку та значним зростанням потужності сучасних автоматизованих комплексів;

– високим темпом росту сучасних інформаційних технологій у всіх сферах діяльності суспільства, і як наслідок, зростанню кількості розподілених баз даних різного призначення й інтеграції до сучасного інформаційного простору;

– поширенню сучасних комутативних та безкомутативних мережних технологій і значному розширенню кількості джерел інформації та кола користувачів, які мають безпосередній доступ до інформаційних ресурсів та широкого спектру послуг, що надаються інформаційними системами.

Актуальність роботи. Розвиток інформаційних технологій ставить актуальні завдання підвищення надійності функціонування комп'ютерних мереж. Для вирішення таких завдань необхідні дослідження існуючих мережевих протоколів, мережевих архітектур, розробка способів підвищення безпеки при передачі інформаційних ресурсів мережі.

Наукова новизна. Запропоновано методику захисту інформації в розподілених безпровідних мережах, заснована на застосуванні програми «маршрутизируючий сервіс».

1 ОГЛЯД ЛІТЕРАТУРИ ТА ПОСТАНОВКА ЗАДАЧІ ПРОЕКТУВАННЯ

1.1 Комп'ютерна мережа

Для з'ясування поняття маршрутизація, введемо початкові визначення.

Комп'ютерна мережа - сукупність обладнання (комп'ютери, сервери, засобів комутації та ін.), поєднана каналами зв'язку, що представляє єдину систему для обміну інформацією. Мережу можна представити у вигляді графа, в якому вузли відіграють роль мережевого обладнання, а ребра, що з'єднують вузли - канали зв'язку. Вузли можуть бути кінцевими, проміжними або суміжними. Устаткування може бути пов'язано один з одним різними способами [4].

Поєднання всіх компонентів мережі називають топологією. Існує безліч способів з'єднання обладнання [2, 5].

Приклади найбільш поширених топологій [1, 2, 6]:

– шина (рис. 1.1). Всі пристрої з'єднуються за допомогою одного кабелю, на кінцях знаходяться термінатори, що запобігають відображення сигналу. Повідомлення, надіслане з однієї машини, пересилається всім, і тільки та, якій воно адресовано, буде його обробляти. Така побудова мережі відрізняється дешевизною і простими налаштуваннями. мінус в тому, що при виході з ладу загального кабелю або термінатора система відмовить у роботі. Так само важко знайти несправність на мережі;

– кільце (рис. 1.2). Устаткування підключається тільки до двох своїх сусідів. Дані передаються від пристроя до пристрою в одному напрямку, внаслідок чого не виникає колізій пакетів даних. Кожен пристрій чекає своєї черги для передачі даних. При відмові будь-якого обладнання вся система виходить з ладу, і знайти несправність складно;

– зірка (рис. 1.3). До центрального вузла підключаються всі робочі станції, в разі їх відмови система не вийде з ладу. Але в разі відмови центрального вузла вся мережа стає не працездатною. Тим не менш, цей вид топології відрізняється високою продуктивністю, при правильному проектуванні мережі, і легкістю пошуку несправностей;

– подвійне кільце (рис. 1.4). У цьому варіанті кільцевої топології буде створено друге кільце для передачі даних в обох напрямках. Система стає більш відмовостійкої;

– дерево (рис. 1.5). Різновид топології зірка. Відмінності лише в тому, що схема складніша і дотримується ієрархічність;

– повнозв'язна (рис. 1.6). Всі вузли з'єднуються один з одним, тому система відмовостійка. Але така топологія дуже дорога і складна, тому краще створювати частково пов'язану топологію [1, 2, 6].

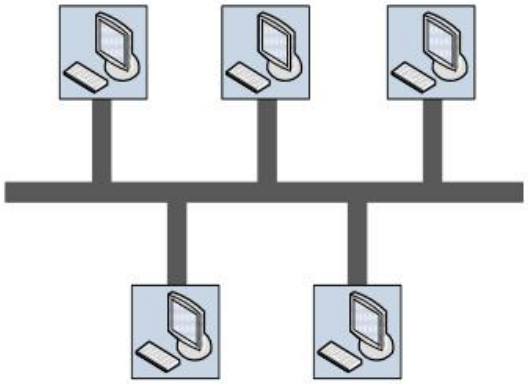

Рисунок 1.1 - Топологія типу «Шина»

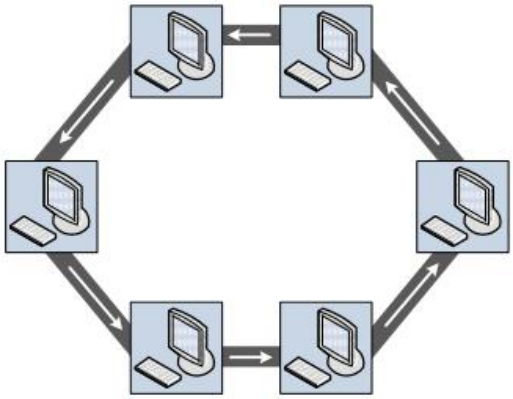

Рисунок 1.2 - Топологія типу «Кільце»

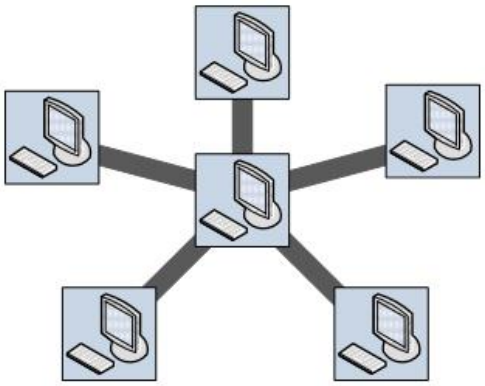

Рисунок 1.3 - Топологія типу «Зірка»

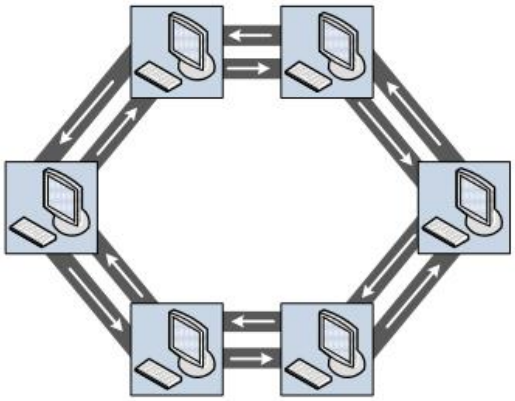

Рисунок 1.4 - Топологія типу «Подвійне кільце»

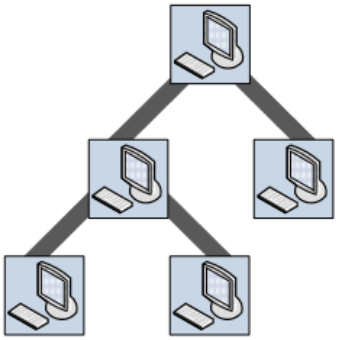

Рисунок 1.5 - Топологія типу «Дерево»

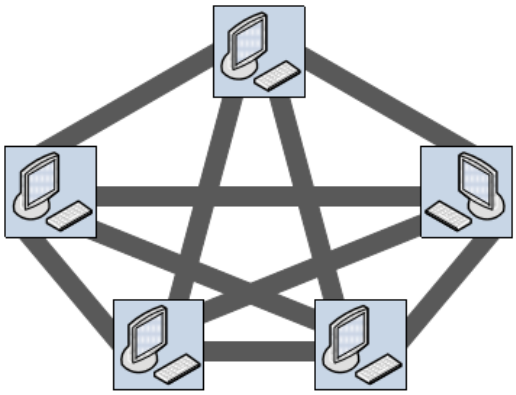

Рисунок 1.6 - Топологія типу «Повнозв'язна»

Для організації передачі даних між вузлами використовують набори правил - протоколи.

Всі протоколи взаємодіють один з одним певним чином.

Міжнародна організація по стандартам розробила модель, яка визначає функції рівнів взаємодіючих систем. Це базова еталонна модель взаємодії відкритих систем (OSI / ISO). Вона включає в себе сім рівнів [2].

У мережі Інтернет використовується стек протоколів TCP / IP. Цей набір протоколів був розроблений Міністерством оборони США (Department of Defence, DoD) ще до появи моделі OSI / ISO. Він включає в себе тільки чотири рівні. Нижче представлено відповідність рівнів моделі OSI / ISO і стека TCP / IP (рис. 1.7) [7].

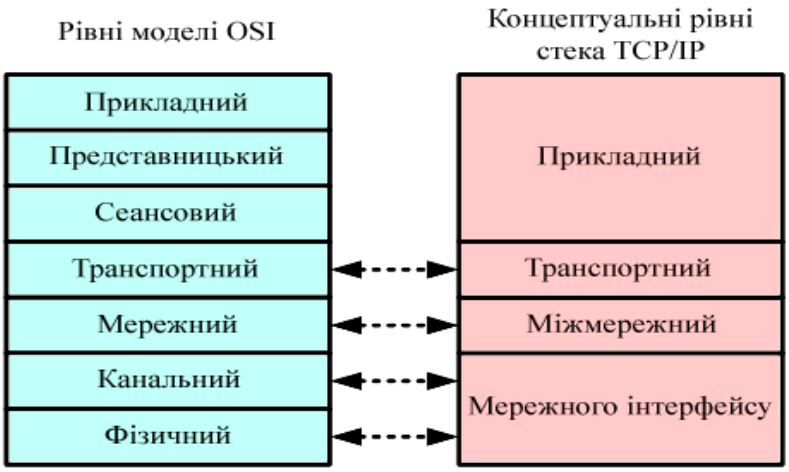

Рисунок 1.7 - Модель OSI / ISO і стек протоколів TCP / IP

Рівні моделі OSI / ISO [2, 7]:

– прикладний рівень - рівень доступу додатків до мережі. Відповідає за обмін даних між додатками на пристрої користувача і мережею. (Приклад протоколу: HTTP);

– представницький рівень - рівень, який відповідає за те, що передача даних на прикладному рівні, будуть прочитані і захищені;

– сеансовий рівень - здійснює обмін між двома додатками. Основний елемент передачі - Protocol Data Unit (PDU) - Модуль даних протоколу. (Приклад протоколу: PPTP);

– транспортний рівень - рівень відповідає за взаємодію безпосередньо двох точок, з'єднання яких вже встановлено. Основний елемент передачі - сегмент. (Приклади протоколів: TCP, UDP);

– мережевий рівень - підключення і вибір шляху між двома точками для передачі даних. Основний елемент передачі - датаграмма. (Приклад протоколу: IP);

– канальний рівень - визначається формат даних для передачі і методи контролю доступу до фізичного середовища. Основний елемент передачі даних - кадр. (Приклад протоколу: Ethernet);

– фізичний рівень - відповідає за фізичне з'єднання між обладнанням. На цьому рівні описуються електричні або оптичні сигнали, необхідні для скріплення двох кінцевих точок. (Приклади: електричний сигнал, модуляція, синхронізація) [2, 7].

При передачі даних інформація «упаковується» в пакет, починаючи з верхнього рівня (прикладного) до нижнього (фізичного), цей процес називається інкапсуляція. Після цього пакет відправляється в мережу. При його одержанні відбувається «розпакування» від нижнього рівня до верхнього, і цей процес називається деінкапсуляція.

Комп'ютерні мережі поділяються на [2]:

– локальні мережі (LAN, Local Area Network) - комп'ютерна мережа, що покриває відносно невелику територію (кімната, офіс, будівля);

– глобальні мережі (WAN, Wide Area Network) - як правило, об'єднання великої кількості локальних мереж.

Інтернет (Internet) - глобальна мережа, що складається з об'єднання тисяч корпоративних, наукових, урядових та домашніх комп'ютерних мереж [8, 9].

Для зв'язку між мережевим устаткуванням в локальних та глобальних мережах зазвичай використовується протокол мережевого рівня - IP (Internet Protocol). На даний момент існує дві версії протоколу [2, 10]:

– IPv4 - кожному вузлу привласнюється IP-адреса довжиною 32 біта (4 байта - 4 октету);

– IPv6 - кожному вузлу привласнюється IP-адреса довжиною 128 біт (16 байт - 8 груп).

Формат IP-адреси (протокол IPv4) являє собою 32-х бітове двійкове число, для простоти це число розбивають на октети по 8 біт кожен і розділяють крапкою. Двійкові числа в кожному октеті перетворять в десяткові від 0 до 255 [2, 4].

13 14 49 121
00001101.00001110.00110001.01111001

У локальних мережах використовуються особливі IP адреси (протокол IPv4), звані приватними, внутрішніми, які не використовуються в глобальній мережі:

– 10.0.0.0 - 10.255.255.255;

– 172.16.0.0 - 172.31.255.255;

– 192.168.0.0 - 192.168.255.255.

Необхідність в таких адресах виникла через те, що не очікували такого великого зростання та використання мережі. Звичайно, проблему збільшення кількості IP-адрес зараз вирішує протокол IPv6, але на даний момент цей протокол ще широко не використовується [4].

1.2 Маршрутизація

Маршрутизація - це процес пересилання пакетів даних між мережами або підмережами за допомогою пристроїв третього рівня моделі OSI / ISO.

Для маршрутизації використовуються таблиці маршрутизації та протоколи, які реалізують алгоритми маршрутизації, для того щоб визначити найбільш раціональний шлях для пересилання пакета даних [11].

Пристрій, який визначає більш прийнятний шлях для передачі даних з однієї мережі в іншу, називається маршрутизатор.

Для обміну даних в мережах маршрутизатор веде таблицю маршрутизації. Вона являє собою список мережевих адрес, а так само зберігає дані про місця призначення та зв'язки з наступними переходами. За допомогою цих зв'язків пристрій розуміє, чи можна дістатися до пункту призначення безпосередньо або через інші маршрутизатори. Таблиця може зберігати такі види записів (один запис для кожної мережі) [11]:

– статичні - інформація про маршрут заповнюється вручну, але цей спосіб призводить до проблем в разі зміни топології мережі або ж відмови на якій-небудь ділянці;

– динамічні - заповнення відбувається завдяки обміну даних маршрутизації між пристроями, отриманих за протоколом маршрутизації, тобто маршрутизатори обмінюються інформацією один з одним шляхом передачі повідомлень про оновлення. Залежно від протоколу поновлення можуть надходити періодично або ж тільки при зміні топології [4].

Виникають ситуації, коли є декілька шляхів передачі інформації від джерела до місця призначення. Кожен протокол маршрутизації використовує свої метрики для визначення найкращого шляху. Якщо ж використовуються різні протоколи, то прийнятний шлях вибирається на основі адміністративної відстані - це число від 0 до 255 (рис. 1.8) [8-10].

Назва протоколу	Значення відстані
Сумарний маршрут EIGRP	5
BGP, який працює поза рамками автономної системи	20
EIGRP, який працює в рамках автономної системи	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
EIGRP, який працює поза рамками автономної системи	170
BGP, який працює в рамках автономної системи	200

Рисунок 1.8 - Значення адміністративної відстані

Протокол з найменшим значенням вибирається як найбільш надійний.

Протокол маршрутизації - це набір правил, які маршрутизатор використовує при «спілкуванні» з іншими маршрутизаторами, щоб визначити

шляхи до ві ддалених мереж, а так само для ведення записів про ці мережах в таблиці маршрутизації [9]. Існують два поняття, які не можна плутати:

– маршрутизуючий протокол - будь-який протокол з адресою мережевого рівня, який здійснює пересилку пакетів між хостами. У цього протоколу, як правило, немає інформації для всього маршруту від джерела до місця призначення. Наприклад, протокол IP;

– протокол маршрутизації - дозволяє забезпечити обмін даних маршрутизації між мережами, і дозволяє створити динамічні таблиці маршрутизації. Маршрутизатор повинен знати, куди відправити пакет, але не його подальший шлях від інших маршрутизаторів [12].

Протоколи маршрутизації розрізняються за типом взаємодії між мережами.

Ця відмінність пов'язана з поняттям автономної системи (рис. 1.9).

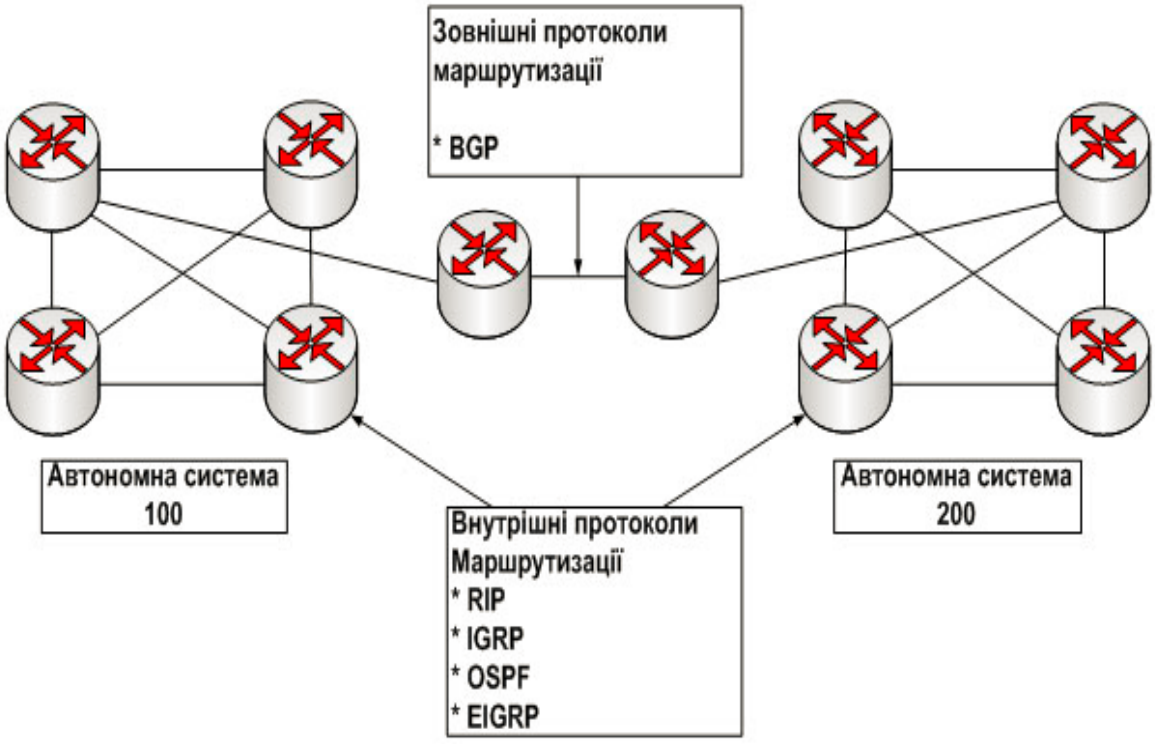

Рисунок 1.9 - Класифікація протоколів по типу взаємодії між мережами

Автономна система (АС) - це сукупність мереж із загальним управлінням, маршрутизатори в АС мають єдині правила маршрутизації. Відповідно до цих поннять є два типи протоколів маршрутизації:

– внутрішній протокол маршрутизації - протокол, службовець для обміну інформацією всередині АС. Наприклад: RIP, OSPF, EIGRP та ін.;

– зовнішній протокол маршрутизації - протокол, службовець для обміну інформацією між автономними системами. Наприклад: BGP [2, 4].

Такий поділ протоколів визначає ієрархічний метод маршрутизації.

Протоколи маршрутизації можна класифікувати по використанню певного алгоритму маршрутизації, який необхідний для визначення оптимального шляху проходження пакетів від джерела до місця призначення.

Вимоги, яким повинні відповідати алгоритми маршрутизації [1]:

– оптимальність - здатність алгоритму вибрати кращий шлях;

– простота - алгоритм не повинен вимагати великої та складної програмної реалізації;

– живучість - алгоритм повинен продовжувати функціонувати в разі непередбачених обставин, таких як відмова обладнання, високі навантаження на мережі і т.д .;

– швидка збіжність - процес угоди між всіма маршрутизаторами по найкращим шляхам. Тобто, наприклад, при відмові будь-якого маршрутизатора, повідомлення про оновлення топології мережі повинні дійти до інших маршрутизаторів з мінімальною затримкою. В результаті маршрутизатори перераховують шлях і вибирають оптимальний. Алгоритми, які сходяться повільно, можуть привести до небажаних наслідків, таких як вихід з ладу всієї мережі;

– гнучкість - алгоритм повинен точно і швидко адаптуватися до змін в мережі. Наприклад, зміна топології мережі, смуги пропускання певних ліній, затримка і т.п.

Розрізняють такі основні алгоритми маршрутизації [2, 4, 5]:

– статичні. Системний адміністратор вручну прописує записи в таблиці маршрутизації. Такий метод маршрутизації непридатний для великих мереж. Так само його складно налаштовувати при зміні топології мережі;

– динамічні. Цей алгоритм враховує зміни в мережі, завдяки повідомленнями, що надходять. При зміні топології відбудеться перерахунок шляхів, після чого відбудеться нова розсилка повідомлень про зміну маршрутів [12].

Протоколи внутрішньої маршрутизації можна класифікувати по використанню однієї з таких динамічних алгоритмів маршрутизації:

– метод маршрутизації на основі вектора відстаней. Цей метод визначає напрямок і відстань (наприклад, кількість переходів) до будь-якого каналу іншої

мережі, шляхом розсилки вектора. При отриманні вектора від сусіда маршрутизатор збільшує відстань, а також додає інформацію про відомі йому мережах і розсилає нове значення вектора по мережі. Мінус цього методу в тому, що у великих мережах широкомовлення негативно позначиться на роботі мережі;

– метод маршрутизації на основі стану канала. Маршрутизатори обмінюються повідомленнями про стан канала зі своїми сусідами, при цьому кожен маршрутизатор створює базу даних топології мережі, на основі отриманих повідомлень. Після цього алгоритм видаляє зайві шляху і становить своє дерево найкоротших шляхів [4].

Ідеального алгоритму пошуку шляху для всієї мережі не існує.

В алгоритмах маршрутизації використовується багато різних показників, які називаються метрикою. Це число, яке генерує алгоритм для кожного можливого шляху.

Найчастіше менша метрика означає найкращий шлях. Складні алгоритми маршрутизації при виборі маршруту можуть базуватися на безлічі показників або їх комбінації. Нижче перелічені метрики, які найчастіше використовуються в алгоритмах маршрутизації [2].

– Кількість переходів. Це число показує, скільки переходів через обладнання повинен зробити пакет, щоб дістатися від джерела до місця призначення.

– Швидкість передачі даних в каналі (смуга пропускання).

– Затримка. Час, необхідний для передачі пакета від джерела до місця призначення. Затримка може залежати від багатьох факторів, таких як завантаження мережі, пропускна здатність каналів і т.п.

– Завантаження. Активність мережевого ресурсу, маршрутизатора, каналу й т.д.

– Надійність. Надійність, відноситься до надійності каналу зв'язку. Деякі канали мережі можуть відмовляти частіше, ніж інші. Відмови одних каналів мережі можуть бути усунуті легше або швидше, ніж відмови інших каналів. При призначенні оцінок надійності можуть бути прийняті до уваги будь-які фактори надійності.

– Вартість. Налаштування роздільної значення [2].

1.3 Загрози комп'ютерної безпеки

У країнах, де високий рівень комп'ютеризації, проблема боротьби з комп'ютерною злочинністю, вже досить давно стала однією з першорядних. І це не дивно. Наприклад, в США збиток від комп'ютерних злочинів становить щорічно близько 5 млрд. доларів, у Франції ці втрати сягають 1 млрд. франків на рік, а у Німеччині за допомогою комп'ютерів злочинці щороку викрадають близько 4 млрд. марок. Й кількість подібних злочинів збільшується щорічно на 30-40% [13].

"Злочини у сфері комп'ютерної інформації":

– неправомірний доступ до комп'ютерної інформації;

– створення, використання і поширення шкідливих комп'ютерних програм;

– порушення правил експлуатації комп'ютерів, комп'ютерних систем і мереж [14].

Відзначимо, що кримінальна відповідальність за перелічене настає тільки в тому випадку, коли знищена, блокована, модифікована чи скопійована інформація, що зберігається в електронному вигляді. Таким чином, просте несанкціоноване проникнення в чужу інформаційну систему покаранню не підлягає.

Правоохоронним органам стають відомі не більше 5-10% скоєних комп'ютерних злочинів. Їх розкриваність теж не перевищує 1-5%. Це пов'язано з тим, що розкрадання інформації довгий час може залишатися непоміченим, оскільки часто це просто копіюються.

Зараз окремі фірми, компанії, корпорації ведуть свою власну наукову роботу, в кожній організації автоматизована система – все це та багато іншого розроблюється, оброблюється і зберігається за допомогою комп’ютерів. А для передачі інформації використовують комп’ютерну мережу. Зрозуміло, що така інформація може бути цікава для конкурентів, а тому виникає проблема її захисту. Під захистом інформації слід розуміти не тільки комплекс технічних, програмних, апаратних заходів але й нормативно-правову базу. На сьогоднішній день сформульовано три принципи інформаційної безпеки [4].

Цілісність інформації - це захист даних від умисного або неумисного пошкодження, знищення, доступу сторонніх осіб.

Неправомірний доступ здійснюється, як правило, з використанням чужого імені, підроблених документів, зміною фізичних адрес технічних пристроїв, зміною програмного і апаратного забезпечення, розкраданням носіїв інформації, установкою апаратури перехоплення інформації з систем її передачі, а також порушенням систем захисту інформації. Неправомірний доступ до файлів законного користувача може бути здійснений через слабкі місця в захисті інформаційної системи. Виявивши такі слабкі місця, злочинець може дослідити інформацію на комп'ютері, причому робити це можна так, що факт "злому" системи захисту буде встановлений дуже пізно. Створення, використання та поширення шкідливих програм для ЕОМ. Мова йде про програми, які спрацьовують при певних умовах й повністю або частково паралізують роботу комп'ютерної системи [12-14].

На рис 1.10 показана статистика атак через глобальну мережу Інтернет на локальний комп’ютер [9].

Розробка та розповсюдження комп'ютерних вірусів. Небезпеку вірусів не слід применшувати. Вірус може виявитися причиною виходу з ладу банківської системи, системи життєзабезпечення в лікувальних установах, систем навігації літаків, кораблів і т.п. Кримінальний кодекс передбачає покарання за внесення вірусу на комп'ютерні системи, навіть якщо вірус не спрацював або не встиг спрацювати.

Покарання за будь-який вид умисного розповсюдження вірусу, будь то продаж програми з вірусом, дарування, обмін чи таємне внесення в систему. Те, що ваш комп'ютер працює нормально, ще не означає, що він не заражений вірусами.

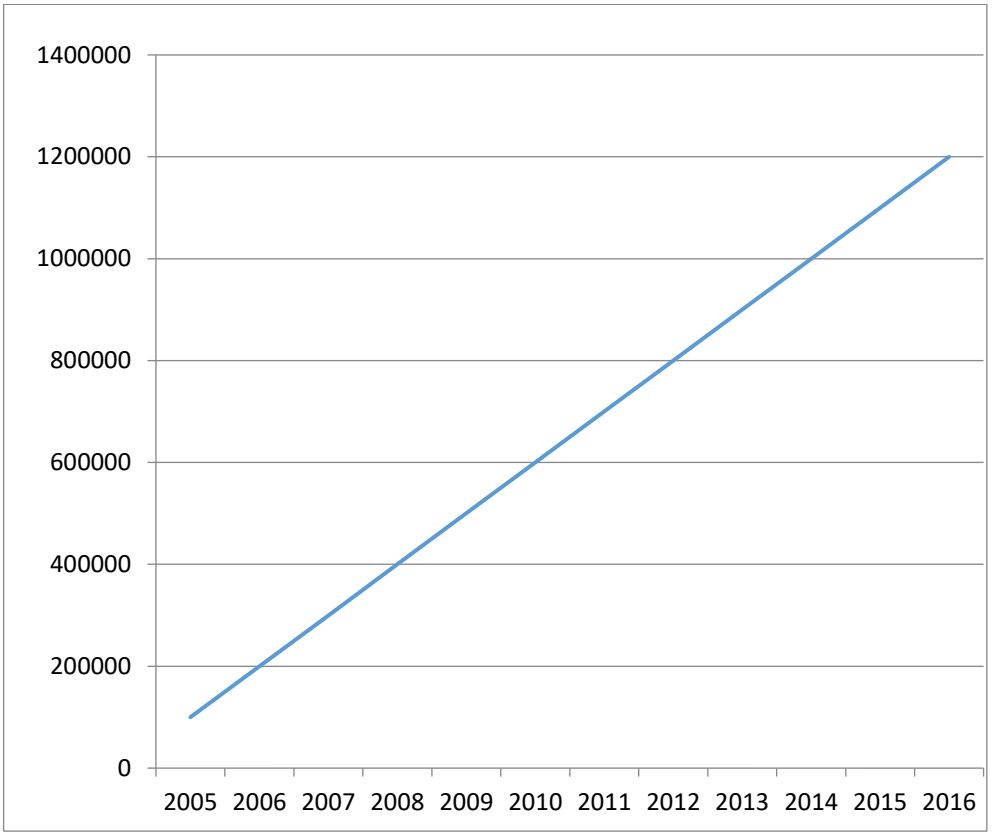

Рисунок 1.10 - Статистика атак в Інтернеті

Можливо, комп'ютер тільки починає "хворіти" і симптоми зараження будуть помітні тільки досвідченим користувачам. І в один прекрасний день комп'ютер перестає нормально працювати. Можливі як вихід з ладу програм на даному комп'ютері, так і пошкодження апаратних частин комп'ютера (жорсткий диск). Варіантів вірусів може бути безліч. На сьогоднішній день відомі сотні типів вірусів і десятки тисяч видів вірусів. Від найпростіших, які уповільнюють роботу комп'ютерів, до складних, що вносять серйозні пошкодження і повністю паралізують роботу [4].

Природно, що проти вірусів прийняті надзвичайні заходи, що призвели до створення захисних програм. Антивірусні програми можна розділити на три види: фільтруючі, що перешкоджають проникненню вірусу на комп'ютер; проти інфекційні, що контролюють роботу додатків в системі; противірусні, що здійснюють пошук вірусів серед файлів комп'ютера і здійснюють "лікування файлів". Однак зауважимо, що віруси спочатку з'являються, а вже потім спеціальні антивірусні лабораторії шукають "вакцину" проти даного конкретного вірусу. Так що, використовуючи останню версію антивірусного пакету, ви можете бути захищені тільки від тих видів вірусів, які були відомі творцям пакету на момент виходу. А від сотень вірусів, написаних пізніше, ви

навряд чи зможете вберегти свій комп'ютер. Можна акуратно управляти своїм транспортним засобом, не заважаючи оточуючим. Але існує можливість по необережності викликати серйозне дорожньо-транспортна пригода, що спричинило тяжкі травми людей, а може бути, навіть й їхньої смерті [4].

Однак, при використанні комп'ютерної техніки існує одна особливість. Практично неможливо розробити алгоритм вирішення задачі, а вже тим більш програмно реалізувати цей алгоритм, без якихось дрібних помилок та неточностей [2].

Помилки реалізації виявляються на етапі налагодження програми, та й то не завжди вони виключаються повністю. Й якщо, наприклад, при будові якихось споруд (мостів, доріг, будинків) розрахунки ведуться з певним запасом надійності, то в області програмування така надійність дуже умовна, не дивлячись на те, що вона є дуже важливою.

Сутність даного виду комп'ютерної злочинності полягає в наступному. Розробник програмного продукту замість, наприклад, побудови математичної моделі об'єкта, з метою отримання якихось вихідних параметрів, просто імітує отримання цих параметрів. Це може бути у випадку, коли об'єкт не відповідає вимогам, які накладаються на нього, а запуск виробництва цього об'єкта дуже важливий для третьої особи. Ну й до того ж, розробити математичну модель складніше, ніж просто зімітувати вихідні дані.

Не секрет, що в нашій країні переважна більшість програмного забезпечення, що продається, є не зовсім ліцензійним. Однак, комп'ютерні програми, як й, наприклад, книги, захищені законами про авторське право. Але не тільки авторські права на програму є предметом розкрадання інформації. Наприклад, неправомірне копіювання планів розрахунку якого-небудь пристрою, виконаних за допомогою персонального комп'ютера, бухгалтерського обліку будь-якої компанії - все це приклади розкрадань інформації. Злочинна недбалість у розробці, виготовленні та експлуатації програмно-обчислювальних комплексів, що призвела до тяжких наслідків [4].

Рисунок 1.11 - Джерела атак на локальний комп’ютер

Рисунок 1.12 - Реалізовані атаки у моделі OSI

1.4 Постановка задачі проектування

Одним із приорітетних напрямків розвитку інформаційного суспільства є створення цифрової спільноти з допомогою інфокомунікаційних систем та мереж. Останні допомагають інтегрувати між собою різних користувачів за допомогою маршрутизаторів, що об’єднують між собою різноманітні маршрути передачі даних з різними технологіями передачі та різними мережами. Особливої уваги при розробці таких маршрутизаторів вимагає не тільки забезпеченя їх переваг при виборі оптимального маршруту, а й переваг захисту інформації, що передається, від несанкціонованого доступу.

Для розробки маршрутизатора, що забезпечує ефективний процес маршрутизації та технічного захисту інформації, необхідно:

1. Дослідити різноманітні методи захисту інформаційних каналів від несанкціонованого доступу до сегментів мережі, які доречно реалізувати в маршрутизаторах.
2. Розробити структурну схему та блок-схему алгоритма роботи маршрутизатора на базі обраного метода підвищення рівня захисту від несанкціонованого доступу в різних сегментах мережі з різноманітними технологіями передачі даних.
3. Розробити функціональну та принципову схеми пристрою.
4. Розрахувати показникі собівартості виготовлення пристрою.

2 НАУКОВО-ДОСЛІДНА ЧАСТИНА

2.1 Проблеми інформаційної безпеки бездротових мереж

Бездротова локальна мережа (Wireless Local Area Network, WLAN) являє собою групу бездротових мережевих вузлів, розташованих на невеликій відстані один від одного, яка здійснює обмін даними через радіоефір. Бездротові локальні мережі мають досить обмежений діапазон дії та застосовуються, наприклад, в офісних будівлях, аеропортах, кафе й т.п., де вони реалізовані у вигляді розширень для існуючої дротової локальної мережі з метою забезпечення мобільності користувачів. В подальшому, при згадуванні терміна «бездротова мережа» мова йтиме про локальні бездротові мережі, що побудовані за бездротовою технологією Wi-Fi [2].

В даний час бездротові мережі завоювали величезну популярність. Повсюдне поширення даних мереж обумовлено незаперечними перевагами перед традиційними кабельними мережами:

- доступність і простота розгортання мережі;
- мобільність користувачів в зоні дії мережі;
- просте підключення до мережі нових користувачів;
- широке поширення мобільних пристроїв.

Згідно з прогнозом компанії Cisco Systems, до 2020 року половина всього трафіку, що генерується в корпоративних інформаційних мережах, припадала на бездротові пристрої. Це обумовлено, в тому числі й зростанням пропускної здатності бездротових мереж.

З іншого боку, невисокий рівень безпеки таких мереж часто обмежує їх застосування. Мережеві кабелі входять до складу структурованої кабельної системи організації і зазвичай прокладені в спеціальних кабель-каналах, в стінах будівлі або під стелею, що ускладнює фізичне підключення зловмисника до мережі. У разі бездротових мереж сигнал поширюється всеспрямовано, тому зловмисник може бути розташований в будь-якій точці зони дії мережі. Крім того, за рівнем потужності та напрямку поширення сигналу можна вирахувати місцезнаходження його джерела [15].

Бездротові мережі за своєю природою, а також через недосконалість використовуваних протоколів схильні до специфічних атак, наприклад, глушіння сигналу або атакам типу «відмова в обслуговуванні» (Denial of Service, DoS). Найчастіше такі дії є початковим етапом досягнення іншої мети -

прослуховування і підміни мережевого трафіку між абонентами, тобто реалізації атаки «людина посередині» (Man-In-The-Middle).

На практиці ще зустрічається організація захисту бездротової мережі за застарілою технологією Wired Equivalent Privacy (WEP), що використовує алгоритм шифрування RC4, односторонню аутентифікацію користувача і однакові для всіх користувачів ключі шифрування довжиною 64 або 128 біт. Атака Флурер-Мантінєє-Шаміра , що базується на уразливості в генерації вектора ініціалізації (Initialization Vector, IV), в якій перші кілька байтів ключового потоку вибираються невипадковим чином, і атака KoreK , яка полягає в побайтовой підборі вмісту мережевого пакету, легко дозволяє підібрати ключ шифрування і отримати доступ до даних, ща транслюються [15].

На зміну WEP прийшла технологія Wi-Fi Protected Access (WPA), в якій забезпечена підтримка протоколу інтеграції тимчасового ключа (Temporal Key Integrity Protocol, TKIP) , стандарту перевірки справжності 802.1X, а також розширюючого протоколу аутентифікації (Extensible Authentication Protocol, EAP). Хоча для шифрування використовується той же алгоритм RC4, що і в WEP, розрядність вектора ініціалізації збільшена вдвічі (до 48 біт), а також реалізовані правила зміни послідовності бітів вектора ініціалізації. Крім того, для кожного переданого пакета створюється новий ключ, а цілісність перевіряється за допомогою криптографічного контрольної суми MIC (Message Integrity Check). Ці зміни дозволили протидіяти атакам з повторним використанням ключів шифрування і підробкою вмісту переданих пакетів. Однак, у листопаді 2008 року на конференції PacSec Ерік Тьюз і Мартін Бек представили перевірений на практиці спосіб злому ключа TKIP, використовуваного в WPA, за 12-15 хвилин. Застосовуючи цей метод, можна розшифровувати і читати дані, що передаються від точки доступу до користувача, а також передавати йому підроблену інформацію. Проте атака має обмеження і можлива, тільки якщо в настройках пристроїв включена підтримка функції IEEE802.11e QoS [15].

Однак, в 2009 році співробітник університету м. Хіросіми Тосихиро Охігасі і професор університету м. Кобе Масакату Морії розробили і реалізували на практиці новий метод атаки, який забезпечує злом будь-якого WPA-з'єднання без будь-яких обмежень, в середньому за одну хвилину [15].

Згадані вище уразливості сприяли появі другої версії технології WPA, яка визначається технічною характеристикою IEEE 802.11i , прийнятою у 2004 році. WPA 2 підтримує шифрування за стандартом AES (Advanced Encryption Standard, вдосконалений стандарт шифрування), алгоритм якого володіє набагато

більшою криптостійкості, ніж використовуваний в WEP RC4, і протокол блочного шифрування з кодом аутентифікації повідомлення (MIC) і режимом зчеплення блоків і лічильника (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, CCMP), створений для заміни TKIP [15].

Стандарт IEEE 802.11i вирішив проблеми забезпечення конфіденційності і цілісності всіх кадрів з даними, однак контрольні та керуючі кадри залишилися незахищеними, так само як і заголовки кадрів на канальному рівні моделі взаємодії відкритих систем (Open System Interconnection, OSI). Це дає можливість проводити DoS-атаки на бездротову мережу з захистом WPA 2 [15].

Варто відзначити, що технологія WPA має спрощений режим, який називається Pre-Shared Key (WPA-PSK). При використанні даного режиму роботи для кожного вузла бездротової мережі (точки доступу, клієнтського пристрою й т.п.) необхідно ввести один пароль. Якщо пароль буде співпадати з вказаними налаштуваннями підключення до мережі, користувач отримає дозвіл на доступ до цієї мережі.

На даний момент в якості основних методів злому WPA 2-PSK застосовуються атака по словниках паролів та перебір паролів методом «грубої сили». Для цього бездротовий мережевий адаптер переводиться в режим моніторингу, сканується трафік і зберігаються необхідні пакети. Далі здійснюється деаутентіфікація клієнта мережі або очікується момент підключення нового користувача з метою захоплення кадрів, що містять аутентифікаційні інформацію (Handshake), після чого вже в оффлайн режимі за допомогою спеціальної програми підбирається пароль. Для прискорення підбору може використовуватися обчислювальна потужність графічного процесора.

23 липня 2010 року стало відомо про вразливість Hole196 в технології WPA2. У разі використання даної уразливості зловмисник після авторизації в бездротової мережі може розшифровувати дані, що передаються іншими користувачами, за допомогою свого закритого ключа. При цьому ніякого злому ключів шифрування або перебору паролів доступу немає потреби [4].

Широке поширення Wi-Fi мереж призвело до спроби зробити налаштування бездротової мережі простіше для людей, що не володіють навичками комп'ютерної грамотності. Результатом стала технологія Wi-Fi Protected Setup (WPS). WPS автоматично призначає ім'я мережі і включає шифрування для захисту бездротової мережі від несанкціонованого доступу, при цьому немає необхідності вручну налаштувати кожен параметр. WPS реалізується на більшості вироблених в даний час бездротових точках доступу,

включаючи Cisco, Linksys, Zyxel, D-Link і Netgear. Крім того, на багатьох пристроях дана функція включена за замовчуванням [2].

Однак, реалізація ідеї використання WPS має недолік, який дозволяє зловмисникові виконати атаку шляхом підбору PIN-коду, за яким відбувається аутентифікація користувача. Хоча довжина PIN-код складається із 8 цифр, він розділений на дві половини, причому остання цифра є контрольною сумою коду. Це зменшує максимально можливу кількість спроб аутентифікації, необхідних для вгадування PIN-коду, з 10^8 (100 000 000) до $10^4 + 10^3$ (11 000). Відновлення PIN-коду дає атакуючому повний доступ до мережі, причому якщо точка доступу віщає в двох діапазонах частот одночасно (2,4 ГГц і 5 ГГц), то так як радіомодулі використовують один і той же WPS PIN-код, знання його дозволяє відновити всі ключі WPA.

З вищесказаного можна зробити висновок, що настройка параметрів бездротового підключення повинна проводитися вручну грамотним фахівцем і відповідно до інструкцій і рекомендацій виробників обладнання. Таким чином, питання захищеності бездротових локальних мереж на даний момент залишаються відкритими [15].

Основні проблеми захисту інформації в бездротових мережах полягають при цьому в наступному:

– поширення сигналу за межі контрольованої зони;

– легкий доступ зловмисника до бездротовому каналу передачі в порівнянні з кабельними мережами;

– використання вразливих протоколів і методів аутентифікації;

– відсутність повноцінного захисту від атак при випуску доповнень до стандартів;

– можливі помилки в налаштуванні різних компонентів бездротової мережі.

2.2 Основні підходи до вирішення проблем інформаційної безпеки

Для організації безпечного функціонування бездротової мережі необхідно побудувати систему багаторівневого захисту. Дана система включає в себе наступні рубежі (заходи) [1, 2]:

– захист периметра бездротової мережі: точок доступу та пристроїв користувачів;

– забезпечення безпеки сеансів зв'язку: застосування надійних методів аутентифікації, стійких алгоритмів шифрування й т. д.;

– постійний моніторинг радіоефіру, включаючи фізичний рівень, виявлення і аналіз підозрілої активності;

– програмне забезпечення від несанкціонованого доступу.

Для вирішення зазначених вище проблем забезпечення безпеки інформації в бездротових мережах використовуються як технічні засоби захисту, так і організаційні заходи. Технічні засоби захисту по об'єкту застосування можна розділити на три основні групи (таблиця 2.1).

Тонке та грамотне налаштування пристроїв, застосування останніх найбільш захищених протоколів дозволяє знизити ймовірність реалізації загроз. Однак і вони мають свої недоліки, наприклад, відсутність в технології WPA 2 аутентифікації запитів на дисоціацію і деаутентификацію, в результаті чого з'являється можливість реалізації атаки роз'єднання абонентів та подальшого впровадження помилкового об'єкта мережі.

Контрольні та керуючі кадри передаються у відкритому вигляді, що дозволяє прослухати їх заголовки і виконати підміну MAC-адреси. Протокол 802.11 n, затверджений у 2009 р. і покликаний захистити керуючі кадри, забезпечує їх шифрування тільки після обміну ключами і не поширюється на контрольну інформацію. Його відмінності від попередникіх полягалє в збільшенні швидкості та теоретичної підтримки частоти 5 ГГц . Вперше в протокол була впроваджена підтримка технології MIMO. Вона полягає у підтримці прийому і передачі даних одночасно по декількох каналах (в даному випадку — з двох). Це дозволяло в теорії досягти швидкості на рівні 600 Мбіт/с. На практиці ж вона рідко перевищує 150 Мбіт/с [2].

Таблиця 2.1 - Методи і засоби захисту інформації в бездротових мережах

Засоби захисту мережі	Засоби захисту точки доступу	Засоби захисту користувача
Міжмережеві екрани	Зміна на пристрої налаштувань за замовчуванням	Персональні міжмережеві екрани

Проксі-сервери	Закриття невикористовуваних портів	Засоби антивірусного контролю
Бездротові системи виявлення атак	Заборона налаштування параметрів через бездротове з'єднання	Перевірка сертифіката сервера x 802.1
Списки контролю доступу по MAC-адресам	Захищені протоколи віддаленого управління	Підтримка стандарту 802.11 w
Контроль доступу до мережі (port security) і аутентифікація 802.1 X	Підтримка стандарту 802.11 w або протоколу MFP	Останні оновлення безпеки, драйверів бездротового модуля
	Включення режиму MultiBSSID (Virtual AP) і PSPF	
Організація демілітаризованої зони	Відключення розсилки імені бездротової мережі Service Set Identifier (SSID)	
Сканери мережевих вразливостей	Відключення технології спрощеної налаштування бездротової мережі Wi-Fi Protected Setup (WPS)	

Застосування віртуальних приватних мереж (VPN) з набором протоколів IPsec забезпечує необхідний рівень безпеки, однак вимагає складних налаштувань апаратних засобів і програмних клієнтів.

У зв'язку з вищесказаним, багато дослідників ведуть пошук можливих удосконалень поточних протоколів сімейства 802.11. Деякі науковці розглядають недоліки протоколів 802.11 та методів побудови захисту бездротової мережі та пропонують різні способи вирішення цього питання.

В якості вирішення проблеми вразливості стандартних протоколів пропонується шифрувати весь блок даних протоколу MAC (MPDU), включаючи MAC-заголовки, крім послідовності перевірки кадру FCS. Однак це стане

причиною помітних затримок у передачі даних і низької пропускної здатності каналу [15].

В іншому випадку при встановленні з'єднання між клієнтом і точкою доступу на запит асоціації поміщається розрахований по алгоритму SHA-512 хеш якогось випадкового набору символів, відомого тільки даному клієнту, який зберігається на точці доступу. У разі появи запиту на закриття з'єднання одержувач звіряє хеш вкладеного в запит значення з раніше збереженим та, у разі збігу, обробляє запит, інакше запит ігнорується. Варто зазначити, що даний спосіб дозволяє захиститися тільки від DoS-атак, які виконуються через підроблені запити на дисоціацію та деаутентифікацию [15].

Пропонується методика захисту інформації в бездротових мережах на основі динамічної маршрутизації трафіку. Проте розроблений алгоритм визначення довіреної маршруту передачі даних більшою мірою спрямований на вирішення завдання забезпечення доступності середовища передачі й не дозволяє гарантувати конфіденційність та цілісність трансльованих даних.

Д. Райт у своїх статтях відзначає особливості мережевого трафіку, що генерується утилітами для активного пошуку бездротових мереж, ін'єкції кадрів в ефір і створення помилкових точок доступу. Автор виявляє шкідливий трафік в ході аналізу значень поля «номер послідовності» (Sequence Number) в заголовку кадру, тега «унікальний ідентифікатор організації» (Organizationally Unique Identifier, OUI) і тега SSID [4].

Рада зі стандартів безпеки індустрії платіжних карт (Payment Card Industry Security Standards Council, PCI SSC), заснована провідними міжнародними платіжними системами, розробила стандарт безпеки даних індустрії платіжних карт (Payment Card Industry Data Security Standard, PCI DSS) [104], який містить вимоги до забезпечення безпеки даних про власників карток, згідно з якими повинна будуватися та функціонувати інфраструктура корпоративних інформаційних мереж.

Базова мережева безпека PCI DSS 3.0 вимагає установки брандмауера між дротової і бездротової мережами і наявності на ньому правил для обмеження доступу між бездротовими мережами і заданими серверами (службами), а також регулярне сканування мережі з метою ідентифікації бездротових пристроїв, пошуку неавторизованих або небажаних точок доступу. Додатковими вимогами є [8]:

- забезпечення фізичної безпеки бездротових пристроїв;
- розгортання бездротової системи запобігання вторгнень;

- зміна паролів та налаштувань за замовчуванням на всіх пристроях бездротового мережі і захищена налаштування бездротових пристроїв;

- протоколювання надання бездротового доступу;

- застосування методів суворої аутентифікації, стійких до злому алгоритмів шифрування і захищених протоколів безпеки: для переданих по корпоративній мережі даних повинен застосовуватися протокол WPA 2 з використанням AES-алгоритму з 128-бітовим ключем;

- розробка та застосування політики безпеки бездротових мереж, визначає правила використання комп'ютерної мережі співробітниками, гостями та контрагентами.

Міжнародний стандарт з інформаційної безпеки ISO/IEC 27001, розроблений спільно Міжнародною організацією по стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), містить вимоги в області інформаційної безпеки для створення, розвитку та підтримки систем менеджменту інформаційної безпеки, у тому числі для забезпечення безпеки бездротових мереж [1].

Якщо бездротові мережі використовуються або плануються до впровадження в організації, то політика безпеки повинна містити опис механізмів захисту, призначених для зниження ризиків, пов'язаних з несанкціонованим доступом до таких мереж.

Стосовно до бездротових мереж в зазначеному стандарті можна виділити наступні заходи [1]:

– розробка та затвердження політики інформаційної безпеки;

– розробка політики використання мобільних пристроїв і віддаленого доступу до мережі;

– навчання користувачів та адміністраторів у відповідності з положеннями політик;

– періодична інвентаризація мережевих ресурсів, що полегшує виявлення нових мережевих пристроїв;

– реалізація контролю підключень до комп'ютерної мережі за допомогою фільтрації за MAC-адресами, відключення незадіяних портів мережевих комутаторів;

– мінімізація привілеїв користувача, що знижує вірогідність несанкціонованого зміни налаштувань бездротових інтерфейсів;

– визначення використовуваних методів аутентифікації, вимог до зберігання аутентифікаційних даних, періодичність їх зміни, складності, безпеки при передачі по мережі;

– визначення та використання криптографічних засобів захисту, протоколів та алгоритмів шифрування трафіку в мережі;

– застосування засобів фізичної безпеки, обмеження доступу користувачів до мережевих портів та слотів розширення комп'ютера, що дозволяє знизити ймовірність підключення до комп’ютерної мережі несанкціонованих бездротових пристроїв;

– протоколювання та аналіз подій безпеки;

– застосування систем виявлення атак і сканерів безпеки, здійснюють контроль появи нових мережевих об'єктів, а також вираховують відхилення параметрів від заданих адміністратором, що дозволяє своєчасно виявляти спроби несанкціонованого доступу;

– сегментація мереж з допомогою брандмауера з виділенням пристроїв бездротового доступу в окремий мережний сегмент;

– визначення процедур розслідування інцидентів в політиці безпеки.

Серед технічних засобів захисту мережі, крім міжмережевих екранів, списків контролю доступу та інших традиційних засобів, слід виділити активно розвиваються в даний час бездротові системи виявлення вторгнень (Wireless Intrusion Detection System, WIDS) [15].

Система виявлення атак здійснює пошук, ідентифікацію, реєстрацію та оповіщення про атаки на інформаційну систему. Системи виявлення атак на безпроводові мережі, які поєднують в собі функції сигнатурних і поведінкових систем. Сигнатурний метод виявлення атак найбільш поширений і просто реалізуємо. Деякі утиліти, використовувані для проведення атак на бездротову мережу, мають чітко виражені сигнатури, і для їх виявлення необхідно прийняття заходів протидії. З іншого боку, багато атак не можуть бути чітко формалізовані, але викликають відхилення від нормального функціонування мережі, особливо на нижніх рівнях моделі OSI: поява невластивих типів кадрів, зміна частоти передачі кадрів, порушення структури та їх порядкової нумерації, мовлення на нестандартної частоті та ін. [6] .У той же час, відхилення можуть бути викликані неправильно сконфігурованим або несправним обладнанням, радіоперешкодами, відображеннями сигналу та іншими факторами, тому перед впровадженням системи слід зібрати значний обсяг статистичних даних про нормальну роботу мережі.

Стандарти сімейства 802.11 передбачають використання двох основних діапазонів частот: 2,4 ГГц та 5 ГГц, які, в свою чергу, діляться на канали. На відміну від традиційних систем виявлення атак, які отримують усі пакети мережі, бездротові системи здійснюють вибірку мережевого трафіку, по черзі скануючи канали на предмет наявності активних атак [11]. Типовими компонентами WIDS є сенсори, які збирають дані про бездротовий трафік, сервер баз даних та управління, а також консоль управління та аудиту. Приклад архітектури WIDS представлений на рисунку 2.1.

Сенсори можуть бути реалізовані кількома способами:

1. Виділений сенсор: перехоплює бездротовий трафік та передає його на сервер управління, при цьому не виконує трансляцію трафіку між клієнтами мережі. Може бути як стаціонарним, так й мобільним (наприклад, у вигляді програми-агента, встановленої на ноутбуці).

2. Сенсор, вбудований в точку доступу: забезпечує менш ретельне сканування, так як необхідно розподіляти час між наданням доступу до бездротової мережі та моніторингом декількох каналів в пошуках шкідливої активності.

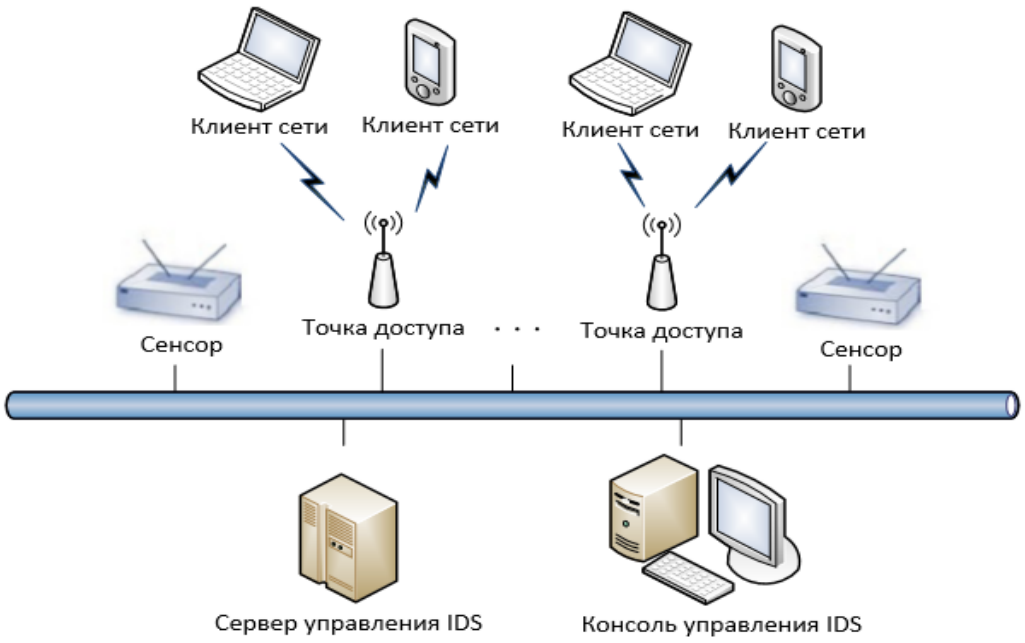

Рисунок 2.1 - Архітектура бездротової системи виявлення вторгнень

3. Програма-агент на клієнті: сканує трафік в межах зони покриття бездротової мережевої карти, виявляє атаки і помилки в налаштуванні та передає їх на сервер управління.

Варто відзначити, що розміщення сенсорів WIDS грає дуже важливу роль у виявленні атак. Для ефективного моніторингу мережі сенсори повинні покривати всю зону, з якої можливий бездротовий доступ. При цьому сенсор повинен володіти не меншою чутливістю, ніж приймач точки доступу, так як чим вище чутливість приймача сенсора, тим більше дистанційне бездротове пристрій виявить. Додатково збільшити дальність виявлення можна за допомогою зовнішніх антен, що підключаються до сенсорам [13].

WIDS дозволяють виявляти несанкціоновані бездротові мережі та пристрої, слабо захищені пристрої, використання бездротових програм-сканерів (Kismet, Wireshark, Netstumbler, Aircrack-ng та ін), DoS-атаки і атаки «людина посередині», а також незвичайні моделі поведінки клієнтів в мережі (аномалії). Перед початком функціонування системи необхідно виконати її налаштування: вказати, які мережі, клієнти та точки доступу є довіреними, та визначити політику безпеки для захищається бездротової мережі.

Однак, в області WIDS на даний момент відсутні загальноприйняті стандарти, виробники систем застосовують закриті алгоритми виявлення та класифікації атак.

Тому завдання виявлення та розпізнавання типів атак в бездротових мережах залишається актуальною. При цьому завдання віднесення фрагмента мережевого трафіку до якого-небудь типу атаки або до нормальної активності можна вирішувати шляхом застосування сучасних методів інтелектуального аналізу даних (ІАД) [1].

2.3 Аналіз існуючих методів та алгоритмів виявлення мережевих атак

Основу функціонування бездротової системи виявлення атак становить класифікуюча модель, на базі якої приймається рішення про віднесення фрагмента мережевого трафіку до нормальної активності або до будь-якого типу атаки.

Формально завдання класифікації мережевого трафіку можна представити наступним чином. Нехай X – множина вхідних образів (записів мережевої активності) x_i, Y – множина виходів (міток класів) y_i. Передбачається, що існує відображення F: X → Y, значення якої відомі на записах кінцевої навчальної вибірки $X^m = \{(x_1, y_1),...,(x_m, y_m)\}$. Потрібно побудувати алгоритм A: X → Y, здатний класифікувати довільний запис мережевої активності x_i є X (рисунок 2.2, а) [5].

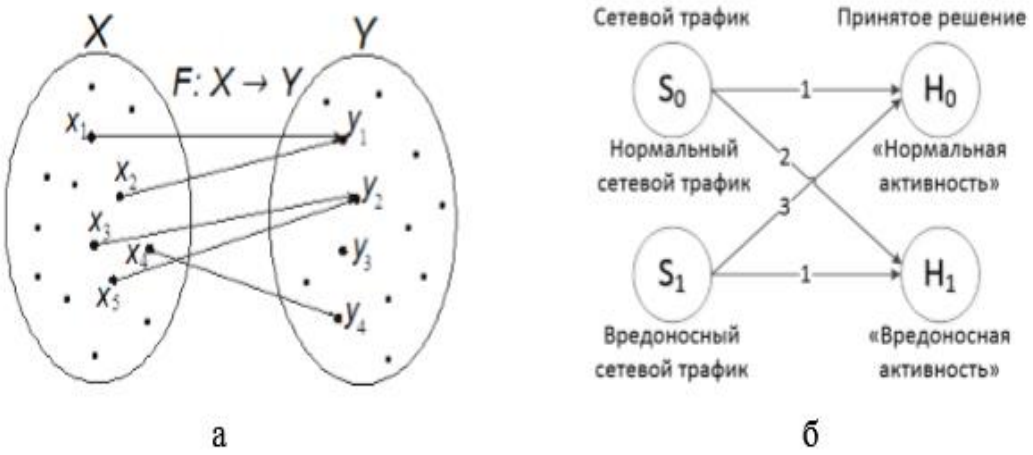

Рисунок 2.2 - Графічне представлення задачі класифікації мережевого трафіку (а) та можливих результатів процесу класифікації (б)

У загальному випадку можливі три результати процесу класифікації записів мережевої активності (рисунок 2.2, б):

1. Правильне рішення: $S_0 \rightarrow H_0$або $S_1 \rightarrow H_1$. Відповідно, ймовірність правильної класифікації записів визначається як:

$$P_{\text{прав}} = \text{P}\{\text{H}_0 | S_0 \text{v } \text{H}_0 \mid S_1\} = \text{P}\{H_0 | S_0 + H_1 \mid S_1\}$$

2. Помилка першого роду: $S_0 \rightarrow H_1$. Ймовірність помилки першого роду:

$$P_1 = \text{P}\{H_1 \mid S_0\}$$

3. Помилка другого роду: $S_1 \rightarrow H_0$. Ймовірність помилки другого роду:

$$P_2 = \text{P}\{H_0 \mid S_1\}$$

Потрібно побудувати таку класифікуючу модель, яка дозволила б мінімізувати сумарну ймовірність виникнення помилок $P_{\text{пом}} = \text{P}_1 + \text{P}_2$ (на практиці потрібно забезпечити значення $\text{P}_{\text{пом}} = 3 \div 5\%$).

Для виявлення найбільш ефективного методу побудови класифікуючою моделі стосовно до бездротової системи виявлення атак в даній роботі проведено

порівняння наступних методів ІАД: методу опорних векторів, метод k-найближчих сусідів, дерев прийняття рішень, а також нейронних мереж.

Метод опорних векторів (Support Vector Machine, SVM) є відносно новим алгоритмом у співтоваристві машинного навчання. За час свого існування він показав як переваги по відношенню до раніше запропонованих методів, так і деякі недоліки, які тим не менш, можуть бути подолані за рахунок більшої обчислювальної потужності комп'ютерного обладнанняи [5].

Основу методу опорних векторів складає алгоритм класифікації, запропонований Вапніком на підставі теорії Вапника-Червоненкіса.

Головна ідея методу опорних векторів полягає в переведенні вихідних векторів в простір більш високої розмірності та пошук розділяючої гіперплощини з максимальним зазором між кластерами в цьому просторі. По обидва боки гіперплощини, яка розділяє різні класи, будуються дві паралельні гіперплощини (рисунок 2.3).

Роздільною гіперплощиною буде така гіперплощина, відстані від якої до двох паралельних гіперплощин будуть максимальними. Такий алгоритм працює на припущенні, згідно з яким збільшення відстані між цими паралельними гіперплощинами призводить до зменшення середньої помилки класифікації [14].

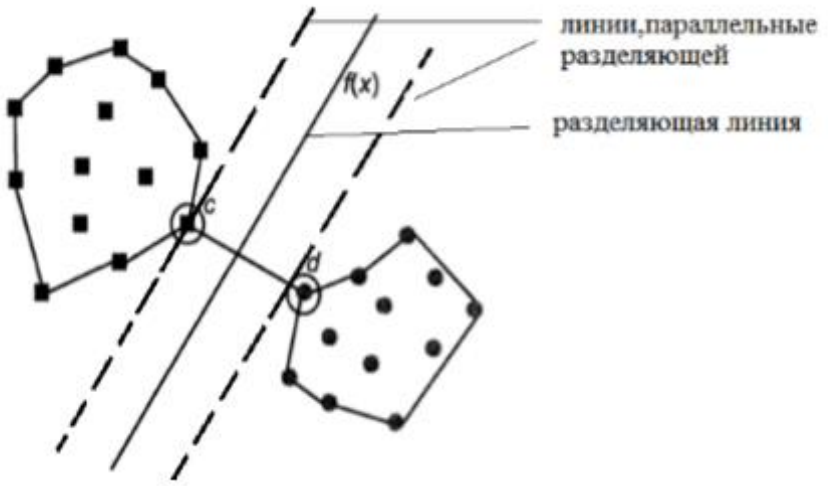

Рисунок 2. 3 - Графічна інтерпретація методу опорних векторів для двовимірного простору ознак

У випадку методу опорних векторів кожний об'єкт даних представлений у вигляді вектора (точки) в n-мірному просторі (послідовність n чисел). Кожна така точка належить лише одному з двох класів. Питання полягає в тому, чи можна розділити ці точки гіперплощиною з розмірністю (n−1). Це називається лінійним

класифікатором. Таких гіперплощин, які класифікують дані, може бути безліч. Так як максимізація зазору між класами сприяє більш впевненій класифікації, вибирається така гіперплощина, відстань від якої до найближчої точки з навчального набору з кожної сторони гіперплощини максимальна. Якщо дана гіперплощина існує, то вона є оптимальною розділючою гіперплощиною, а відповідний їй лінійний класифікатор – оптимально розділюючим класифікатором. Найбільш близько розташовані вектори різних класів називаються опорними векторами (рисунок 2. 3).

В якості переваг SVM можна відзначити здатність до узагальнення, високу точність та низьку обчислювальну складність прийняття рішення. Недоліком даного методу є відносно велика обчислювальна складність побудови класифікуючої моделі.

Ідея застосування SVM при розробці систем виявлення вторгнень (IDS) є відносно молодою. У деяких роботах [12] досліджується спосіб виявлення атак з допомогою особливого варіанту SVM – LMRL (Large Margin Rectangle Learning – навчання на основі прямокутних кластерів з максимальним зазором), в якому також використовується принцип максимізації зазору і, крім того, кожен клас представляється у вигляді набору прямокутних кластерів. Метод застосовувався для побудови класифікуючою моделі системи виявлення атак, що функціонує на основі технології сигнатурного аналізу, з даних навчальної вибірки. Модель випробувана на атаках типу переповнення буфера, руткіт і SYN-FLOOD і показала актуальність застосування методу опорних векторів в якості основи системи виявлення атак.

Метод k-найближчих сусідів (k-nearest сусідів, k-NN) – метод класифікації, принцип роботи якого полягає у присвоєнні об'єкту класу, найбільш поширеного серед сусідів даного об'єкта. Формування сусідів відбувається з безлічі об'єктів з уже відомими класами, і, виходячи з заданого значення k ($k \geq 1$), визначається, який з класів найбільш численний серед них. У разі якщо $k = 1$, то об'єкт просто відноситься до класу єдиного найближчого сусіда.

Метод k-NN є одним з найбільш простих методів ІАД. Результати застосування методу легко піддаються інтерпретації. Недолік методу – його чутливість до локальної структури даних.

Дерева прийняття рішень являють собою деревоподібну структуру з «листя» та «гілок». На ребрах («гілках») дерева прийняття рішень записані атрибути, від яких залежить цільова функція, в «листі» записані значення цільової функції, а в інших вузлах – атрибути, за якими розрізняються об'єкти.

Для класифікації нового об'єкта необхідно спуститися по дереву від кореня до листків та отримати відповідний клас. Таким чином, шлях від кореня до листка виступає правил класифікації на основі значень атрибутів об'єкта.

Перевагами дерев прийняття рішень є простий принцип їх побудови і хороша інтерпретованість результатів, недоліком – невисока точність класифікації.

Перелічені вище методи інтелектуального аналізу даних часто використовуються дослідниками в якості класифікаторів записів про мережеву активность (сигнатур) [15].

В даний час в області нейронних мереж бурхливо розвивається напрямок Deep Learning («глибоке навчання»), що представляє собою третє покоління нейронних мереж. У дану категорію входять багатошарові нейронні мережі, навчання яких здійснюється не на цілих об'єктах, а на їх складових частинах з поступовим збільшенням їх розміру. Прикладом є глибокі мережі довіри (Deep Belief Networks, DBN). В основі їх лежить RBM-мережа (Restricted Boltzmann Machine) – стохастична нейронна мережа, що складається з одного видимого і одного прихованого шарів, представлена на рисунку 2.4.

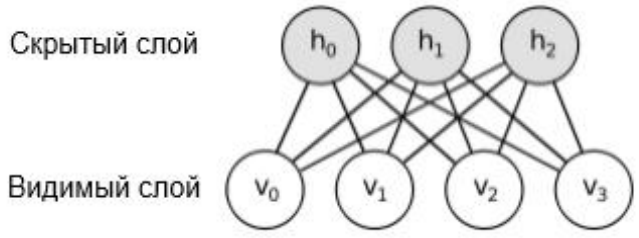

Рисунок 2.4 - Структура RBM-мережі

Головною особливістю мереж глибокого навчання є процес навчання мережі, що проводиться пошарово без вчителя. Прихований шар кожної RBM-підмережі виступає як видимий для наступної підмережі (рисунок 2.5).

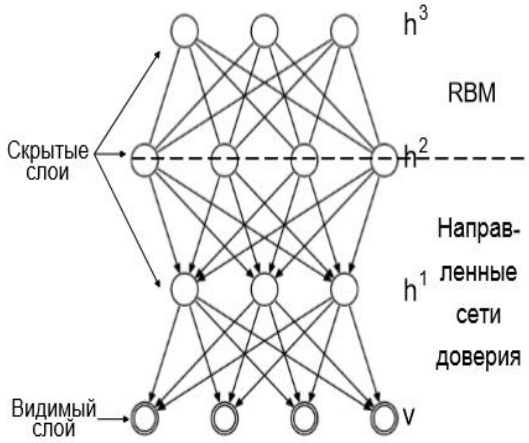

Рисунок 2.5 - Структура DBN-мережі

По закінченні навчання можливе точне доналаштування DBN-мережі з учителем для функціонування в якості класифікатора [7].

Переваги мереж глибокого навчання: скорочення розмірності вектора даних (кількості ознак), що збільшує продуктивність при класифікації, та висока точність в задачах розпізнавання складних об'єктів (зображень, мови).

2.4 «Маршрутизуючий сервіс»

Різноманітність загроз, що впливають на інформацію в розподілених мережах, пояснюється складною структурою останніх. Мережеві атаки багатогранні і визначаються рядом факторів: метою зловмисника, об'єктом впливу, архітектурою сегмента мережі. Алгоритм поділу даних в розподілених мережах виступає в якості альтернативи зниження обчислювальних витрат при використанні шифрування [1].

Найбільш поширений клас так званих активних мережевих атак, це для здійснення яких зловмиснику необхідно безпосередньо здійснити взаємодію з деякою системою, яка є частиною мережі. Набір інструментів настільки ж широкий: створення перевантажень серверів, експлуатація недоліків протоколів, використання вразливостей програмного забезпечення. У міжнародній літературі з питань інформаційної безпеки приклади таких атак можна зустріти під назвами «sniffing», «flooding», «smurf», «spoofing», «hijacking» та ін [1].

Існуючі заходи щодо зниження загроз атак ефективні, але, як правило, вузько спеціалізовані. Наприклад, застосування криптографічних інструментів протоколу IpSec робить перехоплення TCP / IP-пакетів недоцільним, але ніяк не

протидіє атакам, що викликають значне завантаження на деяких ділянках шляху проходження трафіку [1].

Розроблено «маршрутизуючий сервіс» SM передачі даних через розподілені мережі. SM - клієнт-серверний додаток, що дозволяє користувачеві передавати дані специфічним маршрутом. Характер маршруту визначається базою критеріїв SM. Серед них, наприклад, такі як швидкість доставки, надійність, безпека й т.п. [1].

У ролі маршрутизаторів для SM виступає деяка множина довірених серверів розподіленої мережі. Під довіреним сервером будемо розуміти деякий багатофункціональний сервер розподіленої мережі, до якого зловмисник не має доступу.

Одним з видів активних мережевих атак є клас атак, заснованих на сніффінгі. Наведемо приклад однієї з них. Зловмисник, володіючи знаннями, що деяка організація регулярно передає дані з A в G, може досить точно визначити маршрут від A до G в момент часу Δt і здійснити перехоплення на якомусь з ділянок проходження трафіку (рисунок 2.6) [1].

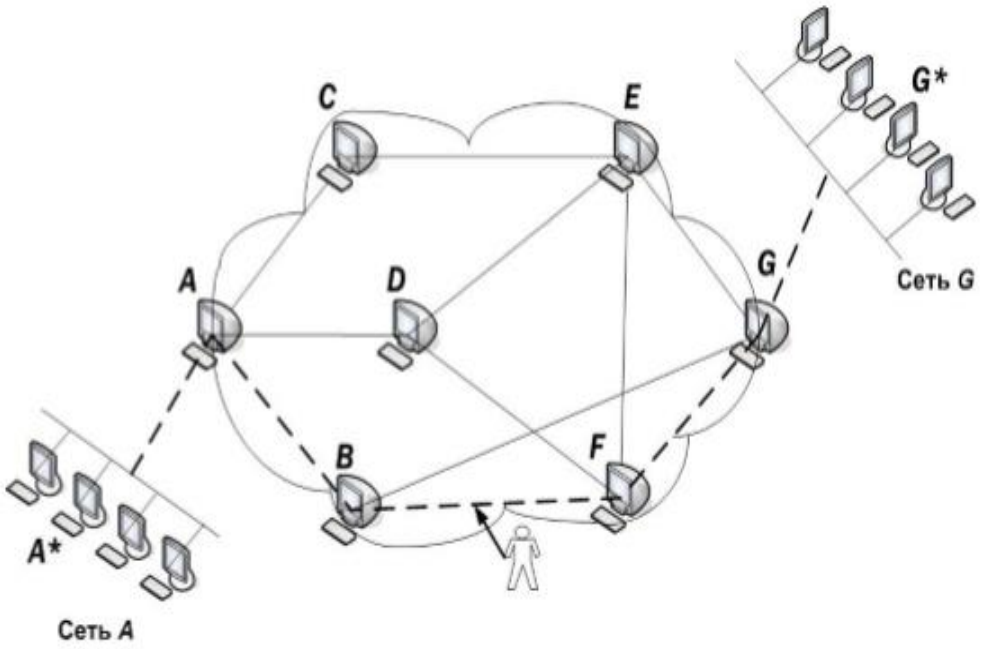

Рисунок 2.6 - Робота протоколів маршрутизації між A і G в момент Δt. Можливий варіант атаки на ділянці BF.

A, B, C, D, E, F, G - поки слід розуміти як деякі вузлові сервера, необхідні для просторового уявлення маршруту слідування трафіку. Так, A - Інтернет-шлюз організації. Виробляючи посилку трасувальних пакетів, зловмисник в

момент часу Δt визначив маршрут прямування трафіку (показано пунктиром) і зробив атаку на підконтрольному маршрутизаторі, розташованому на ділянці BF.

На довірених серверах A_S, B_S, C_S, D_S, E_S, F_S, $G_S \in F$ встановлюється серверна частина сервісу - S_{MS}, що виконує автоматичну «інтелектуальну» маршрутизацію трафіку. Позначимо F - безліч всіх довірених серверів з S_{MS}, а F_t - конкретний довірений сервер. S_{MS} - додатки клієнтської частини сервісу. S_{MS} встановлюється на комп'ютерах користувачів і надає користувачам діалог для ініціалізації процесу передачі даних за участю F_t.

На рисунку 2.7 показано, що використання S_M, дозволило уникнути проходження трафіком підконтрольної зловмисникові ділянки. Дане рішення S_M (підсумковий маршрут) є ймовірним з ймовірністю прийняття p_j, $0<p_j \leq 1, j \in [1,k]$, де k - кількість різних маршрутів від A_S до G_S на графі з вершинами A_S, B_S, C_S, D_S, E_S, F_S, G_S та ребрами, які визначаються поточною топологією мережі. Розрахунок значень p_j буде розглянуто далі. Нагадаємо, що в процесі передачі за допомогою SM дані проходять через деяке число довірених серверів, рівне f (для прикладу на рис. 2.7 f = 3). Вибір кожного наступного сервера відбувається динамічно [1].

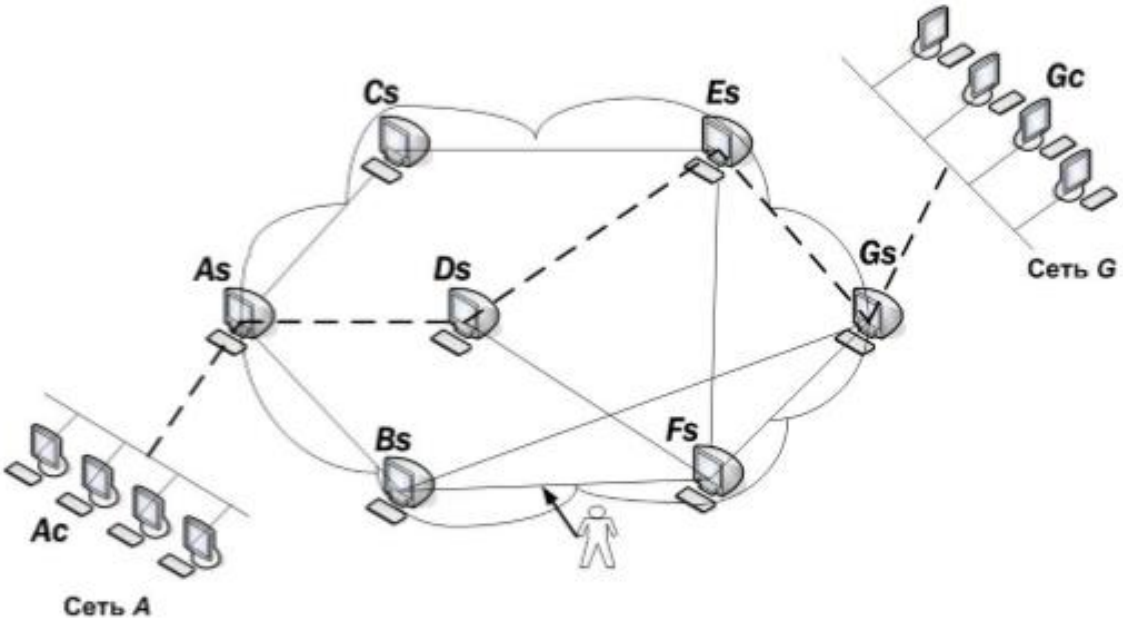

Рисунок 2.7 - Зміна маршруту трафіку за рахунок використання довірених серверів DS, ES

Параметри розподілу:

n - число всіх використовуваних довірених серверів;

c = 1, у разі використання інструменту мультиплексування трафіку c> 1;

a_t - число недоступних для F_t серверів з числа всіх серверів (визначається з динамічної таблиці маршрутизації).

Але далі логічно вважати, що недоступні сервери не беруть участі у вибірці на кожному з етапів передачі.

Таким чином, підсумковий маршрут трафіку від відправника до одержувача при використанні S_M, та f довірених серверів (з n-доступних) буде обраний з ймовірністю [1]

$$p_j = \left(\frac{n-a_0}{c}\right) \times \left(\frac{n-1-a_1}{c}\right) \times \ldots \times \left(\frac{n-f-a_f}{c}\right), j \in [1, k]; \quad (2.1)$$

a_t, – кількість недоступних серверів для F_t, в момент вибору F_{t+1}, довіреного сервера на i + 1 кроці.

$$a_i = n - \sum_{w=1}^{m} m_{iw} \quad (2.2)$$

Якщо мультиплексування не використовується, то

$$p_j = \left(\frac{n-a_0}{c}\right) \times \left(\frac{n-1-a_1}{c}\right) \times \ldots \times \left(\frac{n-f-a_f}{c}\right) = \frac{1}{n-a_0} \times \frac{1}{n-1-a_1} \times \ldots \times \frac{1}{n-f-a_f} \quad (2.3)$$

Розіб'ємо усі мережеві атаки, яким може піддатися розроблена система, на два класи: атаки на трафік між «суміжними» серверами і атаки безпосередньо на довірені сервери f_t. Поняття «суміжності» визначається динамічно для кожного сеансу передачі, наприклад, «суміжними» є сервери f_t і f_{t+1}, вибрані на i та i + 1 етапі передачі [1].

Оцінимо ймовірність реалізації атаки першого класу P_{A1}, коли зловмисник контролює ділянку між довіреними серверами F_t і $F_{t+1}1$. При невідомому просторовому розташуванні F_i вважаємо атаку успішної, якщо при роботі сервісу S_M передавачі F_t і F_{t+1} були обрані на i та i + 1 етапі передач.

$$P_{A1} = \frac{2}{n-a_0} \times \frac{1}{n-1-a_1} + \frac{2}{n-1-a_1} \times \frac{1}{n-2-a_2} + \cdots + \frac{2}{n-(f-1)-a_{f-1}} \times \frac{1}{n-f-a_f} \quad (2.4)$$

Формула (2.4) легко поширюється на випадок підконтрольних зловмисникові ділянок між s-довіреними серверамиF_t , F_{t+1},..., F_{t+3}.

Уявімо другий, більш широкий клас атак у вигляді неординарного (групового) потоку подій, тобто послідовності подій, що входять одна за одною у випадкові проміжки часу.

Той факт, що в один момент часу може надійти кілька загроз різних видів або одного виду, але з різних джерел, визначає неординарність потоку.

Позначимо ω – кількість успішно атакованих серверів в одиницю часу (інтенсивність).

Тоді ймовірність того, що за час t будуть реалізовані атаки на m-довірених серверах (з n доступних) описується розподілом Пуассона [1]:

$$P_{A2}(m,t) = \frac{wt^m}{m!}e^{-wt} \qquad (2.5)$$

Використані спеціальні СВВ-сенсори (система виявлення вторгнень) для реєстрації різних видів мережевих атак на веб-сервери.

Уявімо ω як суму інтенсивностей кінцевого числа різних видів успішних атак, наприклад таких, як спуфинг, «людина посередині», флуд і ін. Таким чином:

$$w = \sum_{i=1}^{k} w_i = \sum_{i=1}^{k} p_i h_i \qquad (2.6)$$

де p_i – ймовірність реалізації атаки і-го вида;

h_i – кількість атак і-го вида.

Практично неможливо дати точну оцінку ω, тому що її величина залежить від багатьох факторів: часу спостереження, розташування сервера, функціонального призначення сервера та ін.

Ця методика захису інформації в розподілених мережах включає в себе послідовність наступних дій [1]:

- аналіз топології розподіленої мережі. Вибір пристроїв мережі для ролі «довірений сервер»;
- встановлення та налаштування SMS на надійних серверах, SMC на робочих станціях;
- вибір параметрів передачі SMC;

- передача даних через довірені сервера на основі алгоритму динамічної маршрутизації;
- приймання даних одержувачем, збір статистики по побудованим маршрутами, оцінки реалізацій можливих атак.

2.5 Розроблення алгоритму роботи маршрутизуючого сервісу

Головною особливістю запропонованого підходу є застосування динамічної маршрутизації для цілей захисту інформації.

Розроблений алгоритм динамічної маршрутизації інформації в розподілених безпровідних мережах, описується наступними етапами.

Крок 1. Обчислення елементів множин M і FS в початковий момент часу t_0.

Крок 2. Ініціалізація передачі. При надходженні запиту SMC на ініціалізацію сеансу передачі даних виконати наступні дії:

2.1. Запитати значення параметра f;

2.2. Створити пакет інструкцій, що містить ip-адресу відправника, ip-адресу одержувача, значення f і розділ «довірені сервера»;

2.3. Використовуючи операцію рандомізації, отримати псевдовипадкове число k;

2.4. Перевірити доступність FSk , якщо сервер недоступний – повернутися до п. 2.3;

2.5. Сформувати пакет даних і промаркувати його як пакет SM;

2.6. Відправити пакет даних і пакет інструкцій на модуль сервер FSk. Якщо потрібно подальша передача даних – повернутися до п. 2.5;

2.7. Завершити роботу SMC.

Крок 3. Динамічна маршрутизація на довіреному сервері.

3.1. Переформувати матрицю маршрутизації у випадку, якщо є різниця поточного часу та часу останньої зміни в таблиці маршрутизації.

3.2. Відкрити отриманий пакет інструкцій, якщо кількість запитів в розділі «довірені сервера» дорівнює f, відправити пакети даних, що відносяться до даного пакету інструкцій, на ip-адресу отримувача и повернутись до п.3.1.

Крок 4. Отримання пакета даних та пакету інструкцій SMC, визначаються ip-адресою одержувача.

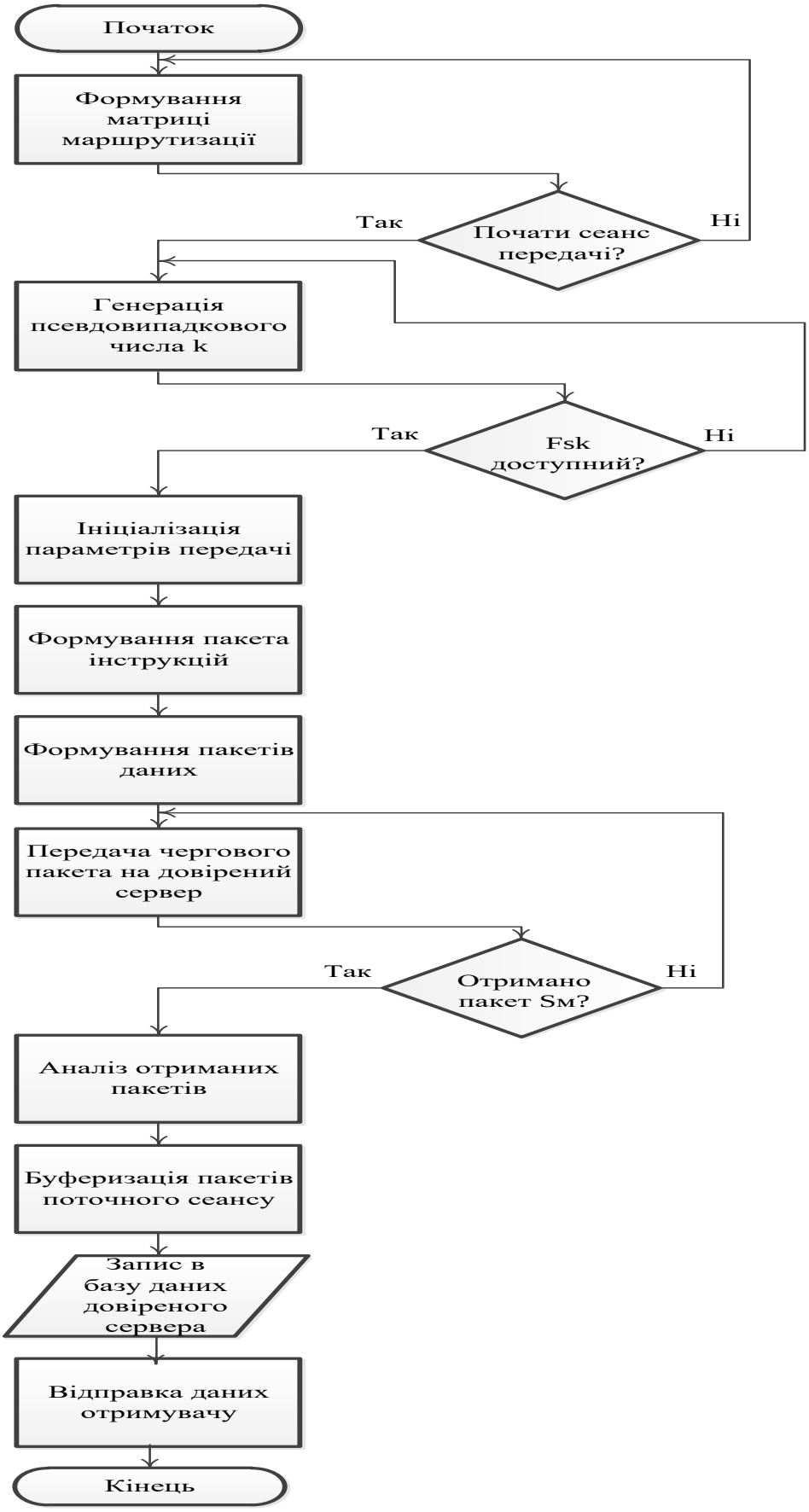

Рисунок 2.8 - Блок-схема алгоритма динамічної маршрутизації

2.6 Розроблення структурної схеми маршрутизуючого сервісу

Відповідно до задач досліджень була розроблена структурна схема, яка наведена на рисунку 2.9.

Структурна схема комплексу «маршрутизуючий сервіс» містить чотири основних блоки. Кожен блок виконує певне функціональне призначення.

1. Блок RD – з потоку IP-пакетів виділяє пакети з маркером SM. Перевіряє їх за допомогою таблиць маршрутизації та робить повторний запит пакетів у разі необхідності.Передає ці пакети блоку SD.

2. Блок SD – база даних, що містить відомості про пакети SM, оброблених довіреним сервером SF. У разі необхідності буферизують пакети даних.

3. Блок AD – аналізує пакети даних та інструкцій, прийнятих від блоку SD, додає інформацію про поточний довірений сервер SF , у пакет інструкцій. Передає блоку MD команди на передачу даних і трасування довірених серверів, формує таблицю маршрутизації. Отримує від SD інформацію про нові надійні сервери, що з'явилися в мережі.

4. Блок MD – відправляє черговий пакет на один з обраних довірених серверів або в пункт призначення.

2.7 Модель потоку атак

Спроектуємо модель потоку атак, котра не залежить від перерахованих вище факторів (рисунок 2.10). У цій схемі змодельований ординарний потік атак, модель групового потоку будується аналогічним чином.

Наведемо позначення змінних і процедур, що використовуються в схемі:

- n - кількість довірених серверів в мережі;
- k - кількість видів атак;
- T - час дії обраного виду атаки;
- u_1 - час очікування в разі невдалого результату атаки;
- u_2 - час блокування довіреної сервера в разі успішного результату атаки;
- F - довірений сервер;
- p_i - ймовірність реалізації атаки і-го виду;
- i, j, t, t_j - допоміжні змінні;
- CurTime - місцевий час.

Рисунок 2.9 – Структурна схема «Маршрутизуючого сервіса»

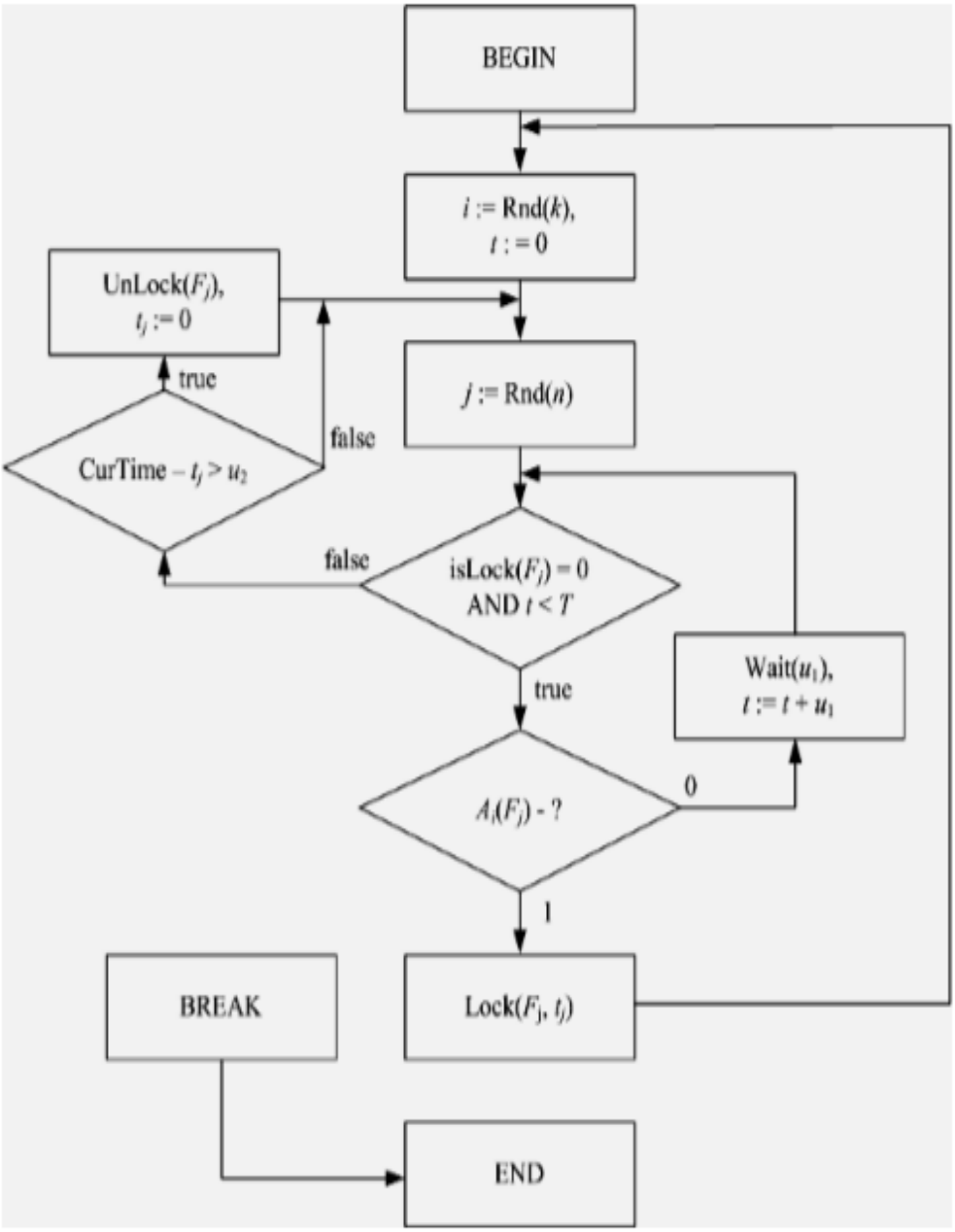

Рисунок 2.10 - Блок-схема алгоритму генерації потоку атак на довірені сервера

Процедури та функції:

- Rnd (x) - генерація випадкового цілого числа на інтервалі [1; x], x> = 1;

- Unlock (F_j) - розблокувати сервер F_j;

- Ai (F_j) - результат експерименту «атака на сервер F_j», що визначається дискретною випадковою величиною з розподілом «ймовірність прийняти значення 1 (успіх) дорівнює p_i, ймовірність прийняти значення 0 (невдача) дорівнює 1 - p_i, »;

- Wait (x) - пауза на час x;

- isLock (F_j) - повертає статус сервера F_j (перебуває за межами покриття заблокований);

- Lock (F_j, x) - заблокувати F_j і повернути даний час в змінну x .

Отримані оцінки реалізації мережевих атак показують, що застосування програми «маршрутизуючий сервіс» дозволяє підвищити безпеку передачі інформації в розподілених безпровідних мережах. Підвищення захищеності інформації в розподілених безпровідних мережах при використанні SM досягається за рахунок підвищення захисту її конфіденційності, цілісності і доступності. Цілісність та конфіденційність переданої інформації забезпечується зменшенням ймовірності реалізації мережевих атак на контрольованих ділянках проходження трафіку в разі застосування «маршрутизуючого сервісу». Доступність обґрунтовується стійкістю системи до блокування порушником одного або кількох довірених серверів. У разі збою в роботі одного або кількох довірених серверів, «маршрутизуючий сервіс» моментально відновлює маршрут прямування трафіку до того часу, поки працездатність довірених серверів не відновиться. Слідує також ще одна важлива якість розробленого додатка - кожен з довірених серверів може динамічно вносити зміни в маршрут проходження трафіку.

2.8 Висновки по науково-дослідній частині

В данній роботі були розглянуті проблеми інформаційної безпеки бездротових мереж, основні підходи до вирішення цих проблем, а також був проведений аналіз існуючих методів та алгоритмів виявлення мережевих атак.

Показана можливість вбудовування в SM алгоритмів мультиплексування. Розроблені математична модель, схема-алгоритм та структурна схема «маршрутизуючого сервісу» на основі динамічної маршрутизації.

Таким чином, можна об'єднати два підходи до забезпечення безпеки інформації, що передається: з одного боку, знизити ймовірність доступу зловмисника до використовуваних каналів зв'язку, а з іншого - застосувати логічне перетворення інформації. У даній роботі в системі поділу даних виділяються три основних елементи: мультиплексор, демультиплексор і передавачі. По виконуваних функцій передавачі близькі до довірених серверів SM. Даний факт створює хороші передумови для інтеграції двох систем. Використання «маршрутизуючого сервісу» SM для передачі даних через розподілені мережі дозволяє значно знизити ймовірність реалізації класу

активних мережевих атак зловмисника без використання будь-яких інструментів шифрування.

3 РОЗРОБЛЕННЯ АЛГОРИТМУ ФУНКЦІОНУВАННЯ ТА СТРУКТУРНОЇ СХЕМИ ПРИСТРОЮ

3.1 Обґрунтування структурної схеми

Рівень мережі (Network Layer) служить для утворення єдиної транспортної системи, що об'єднує декілька мереж, причому ці мережі можуть використовувати різні принципи передачі між кінцевими вузлами і володіти довільною структурою зв'язків.

На рівні мереж сам термін мережа наділяють специфічним значенням. У даному випадку під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до однієї зі стандартних топологій і використовуючих для передачі даних один з протоколів канального рівня, визначений для даної топології [4].

Усередині мережі доставлення даних забезпечується відповідним канальним рівнем, а ось доставленням даних між мережами займається рівень мереж, який й підтримує можливість правильного вибору маршруту передачі повідомлення, навіть у тому випадку, коли структура зв'язку між великими складеними мережами має характер, відмінний від прийнятого в протоколах канального рівня.

Проблема вибору найкращого шляху називається маршрутизацією, й її вирішення є однією з головних задач рівня мереж. Ця проблема ускладнюється тим, що найкоротший шлях не завжди найкращий. Часто критерієм при виборі маршруту є час передачі даних по цьому маршруту; воно залежить від пропускної спроможності каналів зв'язку та від інтенсивності трафіку, яка може змінюватися в часі. Деякі алгоритми маршрутизації намагаються пристосуватися до зміни навантаження, в той час як інші приймають рішення на основі середніх показників за тривалий час. Вибір маршруту може здійснюватися й за іншими критеріями, наприклад надійності передачі [12].

У загальному випадку функції рівня мереж ширше, ніж функції передачі повідомлень по зв'язках з нестандартною структурою. Рівень мереж вирішує також задачі узгодження різних технологій, спрощення адресації у великих мережах та створення надійних і гнучких бар'єрів на шляху небажаного трафіку між мережами.

Повідомлення рівня мереж прийнято називати пакетами (packets). При організації доставлення пакетів на мережевому рівні використовується поняття

"номер мережі". У цьому випадку адреса одержувача складається зі старшої частини - номера мережі та молодшої частини - номера вузла в цій мережі. Усі вузли однієї мережі повинні мати одну й ту ж старшу частину адреси, тому терміну "мережа" на рівні мереж можна дати й інше, більш формальне визначення: мережа - це сукупність вузлів, адреса мереж яких містить один й той же номер мережі [2].

На рівні мереж визначаються два види протоколів. Перший вид - протоколи мереж - реалізують просування пакетів через мережу. Саме ці протоколи мають на увазі, коли говорять про протоколи рівня мереж. Однак, часто до рівня мереж відносять й інший вид протоколів, які називають протоколами обміну маршрутною інформацією або просто протоколами маршрутизації.

Основна функція маршрутизатора - читання заголовків пакетів протоколів мереж, прийнятих і буферизованих по кожному порту, та прийняття рішення про подальший маршрут слідування пакету за його адресою мережі, що включає номер мережі і номер вузла.

Функції маршрутизатора можуть бути розбиті на 3 групи відповідно до рівнів моделі OSI [4].

Рівень інтерфейсів.

Інтерфейси маршрутизатора, виконують повний набір функцій фізичного та канального рівнів по передачі кадру, включаючи одержання доступу до середовища, формування бітових сигналів, прийом кадру, підрахунок контрольної суми і передачу поля даних кадру верхньому рівню.

Рівень протоколу мереж.

Мережевий протокол витягує з пакета заголовок рівня мереж і аналізує вміст його полів. Перевіряється контрольна сума, і якщо пакет прийшов ушкодженим, то він відкидається. Перевіряється час життя пакету, вносяться корегування в вміст деяких полів, перераховується контрольна сума [4].

На рівні мереж виконується одна з найважливіших функцій маршрутизатора - фільтрація трафіку. Маршрутизатор дозволяє задавати та оброблювати складні правила фільтрації. Пакет рівня мереж, що знаходиться в полі даних кадру для маршрутизаторів, представляється неструктурованою двійковою послідовністю. Маршрутизатори, програмне забезпечення яких містить модуль протоколу мереж, здатні виконувати розбирання та аналіз окремих полів пакета. Вони облаштовуються розвиненими засобами для

користувача інтерфейсу, які дозволяють адміністратору задавати складні правила фільтрації [4].

У разі якщо інтенсивність надходження пакетів вище швидкості обробки, пакети можуть утворити чергу. Існують різні дисципліни обслуговування пакетів: в порядку надходження за принципом "перший прийшов - перший обслужений" (First Input First Output, FIFO) випадкове раннє виявлення, коли обслуговування йде за правилом FIFO, але при досягненні чергою певної довжини, знову надходять пакети відкидаються, а також різні варіанти пріоритетного обслуговування.

Основна функція маршрутизатора - визначення маршруту пакета. За номером мережі, витягнутої з заголовка пакета, модуль протоколу мереж знаходить в таблиці маршрутизації, рядок, що містить мережеву адресу наступного маршрутизатора, і номер порту, на який потрібно передати пакет, щоб він рухався в потрібному напрямку. Якщо в таблиці відсутній запис про мережі призначення пакета, і, до того ж, немає запису про маршрутизатор за замовчуванням, то пакет відкидається [7-9].

Перед тим як передати адресу мережі наступного маршрутизатора на канальний рівень тієї технології, яка використовується в мережі, що містить наступний маршрутизатор. Для цього мережевий протокол звертається до протоколу дозволу адрес. Протоколи цього типу встановлюють відповідність між мережевими та локальними адресами або на підставі заздалегідь складених таблиць, або шляхом розсилки широкомовних запитів. Таблиця відповідності локальних адрес, адреси мереж будуються окремо для кожного інтерфейсу мереж. Протоколи дозволу адрес займають проміжне положення між рівнями мереж і канальними рівнями [8].

З рівня мереж пакет, локальна адреса наступного маршрутизатора і номер порту маршрутизатора передаються вниз, канальному рівню. На підставі зазначеного номера порту здійснюється комутація з одним з інтерфейсів маршрутизатора, засобами якого виконується упаковка пакету в кадр відповідного формату. У полі адреси призначення заголовка кадру поміщається локальний адрес наступного маршрутизатора. Готовий кадр відправляється в мережу.

Рівень протоколів маршрутизації.

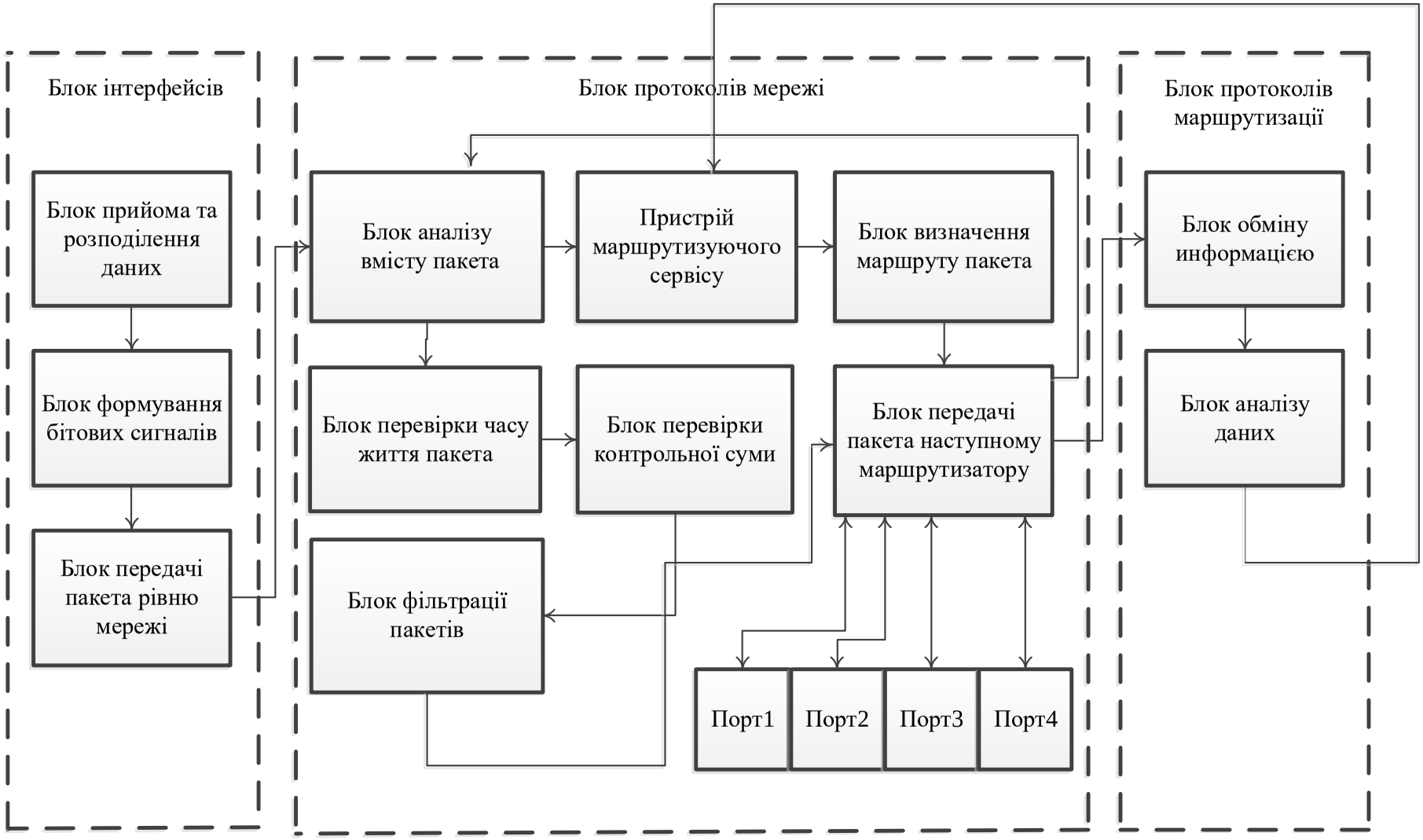

Рисунок 3.1 – Структурна схема пристрою

Протоколи мереж активно користуються у своїй роботі таблицею маршрутизації, але ні її побудовую, ні її підтриманням не займаються. Ці функції виконують протоколи маршрутизації. На підставі цих протоколів маршрутизатори обмінюються інформацією про топологію мережі. А потім аналізують отримані відомості, визначаючи найкращі за тими чи іншими критеріями маршрути. Результати аналізу і складають вміст таблиць маршрутизації [4].

3.2 Розробка алгоритму функціонування

Алгоритм функціонування — це сукупність правил, що ведуть до правильного виконання технічного процесу в якому-небудь пристрої або в сукупності пристроїв (системі).

Алгоритм функціонування маршрутизатора такий: на рівні інтерфейсів маршрутизатор отримує доступ до середовища та виконує функції фізичного та канального рівня по передачі даних. Після чого передає данні кадра верхньому рівню [2].

На рівні протокола мережі виконується виконується фільтрація трафіка. Із пакета витягується заголовок рівня мережі та аналізуються його вміст. Перевіряється час життя пакета та контрольна сума, якщо пакет прийшов пошкодженим, то він видаляється. Якщо час життя не вийшов, то вносяться деякі поправки до вмісту полів, та перераховується контрольна сума.

Робота на рівні мереж дозволяє виробляти інтелектуальну обробку пакетів. Оскільки маршрутизатори в основному працюють з протоколом IP, вони повинні підтримувати зв'язок без створення логічного з'єднання між абонентами. При цьому кожен пакет обробляється і відправляється одержувачу незалежно.

Визначення маршруту пакета виконується по номеру мережі, визначеному із заголовку пакета. В таблиці маршрутизації знаходиться рядок, який містить в собі адресу наступного маршрутизатора та номер порта на який потрібно передати пакет. Коли маршрутизатор отримує пакет, він зчитує адресу призначення і визначає, за яким маршрутом відправити пакет. Зазвичай маршрутизатори зберігають дані про декілька можливих маршрутах.

Таблиці маршрутизації містять в собі отримані дані про топологію мережі, аналізуючи ці дані визначаються найкращий маршрут за певними критеріями. Вираховується вартість доставки та обирається шлях з меншою вартістю. Найпростіші алгоритми маршрутизації визначають маршрут на підставі

найменшого числа проміжних (транзитних) вузлів на шляху до адресату. Більш складні алгоритми в поняття "вартість" закладають кілька показників, наприклад, затримку при передачі пакетів, пропускну спроможність каналів зв'язку або грошову вартість зв'язку. Основним результатом роботи алгоритму маршрутизації є створення та підтримка таблиці маршрутизації, в яку записується вся маршрутна інформація. Зміст таблиці маршрутизації залежить від використовуваного протоколу маршрутизації [2].

Алгоритми маршрутизації застосовуються для визначення оптимального шляху пакетів від джерела до одержувача і є основою будь-якого протоколу маршрутизації. Алгоритми маршрутизації повинні швидко і правильно враховувати зміни в стані мережі (наприклад, відмова вузла або сегмента мережі). Процес узгодження інформації про топологію мережі між маршрутизаторами називається збіжністю [9].

Алгоритми маршрутизації повинні бути прості в реалізації та використовувати якомога менше ресурсів. Алгоритми повинні бути стійкими до відмов обладнання на попередньо вибраному маршруті, високих навантажень та помилок у побудові мережі. Якщо певна подія в мережі приводить до того, що деякі маршрути стають недоступні або виникають нові маршрути, маршрутизатори розсилають повідомлення про це один одному по всій мережі. Після отримання цих повідомлень маршрутизатори виробляють перепризначення оптимальних маршрутів, що в свою чергу може породити новий потік повідомлень. Цей процес повинен завершитися, причому досить швидко, інакше в топології мережі можуть з'явитися петлі, або мережа взагалі може перестати функціонувати.

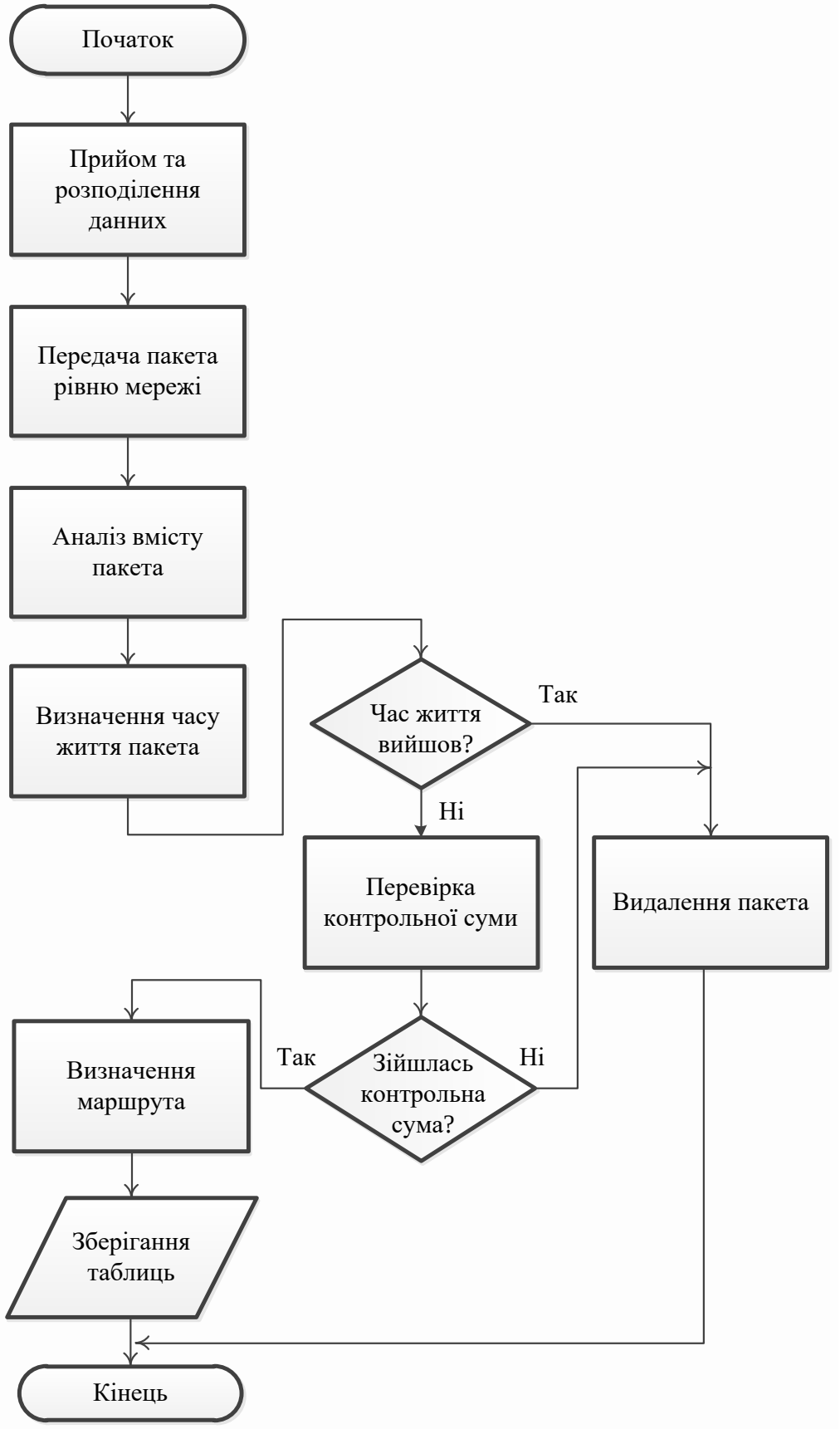

Рисунок 3.2 – Алгоритм функціонування пристрою

4 РОЗРОБЛЕННЯ СХЕМИ ЕЛЕКТРИЧНОЇ ФУНКЦІОНАЛЬНОЇ ПРИСТРОЮ

У даному розділі буде більш детально розглянуто робота пристрою в цілому й окремо кожен блок.

Як було вище викладено, суть пристрою полягає в тому, що використовується одна або більше метрик для визначення оптимального шляху передачі мережевого трафіку на підставі інформації мережевого рівня.

Пристрій розбито на кілька основних блоків, це: мікропроцесорний блок, блок пам’яті, інтерфейсний блок та блок модуля Ethernet контролера.

Мікропроцесорний блок.

Мікропроцесор - центральний пристрій (або комплекс пристроїв) ЕОМ (або обчислювальної системи), яке виконує арифметичні та логічні операції, задані програмою перетворення інформації, керує обчислювальним процесом і координує роботу пристроїв системи (запам'ятовуючих, сортувальних, введення - виведення, підготовки даних й ін.) [11]. В обчислювальній системі може бути декілька паралельно працюючих процесорів; такі системи називають багатопроцесорними. Наявність декількох процесорів прискорює виконання однієї великої або декількох (в тому числі взаємозалежних) програм. Основними характеристиками мікропроцесора є швидкодія та розрядність. Швидкодія - це число виконуваних операцій у секунду. Розрядність характеризує обсяг інформації, який мікропроцесор обробляє за одну операцію: 8-розрядний процесор за одну операцію обробляє 8 біт інформації, 32-розрядний - 32 біта, 64-розрядний - 64 біта. Швидкість роботи мікропроцесора багато в чому визначає швидкодія комп'ютера. Він виконує всю обробку даних, що надходять у комп'ютер і зберігаються в його пам'яті, під керуванням програми, також зберігається в пам'яті [11].

Блок пам'яті.

Блок управління пам'яттю або пристрій управління пам'яттю (англ. MMU) - компонент апаратного забезпечення пристроя, що відповідає за управління доступом до пам'яті, запитуваною центральним процесором. Його функції полягають у трансляції адрес віртуальної пам'яті в адреси фізичної пам'яті (тобто управління віртуальною пам'яттю), захисту пам'яті, управлінні кеш-пам'яттю, арбітражем шини, перемиканням блоків пам'яті [11].

Інтерфейсний блок.

Блок даних, що передається між логічними об'єктами суміжних рівнів. Мікроконтролер - мікросхема, призначена для керування електронними пристроями [11]. Типовий мікроконтролер поєднує на одному кристалі функції процесора та периферійних пристроїв, містить ОЗУ та (або) ПЗУ. По суті, це однокристальний комп'ютер, здатний виконувати прості завдання. Ethernet контролери служать для введення-виведення інформації в канал зв'язку через RJ-45. Відповідно, інтерфейсний блок служить для обміну інформацією мікропроцесорного блоку з Ethernet-контролерами. У цьому пристрої, він виконує функцію обробки пакетів, налаштування затримки та подачі сигналу подальшого влаштування обробки інформації. Управляється даний пристрій, за рахунок програмного забезпечення.

Головним завданням є правильно зібрати даний пристрій, запустити, та провести його наладку. Загальний схемний вид зібраного пристрою представлений на функціональній схемі пристрою.

5 РОЗРОБЛЕННЯ СХЕМИ ЕЛЕКТРИЧНОЇ ПРИНЦИПОВОЇ ПРИСТРОЮ

5.1 Вибір елементної бази

Під час розроблення принципової схеми важливим етапом є вибір елементної бази, яка складає кожен з блоків проектуючого пристрою. Головним при виборі елементної бази є постановка задачі.

Основною характеристикою для вибору елементів буде - адаптація мікропроцесора до особливостей конкретної задачі, що здійснюється в основному шляхом розробки відповідного програмного забезпечення, яке заноситься потім в пам'ять програм.

Один із широко використовуваних класів великих інтегральних схем (ВІС) є однокристальні мікро-ЕОМ. Однокристальної мікро-ЕОМ називають БІС, в напівпровідниковому кристалі якої цілком реалізована закінчена мікропроцесорна система з центральним процесором, пам'яттю, портами вводу-виводу і іншими периферійними пристроями. Широко використовуються безліч серій однокристальних мікро-ЕОМ [12].

Основною архітектурною особливістю однокристальних мікро-ЕОМ є використання роздільної пам'яті програм (ПЗП) та даних (ОЗП) [12]. Такий поділ дозволяє спростити виконання більшості команд і підвищити швидкодію мікро-ЕОМ. Архітектура однокристальних мікро-ЕОМ - результат еволюції архітектури мікропроцесорів і мікропроцесорних систем, обумовленої прагненням істотно знизити їх апаратні витрати і вартість. Як правило, ці цілі досягаються як шляхом підвищення рівня інтеграції БІС, так й за рахунок пошуку компромісу між вартістю, апаратними витратами та технічними характеристиками. Така мікро - ЕОМ представляє прилади, які конструктивно виконані у вигляді однієї ВІС та включає в себе усі пристрої, що необхідні для реалізації цифрової системи управління мінімальної конфігурації. Це процесор, запам'ятовуючий пристрій даних, запам'ятовуючий пристрій команд, внутрішній генератор тактових сигналів, а також програмовані інтегральні схеми для зв'язку із зовнішнім середовищем.

Оскільки основною частиною проектуючого пристрою є МП, то вибір елементної бази буде ґрунтуватися на виборі мікропроцесора. У роботі обрано мікропроцесор серії КР1821ВМ85А.

Мікросхеми КР1821ВМ85А являють собою 8-розрядний статичний мікропроцесор і призначені для побудови мікро-ЕОМ, які використовуються в системах передачі та обробки інформації. КР1821 вимагають одного джерела живлення напругою + 5В, робоча потужність близько 1,5 Вт і працюють з номінальною частотою 18500кГц. По входах і виходах серії 1821 електрично сумісні з інтегральними схемами ТТЛ [13].

Виходячи з даної характеристики однокристальних ЕОМ серії 1821, видно, що вони володіють значними функціонально-логічними можливостями і являють собою ефективний засіб автоматизації різних об'єктів і процесів.

Для управління зовнішніми пристроями, а також для забезпечення необхідної швидкості введення отриманого коду в пам'ять, необхідно застосувати контролер КР580ВВ55.

Запам’ятовуючі пристрої (ЗП) мікропроцесорних систем на базі БІС МП К1821ВМ85 мають байтовую організацію та реалізуються так само, як й ЗП для систем на базі БІС КР580 і 8086А. Тому, як ПЗУ можна використовувати БІС К573РФ5. В якості проектованого ОЗП вибираємо статичне ОЗП HM6116.

Блок модуля Ethernet контроллера на RTL8019AS. RTL8019AS - інтегрований на кристалі контролер Ethernet, повністю відповідний стандарту 10BASE-T/100BASE-TX [12].

5.2 Розрахунок та синтез основних електронних вузлів та блоків пристрою

Мікропроцесор - функціонально закінчений пристрій обробки інформації, що керується пам’яттю, яка зберігається в програмі [12]. Поява мікропроцесорів (МП) стала можливим завдяки розвитку інтегральної електроніки. Це дозволило перейти від схем малого та середнього ступеню інтеграції до великих й надвеликих інтегральних мікросхем (ВІС й НВІС). Центральний процесорний модуль є основним блоком контролера. Він забезпечує управління та синхронізацію роботи всього пристрою, забезпечує прийом, передачу, зберігання та обробку даних, що надходять з системної шині.

Таблиця 5.1 – Призначення виводів микропроцессора

Виводи	**Призначення**	**Опис**
AD0 – AD7	Двонаправлена, три стани	Шина адреси/даних

AD8 – AD15	Вихід, три стани	Шина адреси
ALE	Вихід	Роздільна здатність захвата адреси
RD	Вихід, три стани	Управління зчитуванням
WR	Вихід, три стани	Управління записом
IO/M	Вихід, три стани	Показник ВП або пам’яті
S0 , S1	Вихід	Показник стану шини
READI	Вихід	Виклик стану очікування
SID	Вихід	Введення послідовних даних
SOD	Вихід	Вивід послідовних даних
HOLD	Вихід	Вимоги захвата
HLDA	Вихід	Підтвердження стану захвата
INTR	Вхід	Запит переривання
TRAP	Вхід	Запит немаскованого переривання
RST 5.5 RST 6.5 RST 7.5	Вхід	Запит апаратного векторного переривання
INTA	Вхід	Підтвердження запита на переривання
RESET IN	Вхід	Анулювання системи
RESET OUT	Вхід	Анюлювання периферії
X1 , X2	Вхід	З’єднання кристала або зовнішнего ГТІ
CLK	Вхід	Сигнал внутрішнього ГТІ

Центральний процесорний модуль базується на мікросхемі КР1821ВМ85А (DD1), й до його складу входять два буферних регістра КР580ІР82 (DD5, DD6), двонаправлений шинний формувач КР580ВА86 (DD7), мультиплексор К555КП11 (DD8), зовнішній резонатор (ZQ, C1) та схема формування скидання (R1, C2, S) [12].

Мікросхеми КР1821ВМ85А являють собою 8-розрядний статичний мікропроцесор і призначені для побудови мікро-ЕОМ, які використовуються в системах передачі та обробки інформації [13]. Мікропроцесор серії КР1821ВМ85А має суміщені шину даних та шину адреси. Для розділення сигналів цих шин застосовуються буферні регістри. Поява в першому такті машинного циклу на шині A15-A8 старшого байта адреси, а на шині AD7-AD0 - молодшого, стробується сигналом процесора ALE, який використовується для дозволу запису в регістри. При передачі по шині AD7-AD0 даних цей сигнал відсутній. Таким чином, в регістрах буде записана адреса, а дані будуть передаватися через шинний формувач. До того ж, регістри та шинний формувач виконують функцію збільшення навантажувальної здатності ЦПМ (32 мА / вивід).

Буферний регістр адреси служить для прийому та зберігання адресної частини виконуваної команди.

Буферний регістр даних використовується для тимчасового зберігання вибраного з пам'яті слова перед видачею його в зовнішню шину даних. Його розрядність визначається кількістю байтів інформаційного слова.

Таблиця 5.2 - Призначення виводів буферного регістра КР580ІР82

Номер вивода	**Позначення**	**Назначення**
1 – 8	DI0 – DI7	Входи регістра
9	OE	Дозволення вихода
10	GND	Загальний
11	STB	Строб
19 – 12	DO0 – DO7	Виходи регістра
20	Ucc	+5 В

Мультиплексор (DD5) перетворює сигнали процесора в сигнали читання / запису пам'яті та зовнішніх пристроїв - MEMR, MEMW, I / OR, I / OW.

Саме від вибору процесора залежить швидкодія системи в цілому, точність обробки даних, а також зручність розробки програмного забезпечення для всього контролера.

Таблиця 5.3 - Призначення виводів шинного формувача КР580ВА86

Номер вивода	**Позначення**	**Призначення**

1 – 8	A0 – A7	Шина
9	OE	Дозволення
10	GND	Загальний
11	T	Направлення
19 – 12	B0 – B7	Шина
20	Ucc	+5 В

Оптимальним для проектованого пристрою буде мікропроцесор КР1821ВМ85А, який має ряд переваг [12]:

- орієнтування на роботу в складі мікроконтролерів;
- низька вартість;
- програмна сумісність з мікропроцесором КР580ВМ80А;
- наявність одного джерела живлення +5 В;
- наявність вбудованого генератора тактових імпульсів;
- вбудований системний контролер;
- вбудований контроллер переривання.

Недоліки цього мікроконтролера:

- розрядність оброблюваних даних 8 біт;
- низька швидкодія (тривалість одного машинного такту ~ 0,5 мкс;
- час виконання однієї команди ~ 7-8 мкс);
- відсутність команди ділення в наявному складі команд.

Що б стабілізувати частоту системного генератора до виводів X1 та X2 ВІС КР1821ВМ85А підключають кварцовий резонатор з номінальною частотою 18500кГц. При цьому тривалість машинного такту буде дорівнює 0,486 мкс [12].

Конденсатор С2 - підстрочечний та використовується для регулювання частоти системного генератора в невеликих межах. Ланцюжок R1C1 служить для короткочасного формування імпульсу з негативним переднім фронтом тривалістю не менше 1,5 мкс.

R1C1 τ = 10 мкс, R1 = 10 кОм, а C1 = 1000 пФ.

Принцип роботи формування схеми скидання полягає в наступному: в нормальному стані С1 заряджений і вхід ВІС КР1821ВМ85А RESI через резистор R1 з'єднаний з джерелом живлення + 5В, що тримає на ньому «логічну одиницю» [12]. При замиканні перемикача S, конденсатор С1 розряджається на корпус. При розмиканні перемикача починається зарядка конденсатора, а вхід RESI ВІС КР1821ВМ85А виявляється при цьому замкнутим на корпус, що відповідає стану «логічного нуля». По закінченню зарядки, на вході RESI знову встановлюється «логічна одиниця».

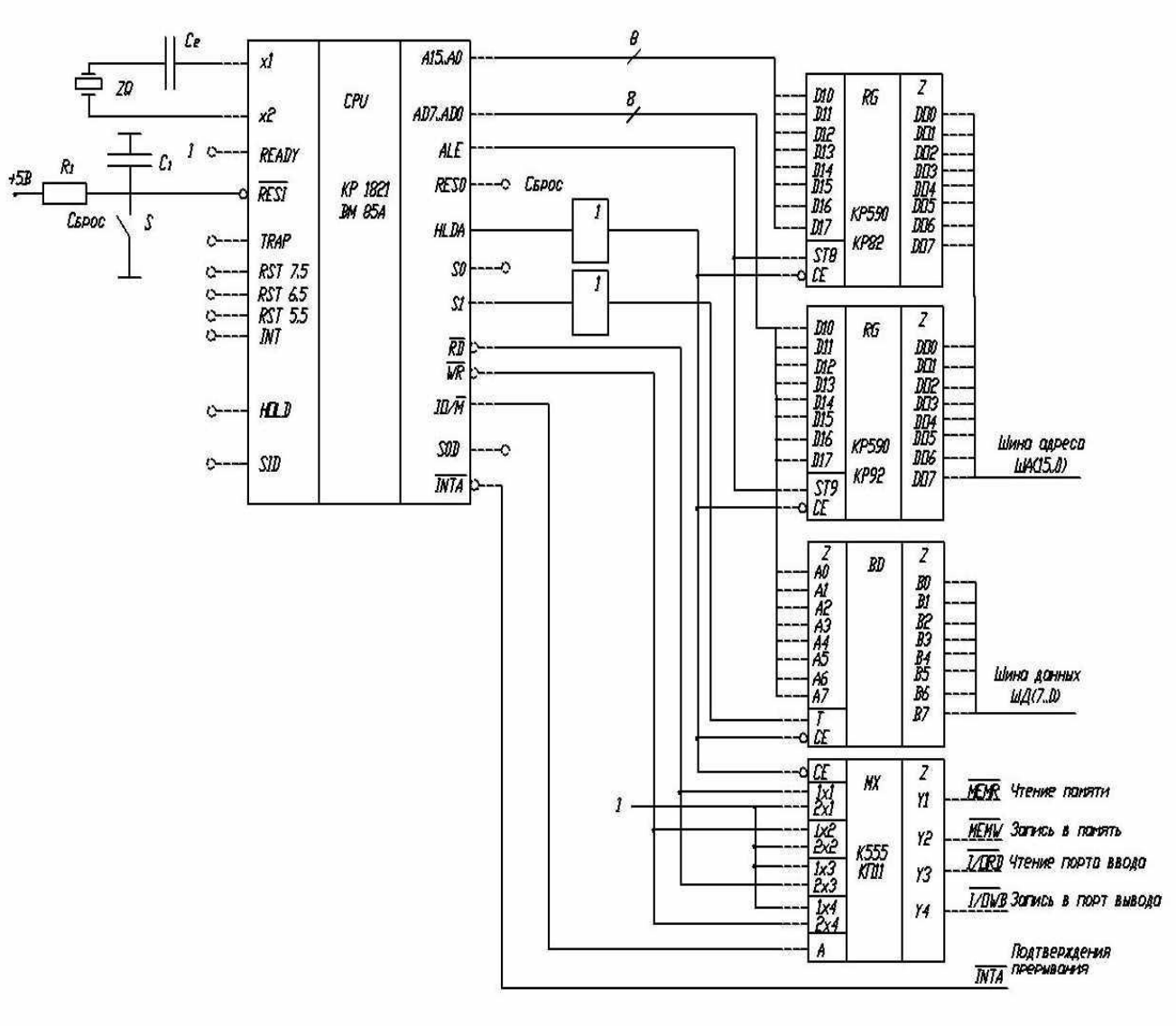

Рисунок 5.1 – Структура процессора на КР1821ВМ85А

Завданням блоку пам'яті є зберігання програм та даних. Існує два класи запам'ятовуючих пристроїв, а саме первинні та вторинні. Первинний пристрій (primary storage) - це пам'ять, швидкодія якої визначається швидкістю роботи електронних схем. Поки програма виконується, вона повинна зберігатися в первинній пам'яті. Ця пам'ять складається з великої кількості напівпровідникових осередків, кожна з яких може зберігати один біт інформації. Осередки рідко зчитуються окремо - зазвичай вони обробляються групами фіксованого розміру, званими словами. Пам'ять організована так, що вміст одного слова, що містить n біт, може записуватися або зчитуватися за одну базову операцію [12].

Для полегшення доступу до слів в пам'яті з кожним словом пов'язується окрему адресу. Адреси - це числа, що ідентифікують конкретні місця розташування слів у пам'яті. Для того щоб прочитати слово з пам'яті або записати його в пам’ять, необхідно вказати його адресу і задати керуючу команду, яка почне відповідну операцію.

До складу блоків пам'яті в проектованому пристрої входять постійний запам'ятовуючий пристрій (ПЗП) та оперативний пристрій (ОЗП). У ПЗП зберігається код програми, в ОЗП - вхідні змінні, проміжні дані, результат обчислень. Для нормального функціонування проектованого контролера достатньо невеликого обсягу ПЗП, тому доцільно використовувати ПЗУ К573РФ обсягом 2 Кбайт . ІМС має 11 адресних входів, 8 виходів даних, входи дозволу програмування WE, вибірки кристала CS, дозволу виходів OE.

Адресні входи A0-A10 підключаються до шини адреси контролера, виходи даних D0-D7 - до шини даних. Вибірка кристала та дозвіл виходу управляються дешифратором ОЗП / ПЗП. Вхід дозволу програмування з'єднаний з джерелом живлення, бо передбачається, що ІМС ПЗП спочатку містить керуючу програму. При включенні живлення і після скидання, мікропроцесор завжди починає зчитувати код команди, розташований в осередку з адресами 0000H-087FH. Апаратним шляхом осередків пам'яті ПЗП та ОЗП можна привласнити будь-які адреси, починаючи від 0 до 65535, але при цьому треба враховувати ту обставину, що при включенні живлення та після скидання мікропроцесор завжди починає зчитувати код команди, розташований в комірці з адресою 0000H [12].

В якості проектованого ПЗУ вибираємо мікросхему К573РФ5.

Для поділу області ПЗП та ОЗП необхідно розшифрувати верхні розряди адреси. Після подачі сигналу скидання на процесор лічильник команд приймає значення 0, тобто виконання програми починається з адреси 0.

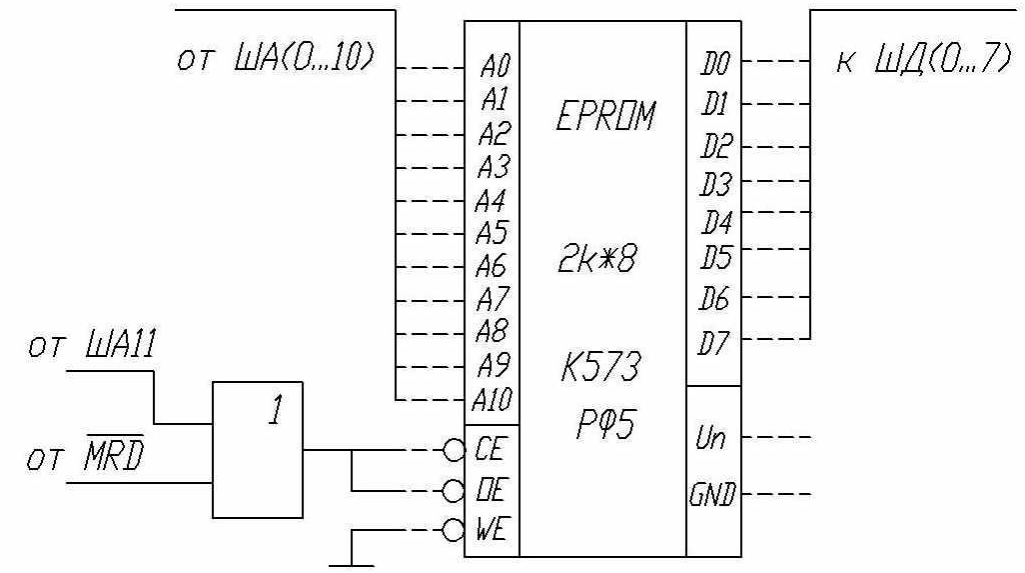

Рисунок 5.2 - Функціональна схема блоку ПЗП

Отже, область ПЗП, в якій зберігається код програми, повинна починатися з адреси 0 [12]. Тоді верхній адреса ПЗП 2 Кбайт буде дорівнює 2047 (07ffH), що відповідає бінарного 0000011111111111. Область ОЗП починається з наступних адрес. Нижній адреса ОЗУ в цьому випадку 2048 (0800H), тобто 0000100000000000. Верхня межа в 2 Кбайт відповідає адресі 4095 (0fffH), тобто 0000111111111111. Як видно, для адресації до пам'яті використовуються тільки нижні 12 біт адреси A0-A11. При цьому біти A15-A12 приймають значення 0 як для ПЗП, так і для ОЗП, а біт A11 приймає значення 0 для ПЗП та 1 для ОЗП. Ця обставина й застосовується для побудови дешифратора, що розділяє області ПЗП та ОЗП. Також враховується, що при зверненні до пам'яті, ЦПМ встановлює в 0 сигнали MEMW або MEMR, звернення ПЗП можливо тільки при читанні даних, але не при їх запису. Сигнали з дешифратора мають активний рівень 0 і підключені до входів вибірки кристала CS та переведення виходів у Z-стан OE мікросхем ОЗП та ПЗП. Висновки мікросхем об'єднані в загальну шину даних відповідними розрядами і підключаються до ЦПМ.

Таблиця 5.4 - Карта пам'яті

Тип ЗП	**ША**	**Номер розряду шини адреси**															
		15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
ПЗП 2Кб	0000h	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	07FFh	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1

ОЗП 2Кб	0800h	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
	0FFFh	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1

В якості проектованого ОЗП вибираємо статичний ОЗП К537РУ8.

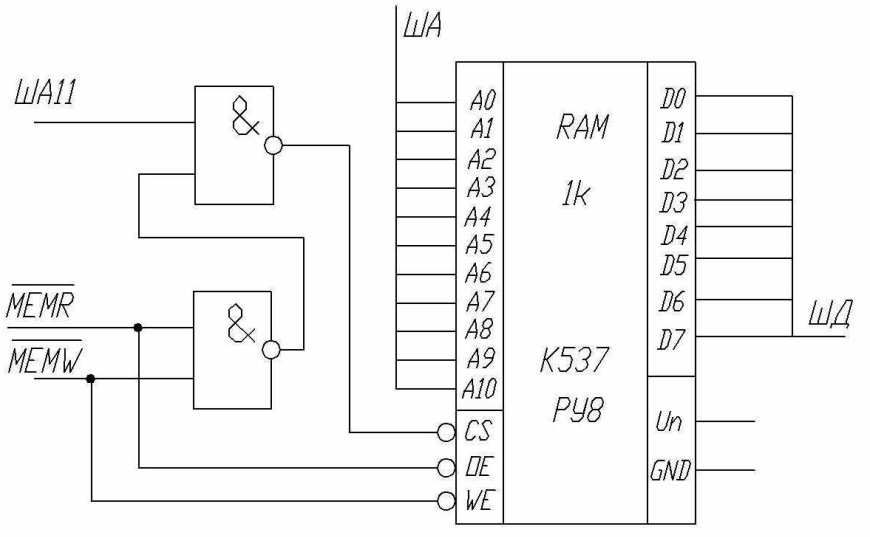

Рисунок 5.3 - Схема блоку ОЗП

Використання ОЗП статичного типу дозволяє вирішити завдання збереження даних у пам'яті. Для запису даних з входів D0-D4 в мікросхему необхідно на входах A0-A9 встановити потрібну адресу комірки пам'яті, подати на входи CS і WR напруга низького рівня. Для читання даних з пам'яті необхідно встановити адресу комірки, на вхід CS подати напругу низького рівня, а на вхід WR - високого.

Інтерфейс являє собою сукупність можливостей, способів та методів взаємодії двох систем (будь-яких, а не лише тих, що обов'язково є обчислювальними або інформаційними), пристроїв або програм для обміну інформацією між ними, певна їх характеристиками, характеристиками з'єднання, сигналів обміну й т. п.

Щоб управляти зовнішніми пристроями та забезпечити необхідну швидкість введення отриманого коду в пам'ять, потрібно застосувати контролер КР580ВВ55А, який дозволяє організовувати введення - виведення паралельної інформації різного формату. До його складу входять три восьмирозрядних порти введення / виведення РА, РВ, РС [12].

БІС КР580ВВ55 має у своєму складі входи - виходи для різних підключень до інших функціональних блоків.

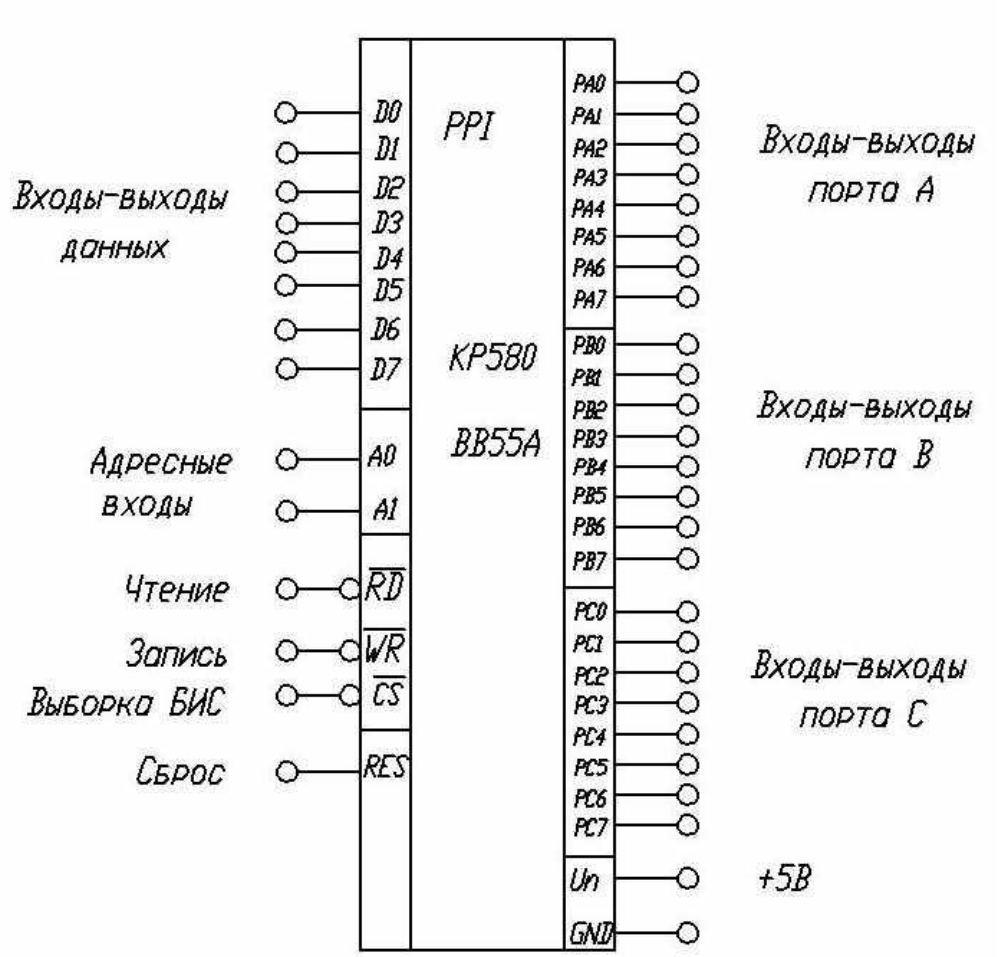

Рисунок 5.4 - Функціональне позначення і призначення виводів БІС КР580ВВ55А

Призначення виводів даної мікросхеми:

1) Адресні входи A0 і A1 задають адреса поточного порту, тобто для РА – 00, РВ - 01, РС - 10, регістр керуючого слова (РУС) - 11, а так само вони підключаються до 2-м молодшим бітам адресної шини.

2) Входи шини даних - D0 .. D7.

3) Виводи портів РА, РВ, РС - РА7..РА0, РВ7..РВ0, РС7..РС0.

4) Вивід читання - RD. Нульовий рівень означає, що процесор читає дані з шини даних, яка в даний момент підключена до порту (РА, РВ, РС) залежно від

адреси, що визначається виводами A1, A0. Підключається до виводу системного контролера IOR.

5) Вивід запис - WR. Нульовий рівень означає, що процесор видав дані на шину даних, підключену в даний момент до порту (PA, PB, PC) залежно від адреси, що визначається виводами A1, A0. Підключається до виводу системного контролера IOW.

6) Вивід вибірки мікросхеми - CS. Одиничний рівень переводить входи мікросхеми в Z-стан. При подачі сигналу з дешифратора ВУ, задається адреса порту.

Керуюче слово використовується для необхідної заданої роботи. Безпосередньо в регістрі керуючого слова міститься інформація, яка налаштовує порти на введення або виведення. Обмін з портами введення / виводу і регістром керуючого слова здійснюється через трехстабільну шину даних D7 ... D0 під управлінням сигналів, що подаються на входи вибірки CS, адреси A1, A0 та читання / запису [13].

Призначення виводів D7 ... D0:

D6-5: номер режиму порту PA в двійковій системі;

D4: 1 - введення PA, 0 - вивід PA;

D3: 1 - введення PC7 ... PC4, 0 - вивід PC7 ... PC4;

D2: номер режиму порту PB в двійковій системі;

D1: 1 - введення PB, 0 - вивід PB;

D0: 1 - введення PC3 ... PC0, 0 – вивід PC3 ... PC0;

D7: 1 - в режимі встановлення.

Порт A програмується на вивід даних (для управління входами аналогового комутатора). Порт B на введення даних з АЦП, PC0 ... PC3. PC4 ... PC7 - на цих виходах формується послідовно логічні одиниці, по фронту яких проводиться запис семисегментного коду у відповідний регістр.

За вихідними даними розрахунково-графічної роботи діапазон адрес для зовнішніх пристроїв таке: 32h-47h. У двійковому вигляді ці адреси будуть мати наступний вигляд:

0011 0010 - 32h

0100 0111 - 47h

Далі необхідно адресні входи мікросхеми КР580ВВ55 підключити до молодших розрядів молодшого або старшого біта шини адреси. Це можливо завдяки тому що команда висновку є двобайтового командою й міститься у другому байті адреса зовнішнього пристрою, а так як шина адреси

шістнадцятирозрядна, то значення молодшого та старшого байтів при цьому збігаються. Підключимо адресні входи до молодших розрядів старшого байта шини адреси (ША8, ША9).

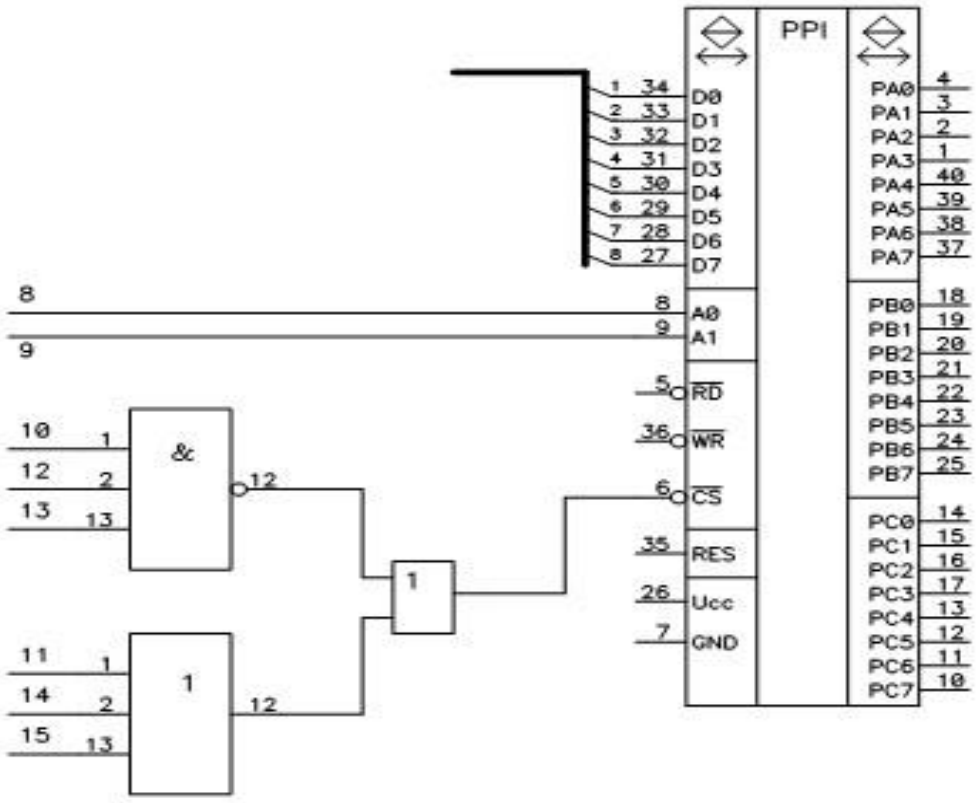

Рисунок 5.5 - Інтерфейсний блок

Адреси портів виберемо таким чином:

0011 0100 - PA

0011 0101 - PB

0011 0110 - PC

0011 0111 - РУС

Щоб уникнути постійного підключення зовнішніх пристроїв, коли розряди ША8 і ША9 приймають зазначені вище значення, потрібно застосувати дешифратор адреси. При його наявності можна виключити помилкові спрацьовування. Вихід дешифратора потрібно підключити на вхід CS мікросхеми КР580ВВ55А. Що б виключити помилкові підключення зовнішніх пристроїв, необхідно контролювати значення старших розрядів старшого байта шини адреси, а також сигнали читання і запису зовнішніх пристроїв [12].

RTL8019AS - інтегрований на кристалі контролер Ethernet, повністю відповідний стандарту 10BASE-T/100BASE-TX. Для зв'язку з хостом (мікроконтролером) він використовує паралельний інтерфейс SPI. Мікросхема практично не вимагає зовнішніх компонентів для роботи і підтримує кілька режимів відключення живлення.

Рисунок 5.6 – Загальний вигляд мікросхеми RTL8019AS

RTL8019AS інтегрує RTL8019A та 16 Кбайт SRAM в одній мікросхемі. Він призначений не тільки для забезпечення більш зручних функцій, але й для заощадження зусиль SRAM джерела та інвентарю.

Особливості:

- 100-контактний PQFP;
- 16 Кбайт SRAM;
- сумісність з Ethernet II і IEEE 802.3 10Base5, 10Base2, 10BaseT;
- підтримка UTP, AUI і BNC автовизначення;
- програмне забезпечення сумісне з NE2000 на обох 8 і 16-бітових слотах;
- підтримка дуплексного Ethernet. Функція подвійний смуги пропускання каналу;
- підтримує три рівні потужності;
- вбудована функція попередньої вибірки даних для підвищення продуктивності;
- підтримка автоматичного визначення полярності корекції 10BaseT;
- підтримка 8 ліній переривань.

На рис. 5.7 представимо спрощену функціональну схему блоку RTL8019AS з показаннями підключеними виходами для RJ-45, шини даних, управління.

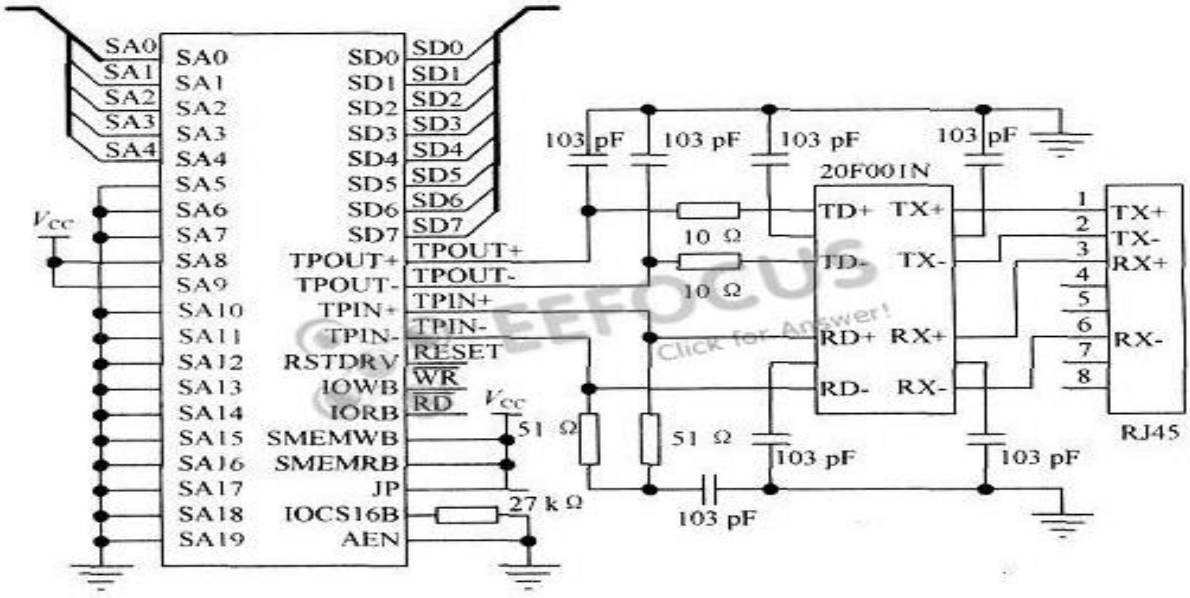

Рисунок 5.7 – Спрощена функціональна схема блоку RTL8019AS

На рис. 5.8 наведена функціональна схема блоку RTL8019AS.

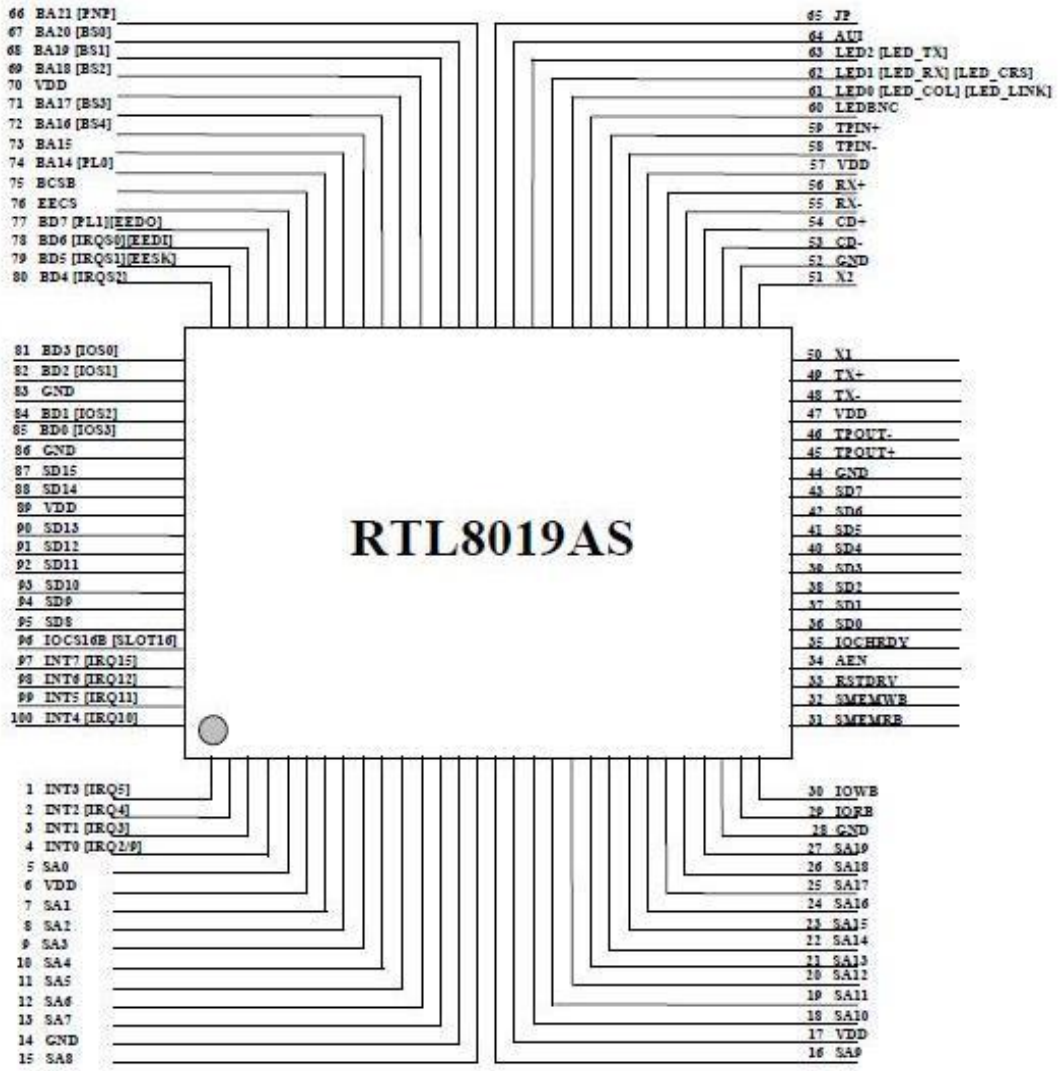

Рисунок 5.8 – Розташування вводів-виходів мікросхеми RTL8019AS

6 РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Програмований контроллер послідовного введення-виведення.

Фрагмент програми на асемблері для мікроконтроллера КР1821ВМ85, приведений нижче, представляє один з варіантів організації асинхронної передачі елементів масиву по послідовному каналу, використовуючи програмований контроллер послідовного введення-виведення КР1821ВМ85А.

Для введення в контроллер послідовного введення-виведення інструкцій та виведення даних використовуються символічні адреси INSTR і DATA, відповідно. Ідентифікатор N означає число елементів масиву даних, а ADDR - адреса початку буфера даних в пам'яті. При виникненні помилки парності відбувається звернення до підпрограми обробки помилки, розташованої за адресою ERR (у цьому фрагменті відсутній).

```
Мітка – Мнемокод - Коментар
BEGIN  DI ;Заборона переривання
MVI A,40H ;Запис інструкції програмного скидання
        OUT INSTR
        MVI A,7DH       ;Запис інструкції режиму
        OUT INSTR
        MVI A,31H ;Запис інструкції команди передачі
        OUT INSTR
        MVI B,N     ;Установка лічильника масиву даних
        LXI H,ADDR      ;Завантаження початкової адреси масиву
ENTR:       MOV A,M  ;Передача елементу масиву в акумулятор
        OUT DATA        ;Запис елементу масиву в УСАПП
WAIT:       IN INSTR   ;Слово стану УСАПП

        MOV C,A   ;Зберігання  слова стану
        ANI 08        ;Виділення біта помилки парності

CNZ ERR    ;Якщо помилка, то на програму обробки
        MOV A,C    ;Відновлення слова стану
        RAR  ;Контроль готовності передавача
        JNC WAIT  ;Якщо  не готовий, то повтор
        DCR B        ;Зміна лічильника елементів масиву
```

```
        JZ EXIT      ;Якщо все, то вихід з програми
        INX H        ;Наступний елемент масиву
        JMP ENTR ;Повторення  циклу  передачі
EXIT:       MVI A,38H ;Запис інструкції команди кінця передачі
        OUT INSTR
        EI      ;Дозвіл преривання
```

7 ТЕХНІКО-ЕКОНОМІЧНА ЧАСТИНА

7.1 Оцінка ефективності інформаційних систем

Останнім часом особливу роль для організації відіграє ефективне використання існуючих у неї інформаційних ресурсів. У цьому випадку ключове значення отримує інформаційна інфраструктура організації, в якій зазвичай виділяють технічне, програмне та організаційне забезпечення.

Технічне забезпечення включає в себе використовувані в організації обчислювальні машини, обчислювальні мережі і периферійне устаткування. Процес вибору того чи іншого технічного забезпечення залежно від потреби організації досить формалізований і може бути вирішене силами самої організації при консультаціях з постачальниками техніки, а також через замовлення у відповідній проектній організації [15].

У той же час, питання вибору програмного забезпечення до цих пір не мають подібної опрацювання. В основному це пов'язано з тим, що такі дослідження проводилися або компаніями, що випускають програмні продукти, у тому числі з метою реклами своєї продукції, або прихильниками вільного програмного забезпечення (ПЗ), які також зацікавлені в просуванні конкретних продуктів. Відповідно, незалежного всебічного дослідження проведено не було. Оскільки ефективне використання ПЗ є визначальним фактором використання IT-інфраструктури, то завдання вибору та оцінки ефективності програмного забезпечення в залежності від особливостей конкретної організації є актуальною. Більше того, без вирішення цього завдання неможливо створити ефективне організаційне забезпечення IT-інфраструктури, так як практично не існує фахівців, одночасно володіють професійними навичками управління вільним ПЗ різних виробників. Навіть якщо такий фахівець є, утримувати його нерентабельно внаслідок досить високої заробітної плати [11, 15].

Однією з причин відсутності універсальної методики вибору ПЗ є велика різноманітність у формах, структурах, завданнях існуючих організацій, кожна з них по-своєму унікальна, що ускладнює формалізацію даної задачі. При цьому є певний сегмент, на який унікальність організації практично не робить ніякого впливу, - це общесистемное та офісне програмне забезпечення. Для даного сегмента можна визначити обмежену кількість типів організацій, що дозволяє спростити методику вибору ПЗ. Для визначення типу організації в першу чергу

необхідно виявити її основні характеристики (критерії). Проведене дослідження показало, що до таких критеріїв належать [6]:

- кількість робочих місць (робочих станцій);
- наявність обчислювальної мережі;
- кількість і тип використовуваних серверів;
- наявність виходу в Інтернет (передбачається, що виходи в Інтернет є у всіх, а особливість даної характеристики визначається способом управління доступом);
- наявність і тип територіальної розподіленості: в межах одного приміщення, будівлі, декількох будівель, одного міста, кількох районів (необхідність віддаленого доступу);
- наявність функціональної ієрархічної організаційної структури, що накладає певні особливості на управління IT-інфраструктурою, а також на розподіл потоків даних в межах обчислювальної мережі.

Кожен тип мережі організації має свої особливості в побудові IT-інфраструктури, але з точки зору конфігурації загальносистемного та офісного ПЗ, всі організації схожі. Виняток становлять лише великі організації, кожна з яких унікальна. Однак, самий для них ефективний вибір офісних систем і загальносистемного ПЗ не представляє особливих складнощів, оскільки підприємству достатньо оголосити тендер з грамотно сформульованими умовами придбання та підтримки ПЗ. Так як сума контракту досить велика, то велика кількість компаній, що займаються ПЗ, буде пропонувати свої рішення, й підприємству залишається тільки вибрати серед них оптимальне для себе ПЗ [12].

Більше проблем виникає у малих та середніх підприємств, які в більшості своїй змушені самостійно вирішувати проблеми вибору загальносистемного та офісного ПЗ, орієнтуючись на рекламні проспекти вендорів. Але так як їх структура є типовою, то існує можливість визначити типовий функціонал їхнього ПЗ.

Як раніше було зазначено, питання вибору ПЗ нерозривно пов'язані з побудовою організаційного забезпечення IT-інфраструктури, для чого була сформована опис типів користувачів. У комп'ютерному середовищі будь-якої організації користувачі зазвичай діляться на кілька категорій. Умовно можна виділити такі типи:

- фахівець базових знань - основну роботу виконує за допомогою офісних програм, сюди можна віднести Web-браузер, поштовий клієнт і стандартний

набір офісних додатків: текстовий процесор, електронні таблиці, презентації, програма для малювання і в деяких випадках СУБД;

- досвідчений фахівець - просунуті користувачі, що володіють глибокими знаннями офісних додатків; цього типу користувачів властиво також працювати з програмними засобами, що підвищують ефективність роботи. До цього типу користувачів можна віднести управлінські кадри підприємства;

- технічний працівник - в цю групу можна віднести системних і мережевих адміністраторів. Зазвичай використовують той же ПО, що і фахівці базових знань, але до цього списку додаються спеціалізовані засоби розробки, моніторингу, а також засоби проектування.

У невеликих організаціях подібний поділ може не мати особливої важливості, проте для великих організаціях, де присутня вузька спеціалізація діяльності співробітників, важливо визначити число і тип користувачів, це в свою чергу дозволить визначити кількість і тип використовуваного ПЗ [12, 16].

На основі характеристик організації та типів користувачів можна припустити, яке ПЗ повною мірою задовольняє функціональним потребам підприємств різних типів.

Організація з однієї ЕОМ.

Для організації з однієї ЕОМ відсутня функціональна ієрархічність, а користувача, як правило, можна віднести до категорії «Спеціаліст базових знань», а також «Просунутий користувач», який може виконувати роль технічного спеціаліста в найпростіших випадках. В організаціях подібного роду перелік загальносистемного ПЗ зводиться до вибору операційної системи, а прикладного - до вибору офісного пакету.

За великим рахунком, вбудованих засобів ОС цілком вистачить для вирішення простих повсякденних завдань: перегляду електронної пошти, Web-серфінгу, створення простих документів, однак якщо виникне необхідність створення документа зі складним форматуванням або створити електронну таблицю, то засобами вбудованих в ОС програм не обійтися, що призводить до необхідності використання офісного пакету [15].

Процес вибору ПЗ в більшості випадків обумовлюється особистими уподобаннями, варто також зазначити, що більшість виробників комп'ютерів постачають свою продукцію з встановленою ОС.

Мікропідприємства.

Даний тип організації, як й підприємство з однієї ЕОМ, не має функціональної ієрархічної структури, користувачів також можна віднести до

типу «Спеціаліст базових знань» та «Просунутий користувач»; як й у попередньому випадку, цей тип користувача може виконувати роль технічного персоналу у вирішенні найпростіших проблем. Перелік необхідного ПЗ зводиться до наявності настільної ОС та офісного пакету [16, 17].

Відмінною особливістю мікропідприємства є наявність тимчасової локальної обчислювальної мережі (ЛОМ) та загального доступу до Інтернет, однак ці особливості ніяк не впливають на вибір загальносистемного та прикладного ПЗ. Як правило, організація ЛОМ в межах одного приміщення не вимагає ніяких програмних засобів, достатньо придбати комутатор і прокласти мережеві проводи, а для загального доступу в Інтернет використовується апаратний маршрутизатор або вбудовані засоби самої ОС.

Варто відзначити, що для забезпечення максимальної сумісності доцільно, щоб общесистемное ПЗ належало до одного сімейства ОС.

Мале підприємство.

Основну частину працівників малих підприємств можна віднести до типу «Спеціаліст базових знань». Однак, відмітними особливостями організацій даного типу, в порівнянні з розглянутими вище, є наявність функціональної ієрархічності, хоча і слабко, що призводить до необхідності управління доступом до локальних ресурсів ЛОМ підприємства. Це передбачає наявність власних або запрошених (аутсорсинг) технічних фахівців [17].

На підприємствах даного класу зазвичай використовується спеціалізоване програмне забезпечення, наприклад пакети бухгалтерського обліку, що з одного боку увазі створення файлових серверів з відповідним ПЗ, а з іншого - накладає певні обмеження на можливість вибору операційних систем. Подібні обмеження існують й для підприємств більшого масштабу. Все це необхідно враховувати при розробці IT-інфраструктури.

Структура ЛОМ та організація загального доступу до Інтернет повністю ідентичні для таких підприємств.

У перелік використовуваного ПЗ входять: серверна ОС, настільна ОС, офісний пакет, спеціалізовані засоби розробки та моніторингу.

Невелике середнє підприємство.

Для IT-інфраструктури даного виду організації доцільно використовувати клієнт-серверну архітектуру ЛОМ. Це пов'язано з тим, що адміністрування тимчасової мережі з великим (більше 20) числом клієнтів вимагає серйозних тимчасових витрат, що робить дану інфраструктуру неефективною.

Клієнт-серверна архітектура дозволить ввести централізоване управління правами користувачів через створення домену. Оскільки в організації даного типу присутній функціональна ієрархічність, створення в домені різних груп користувачів з різними правами, виходячи з їх функціональних обов'язків, дозволить оперативно управляти доступом до інформації. Але створення групових політик на контролері домену - це лише частина рішення, основна проблема полягає в розподілі прав доступу до локальних ресурсів комп'ютера користувача. Все сказане вище припускає використання спеціалізованого серверного ПО, а також наявність відповідних технічних фахівців [15].

Виходячи з масштабу підприємства і наявності функціональної ієрархічності може виникнути ситуація групової роботи кількох людей над одним проектом, що в свою чергу призводить до необхідності створення електронного архіву [15].

Організація доступу до мережі Інтернет теж має свої особливості у порівнянні з підприємствами меншого масштабу. З'являється необхідність централізовано керувати авторизацією для обмеження доступу певних користувачів до деяких ресурсів, а кешування запитів дозволяє знизити витрати на трафік. Такі завдання не можуть бути вирішені простими маршрутизаторами, а апаратні рішення, що відповідають потребам організації, коштують досить дорого. Використання програмного проксі-сервера вирішує цю проблему. У випадку з проксі-сервером, так само як і з контролером домену, передбачається використання спеціалізованого ПЗ і кваліфікованого технічного персоналу.

У підсумку в перелік необхідного ПЗ можна внести:

- серверну ОС;
- спеціалізоване серверне ПЗ:
- проксі-сервер (він може входити до складу ОС або поставлятися стороннім виробником);
- ПЗ для створення електронного архіву;
- контролер домену (аналогічно проксі-серверу);
- спеціалізовані засоби моніторингу;
- настільну ОС;
- офісний пакет.

Середнє підприємство.

Незважаючи на схожість основних показників даного типу підприємств з невеликими середніми, IT-інфраструктура перших має ряд істотних відмінностей.

По-перше, при побудові IT-інфраструктури необхідно враховувати територіальну розподіленість, що призводить до необхідності об'єднання будівель в мережу, при цьому з'являється гостра необхідність у захисті переданої інформації. Для цього необхідно використовувати спеціалізоване ПЗ [15].

По-друге, присутність декількох потоків даних передбачає наявність декількох підмереж з власними серверами і службами, що веде до використання шлюзів і складною маршрутизації, ускладнює конфігурація мережі. У ряді випадків це також передбачає виділення декількох доменів всередині організації.

По-третє, якщо в попередньому типі підприємства для організації групової роботи можна було обійтися лише електронним архівом, то більша кількість користувачів вимагає ускладнення системи контролю за їх роботою, що дозволяє говорити вже про необхідність впровадження системи електронного документообігу (СЕД). Як правило, для СЕД потрібно внутрішній поштовий сервер, і в даному випадку його використання виправдане. Щоб обмежити кількість спаму і убезпечити себе від шкідливого коду у вхідній пошті, необхідно використовувати спеціальне ПЗ для захисту поштового сервера [15].

Відповідно до переліку ПЗ для середнього підприємства додаються система криптозахисту (за рішенням підприємства рівень секретності встановлює саме підприємство), спам-фільтр і антивірусне ПЗ для поштового сервера, а також СЕД.

Перш ніж розраховувати ефективність використання програмного забезпечення, необхідно врахувати потреби в ПЗ конкретної організації.

Особливість загальносистемного і офісного ПЗ полягає в тому, що існує невелика кількість видів організацій, які визначають ПЗ та їх вибір.

Визначено основні види організацій та їх характеристики, для кожного виду визначено перелік необхідного ПЗ.

Однією з проблем визначення ефективності загальносистемного та офісного програмного забезпечення (ПЗ) є вибір методики оцінки. У класичній літературі, присвяченій питанню оцінки ефективності, вона розраховується за формулою [17]:

Ефективність = ефект/витрати.

Витрати - сукупні витрати на придбання, встановлення та конфігурування, супровід і підтримку, а також витрати пов'язані з простоєм устаткування під час технічне обслуговування або усунення несправностей.

Ефект - ефект, що досягається при впровадженні ПЗ. Однак, через специфіку використання загальносистемного і офісного ПЗ визначити прямий

ефект від їх впровадження (в тимчасових або фінансових показниках) важко. Внаслідок цього виникає завдання вибору методу оцінки, усю множину яких можна поділити на наступні види [17].

Витратні методи. Оцінка проводиться не на основі вимірювання кінцевого продукту або результату, а на основі витрачених ресурсів або сил.

Методи оцінки прямого результату. Методика оцінює прямий вимірний результат, наприклад, зниження вартості володіння, підвищення функціональності системи, зниження трудовитрат або поява побічного продукту основного трудопроізводства.

Методи, засновані на оцінці ідеальності процесу. Такі методики базуються на статичних або динамічних порівняльних алгоритмах. Базовим показником вибирається об'єкт розглянутої системи, тоді ідеальною вважається інформаційна система з кращими для галузі показниками витрат на одиницю виходу. Популярні також підходи на базі порівняння з альтернативним рішенням.

Витратні методи оцінки.

Котловий метод. Метод заснований на визначенні співвідношення обсягів вкладень в програмне забезпечення, включаючи впровадження і супровід, з розмірами підприємства і напрямами його бізнесу. Часто дане співвідношення задається у вигляді максимально-допустимого обсягу вкладень по відношенню до річного обороту компанії, наприклад не більше 1% для невеликих компаній і не більше 3% для великих.

Метод функціональної точки. Даний метод використовується для приблизної оцінки вартості створення і впровадження інформаційної системи (ІС) в залежності від вимог користувача. Кожне таке вимога оцінюється як за шкалою труднощі (легкі, середні та важкі), так й за шкалою важливості для користувача. Вимоги представляються у вигляді вектора (функціональної точки) в багатовимірному просторі. Далі відповідно до гіпотезою «компактності» передбачається, що чим ближче функціональні точки проектів один до одного в просторі вимог, тим їх параметри, включаючи й ефективність, більш схожі. Відповідно в базі раніше впроваджених проектів знаходиться такий, чия функціональна точка найближче знаходиться до проектованої ІС, та передбачається, що їх ефективності максимально близькі [14].

7.2 Розрахунок собівартості та оптової ціни пристрою, що розроблюється

7.2.1 Розрахунок собівартості. В процесі виробництва будь-якого виробу споживаються різні матеріали, комплектуючі вироби, використовуються різні види обладнання та інструменти, проводиться велика кількість технологічних операцій [18]. У зв'язку з цим для обліку фактичних витрат на виробництво та для обґрунтування собівартості необхідна певна класифікація цих витрат. Для розрахунку собівартості одиниці певного виду продукції, що випускається, застосовується класифікація за калькуляційними статтями витрат. У плануванні та в обліку собівартості продукції застосовується наступне типове групування за статтями калькуляції:

- основна заробітна плата;
- додаткова заробітна плата;
- відрахування від заробітної плати;
- матеріали та комплектуючі;
- витрати на утримання та експлуатацію обладнання;
- виробничі витрати;
- адміністративні витрати;
- позавиробничі витрати (комерційні витрати) [18].

Групування витрат по калькуляційних статтях витрат дозволяє визначити рівень собівартості виробу, а відповідно й рівень його ціни. Вона характеризує місце виникнення витрат та їх цільове призначення.

Вихідними даними для складання калькуляції собівартості на проектований пристрій є стаття калькуляції на покупні та комплектуючі вироби. Необхідно врахувати вартість напівфабрикатів, що йдуть на виготовлення друкованої плати.

Дані по цій статті витрат приведені в таблиці 7.1.

Таблиця 7.1 - Дані на покупні та комплектуючі вироби

Найменування комплектуючих	**Кількість**	**Ціна однієї одиниці,(грн.)**	**Сума на один виріб (грн.)**
1	**2**	**3**	**4**
Мікросхеми			
КР1821ВМ85А	1	110	110
К1533ЛА3	1	15	15

КР580ВА86	1	10	10
К537РУ8	1	20	20
КР580ВВ55А	2	25	50
RTL8019AS	4	145	580
КР580ИР82	2	20	40
К1533ЛИ1	1	10	10
К573РФ5	1	60	60
MAXRS232	4	15	60
К555НП11	1	15	15
К555ЛИ1	1	10	10
Конденсатори			
К10-9 – 20В – 100 нФ ±20%.	2	5	10
К53-7– 15В – 150 мкФ ±20%	8	10	80
К53-16 – 15В – 10 мкФ±20%	8	10	80
М47-35-0,1мФ±5%	2	5	10
К50-20-16В – 10 мкФ±20%	12	10	120
М47-17-100мФ – 20В ± 5%	20	10	200

Продовження таблиці 7.1

1	**2**	**3**	**4**
Резистори			
С2 – 29В – 0.125 – 270 Ом	2	1	2
С2 – 29В – 0.125 – 100 Ом	21	1	21
С2 – 29В – 1кОм	4	1	4
Резонатор			
КР 169-12 МГц	1	10	10
Витратні матеріали			
Гетінакс(двосторонній)	100 $см^2$	30	30
Припой, флюс і др.		10	10
Загальна вартість, (грн.)			**1557**

Витрати на основну заробітну плату (Зо):

$$З_о = Т * Г * К * А, \quad (7.1)$$

де Т – сумарна трудомісткість розробки продукту (годин), яка визначається експертним шляхом виходячи з фактично витраченого часу на виробництво та налаштування продукту, Т = 8 (годин);

Г – середня годинна тарифна ставка одного робітника задіяного у виробництві продукту, грн. / год, Г = 60 грн. / год;

К – коефіцієнт трудової участі (розрядності), К = 1,3;

А – кількість працівників задіяних у виробництві, А = 2.

Тоді

$$З_о = Т * Г * К * А = 8*60*1,3*2 = 1248 \text{ (грн.)}.$$

Додаткова заробітна плата (10 – 30% від $З_о$):

$$З_д = З_о * К_д/100, \quad (7.2)$$

де $К_д$ – відсоток додаткової заробітної плати, $К_д$ = 10%.

$$З_д = З_о * К_д/100 = 1248*(10\%/100) = 124,80 \text{ (грн.)}.$$

Нарахування на заробітну плату – єдиний соціальний внесок у розмірі 22%.

$$Н_в = (З_о + З_д) * 22/100. \quad (7.3)$$

$$Н_в = (1248+124,8) * 22/100 = 302,02 \text{ (грн.)}.$$

Витрати на утримання та експлуатацію обладнання.

Оренда машинного часу ($О_м$):

$$О_м = М_в * Ч_м, \quad (7.4)$$

де $М_в$ – величина машинного часу, необхідного для розробки та налагодження продукту, годин, $М_в$ = 1дн * 8ч = 8 годин;

$Ч_м$ – вартість оренди машинного часу, грн. / год:

$$Ч_м = Ц_{еом} / Н_р * 259 * 8, \quad (7.5)$$

де $Ц_{еом}$- ціна обладнання, задіяного при виробництві виробу,

$Ц_{еом}$ = 35000 грн;

$Н_р$ – термін ефективної роботи, $Н_р$ = 5;

259 – кількість робочих днів;

8 – тривалість зміни.

$$Ч_м = 35000/5*259*8 = 3,40 \text{ (грн./ч).}$$

Тоді

$$О_м = М_в * Ч_м = 8*3,4 = 27,20 \text{ (грн.).} \quad (7.6)$$

Загальновиробничі витрати. Являють собою витрати, що пов'язані з управлінням підрозділом, витрати на службові відрядження співробітників підрозділу, амортизаційні відрахування від вартості основних фондів загальноцехового призначення і т.д.

Загальновиробничі витрати ($В_{зв}$) визначаються в розмірі 130-250% від основної заробітної плати.

$$В_{зв} = З_о * \% В_{зв} = 1248 * 1,3 = 1622,40 \text{ (грн.).} \quad (7.7)$$

Визначимо виробничу собівартість:

$$В_с = З_о + З_д + Н_в + М + О_м + В_{зв} =$$
$$= 1248 + 124,80 + 302,02 + 1557 + 27,20 + 1622,40 = 4881,42 \text{ (грн.).} \quad (7.8)$$

Адміністративні витрати можуть містити:

- витрати, пов'язані з управлінням підприємством;
- витрати на службові відрядження адміністрації підприємства;
- витрати на пожежну і сторожову охорону;

- витрати, пов'язані з підготовкою (навчанням) і перепідготовкою кадрів;
- витрати на перевезення працівників до місця роботи і назад;
- витрати на оплату відсотків за фінансові кредити, а також відсотків за товарні і комерційні кредити;
- витрати, пов'язані з оплатою відсотків за користування матеріальними цінностями, взятими в оренду (лізинг);
- витрати, пов'язані з оплатою послуг комерційних банків та інших кредитно-фінансових підприємств;
- податки, відрахування.

Адміністративні витрати ($В_а$) визначаються в розмірі 140 - 200% від основної заробітної плати.

$$В_а = З_о * \% В_а = 1248 * 1,4 = 1747,20 \text{ (грн.)}. \quad (7.9)$$

Витрати на збут ($В_з$). Включають витрати на рекламу і предреализационная підготовку пристрою. Орієнтовно ці витрати визначаються в розмірі 5 - 10% від виробничої собівартості.

Тоді

$$В_з = В_с * (5 – 10)\% = 4881,42 * 0,05 = 244,07 \text{ (грн.)}. \quad (7.10)$$

Повна собівартість пристрою (С):

$$С = В_с + В_а + В_з . \quad (7.11)$$

$$С = 4881,42 + 1747,20 + 244,07 = 6872,70 \text{ (грн.)}.$$

Калькуляція собівартості виробу зводиться в таблицю 7.2.

Таблиця7.2 - Калькуляція собівартості виробу, що розробляється

Найменування статей калькуляції	Величина, грн.
1. Основна заробітна плата	1248
2. Додаткова заробітна плата	124,80
3. Нарахування на заробітну плату	302,02

4. Матеріали та комплектуючі	1557
5. Оренда машинного часу	27,20
6. Загальновиробничі витрати	1622,40
7. Адміністративні витрати	1747,20
8. Витрати на збут	244,07
Разом повна собівартість	6872,70

7.2.2 Розрахунок ціни пристрою. Розрахунок оптової ціни виробу проведемо за схемою «собівартість плюс прибуток»:

$$Ц_{опт} = С + П, \quad (7.12)$$

де С – собівартість пристрою;

П – величина прибутку.

Прибуток визначається виходячи з нормативу рентабельності виробництва продукції:

$$R = (П / С) * 100\%, \quad (7.13)$$

де R - рентабельність продукції (продукту), приймається в розмірі до 35%.

R = 10%.

Тоді оптова ціна:

$$Ц_{опт} = С + (R * С / 100) = 6872,70 +0,1*6872,70 = 7560 \text{ (грн.)}. \quad (7.14)$$

Визначимо роздрібну ціну розробленого виробу:

$$Ц_{розн} = Ц_{опт} * 1,2 = 7560 * 1,2 = 9072 \text{ (грн.)}, \quad (7.15)$$

де 20% ПДВ.

Позитивні сторони даної методики полягають в її простоті, комплексної очевидності такої функції ціни як відшкодування витрат на виробництво та забезпечення прибутковості від створення та реалізації пристрою. Недолік даної методики полягає в тому, що вона недостатньо враховує ринкові чинники ціноутворення й, перш за все, попит. Однак, у реальній перехідній економіці

існують ситуації, коли підприємствам доцільно її застосовувати: в умовах відсутності конкуренції (монополії), при обмеженні рентабельності продукції з боку держави, виконанні одноразових замовлень, при виготовленні оригінальної продукції.

Необхідно відзначити, що для встановлення реальної ціни, яка б відповідала умовам існуючого ринку, необхідні відповідні маркетингові дослідження.

ВИСНОВКИ

У ході виконання кваліфікаційної магістерської роботи були розглянуті проблеми інформаційної безпеки бездротових мереж, основні підходи до вирішення цих проблем, а також був проведений аналіз існуючих методів та алгоритмів виявлення мережевих атак. Досліджено різноманітні методи захисту інформаційних каналів від несанкціонованого доступу до сегментів мережі, які доречно реалізувати в маршрутизаторах.

Показана можливість вбудовування в маршрутизуючий сервіс алгоритмів мультиплексування. Розроблені математична модель, схема-алгоритму та структурна схема «маршрутизуючого сервісу» на основі динамічної маршрутизації.

Розроблено структурну схему та блок-схему алгоритма роботи маршрутизатора на базі вибраного метода підвищення рівня захисту від несанкціонованого доступу в різних сегментах мережі з різноманітними технологіями передачі даних.

Розроблено функціональну та принципову схеми пристрою.

Розглянуті питання економіки, розраховано показники собівартості та ціни пристрою.

СПИСОК ЛІТЕРАТУРИ

1. Тарбаєв С.І. Проектування інфокомунікаційних мереж. Навчальний посібник / С.І. Тарбаєв, К.О. Домрачева, В.Ф. Заїка, М.П. Трембовецький. – Київ: ННІТІ ДУТ, 2019. – 186 с.
2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник/ В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2016. – 992 с.
3. Бережна О.В. Про особливості шифрування в розподілених системах відображення числових даних / О.В. Бережна, О.А. Борисенко, М.М. Яковлев, О.О. Рахматоль, М.С. Фурса // Фізика, електроніка, електротехніка (ФЕЕ-2020). Матеріали та програма науково-технічної конференції. – Суми: СумДУ, 2019. - С. 90.
4. Куроуз Ф. Джеймс. Компьютерные сети: Нисходящий подход / Джеймс Куроуз, Кит Росс. – 6-е изд. – Москва: Издательство «Э», 2016.– 912 с.
5. IEEE 802.11ac-2013. IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz. IEEE Standards Association, 2013.
6. http://www.ua5.org/lan// 2018 / 12 /124-lokaln-merezh.html, 2018.
7. http:// easy-code.com.ua / 2016 / 08 / ethernet-v-promislovosti-lokalni-merezhi, 2016.
8. https://www.quora.com/What-is-network-technology/ Dec 20 / 2018.
9. Autonomic Systems: Concept for Self-Managing IT Infrastructure White Paper. Fujitsu Siemens Computers, March 2003.
10. https://infotel.ua/ua // 2017 / 12 / local-aria-network-data-transfering, 2017.
11. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.
12. http://www.navgeocom.ru/infra/hard/ leica_ 1200gg/ar25.htm, 2016.
13. Noulas A.K., Kröse B.J.A. Deep Belief Networks for dimensionality reduction. Proceedings of the twentieth Belgian-Dutch Conference on Artificial Intelligence. University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Enschede, 2008. – Pp. 185–191.

14. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.
15. Антипов И.Е., Василенко Т.А., Михеев И.В. Разработка модели Wi-Fi сети с целью предотвращения вторжений // Восточно-Европейский журнал передовых технологий. – 2014. – № 1(9). – С. 4-8. [Электронный ресурс]. - URL: http://nbuv.gov.ua/j-pdf/Vejpte_2014_1(9)__2.pdf.
16. Клочкова Е.Н. Экономика предприятия: учебник / Е.Н. Клочкова, В.И. Кузнецов, Т.Е. Платонова; под редакцией Е.Н. Клочковой. – М.: Издательство Юрайт, 2019. – 447 с.
17. Тарасюк М. Бюджетне планування в Україні // Вісник КНТЕУ. – 2018. – № 2. – С. 19-31.
18. Типовое положение по планированию, учету и калькулированию себестоимости продукции. Утверждено КМ Украины от 26 апреля 1996 №473//Бізнес.-№32-35.