Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії
Кафедра захисту інформації

Пояснювальна записка

до магістерської кваліфікаційної роботи

на тему «Система моніторингу безпеки розумного будинку»
08-20.МКР.008.00.000 ПЗ

Виконав: групи 1 БС-18 м
спеціальність 125 – Кібербезпека
ОПП Безпека інформаційних і
комунікаційних систем

_____Круговий В. В.

Керівник к.т.н., доц., доц.. каф. ЗІ

_____Войтович О. П.

Рецензент к. т. н., доц., доц. каф. ОТ

_____Крупельницький Л.В.

Вінниця - 2019 року

АНОТАЦІЯ

У магістерській кваліфікаційній роботі розроблено метод для моніторингу безпеки розумного будинку, який виконує перевірку пристрою по цифровому підпису. Проаналізовано роботу систем моніторингу, Wi-Fi мережі, малоресурсних засобів шифрування. Система передбачає моніторинг підключених до Wi-Fi пристроїв. Для демонстрації роботи системи моніторингу розроблено програмний засіб. В економічній частині оцінено витрати на розробку.

ABSTRACT

Master’s tesis is devoted to the development monitoring method for the safety of a smart house, which attach a digital signature. Analyzed the operation of monitoring systems, Wi-Fi measures, low-resource encryption. Method satisfy monitoring and connection to Wi-Fi add-ons The software was developed. The economic section estimates development costs.

Вінницький національний технічний університет

Факультет Інформаційних технологій та комп'ютерної інженерії
Кафедра Захисту інформації
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки 125 – Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри ЗІ, д.т.н., проф.

_____В.А.Лужецький

_____ _____ 2019 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІНУ РОБОТУ СТУДЕНТУ

Круговому Владиславу Віталійовичу

1. Тема роботи: «Система моніторингу безпеки розумного будинку» керівник роботи: Войтович Олеся Петрівна, к.т.н., доц., доц. каф. ЗІ, затверджена наказом ректора ВНТУ від 02.10.2019 року №254.
2. Строк подання студентом роботи .12.2019 р.
3. Вихідні дані до роботи:
   - параметри для моніторингу: наявність пристроїв, помилки, запити;
   - наявність автентифікації пристроїв;
   - використання мало ресурсної криптографії;
4. Зміст розрахунково-пояснювальної: Вступ. Аналіз відомих методів. Розробка методу моніторингу мережі. Розробка програмного додатку. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Загальна схема децентралізованого розумного будинку, схема підписання даних, принцип роботи хешування, складові системи моніторингу, складові на стороні серверу та роутеру, алгоритм роботи програми.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Войтович О.П., к.т.н., доц., доц. каф. ЗІ		
2	Войтович О.П., к.т.н., доц., доц. каф. ЗІ		
3	Войтович О.П., к.т.н., доц., доц. каф. ЗІ		
4	Мацкевічус С. С., ст. викл. каф. ЕПВМ		

7. Дата видачі завдання 01 вересня 2019 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	**3.** Примітка
1	Аналіз завдання. Вступ	01.09.2019 – 04.09.2019	
2	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	05.09.2019 – 15.09.2019	
3	Науково-технічне обґрунтування	16.09.2019 – 22.09.2019	
4	Розробка технічного завдання	23.09.2019 – 29.09.2019	
5	Розробка рішень	30.09.2019 – 12.10.2019	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2019 – 10.11.2019	
7	Розробка розділу економічного обґрунтування доцільності розробки	11.11.2019 – 17.11.2019	
8	Аналіз виконання ТЗ, висновки	18.11.2019 – 24.11.2019	
9	Оформлення пояснювальної записки	25.11.2019 – 30.11.2019	
10	Попередній захист та доопрацювання МКР	28.11.2019 – 01.12.2019	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2019 – 10.12.2019	
12	Представлення МКР до захисту	11.12.2019 – 14.12.2019	
13	Захист МКР	16.12.2019 – 20.12.2019	

Студент_____Круговий В. В
(підпис)

Керівник роботи _____Войтович О. П.
(підпис)

Зміст

ВСТУП

Стрімкий розвиток «розумних» технологій робить надзвичайно актуальними питання, пов'язані з їхньою інформаційною безпекою. Так, директор ЦРУ Девід Петреус заявив, що дані з підключених до Інтернету побутових приладів можна використовувати для складання максимально докладного досьє на будь-яку людину.

Сьогодні до складу систем типу «розумний будинок» можуть входити системи спостереження, системи моніторингу (в тому числі здоров'я) і системи безпеки, до яких можна отримати віддалений доступ, через які можуть атакувати зловмисники[1].

Розумний будинок — це комплекс рішень для автоматизації повсякденних дій, який позбавить вас від рутини. Це і побутова техніка, і системи контролю всього, що відбувається в будинку. Через те, що всі елементи кола мають доступ в Інтернет, це робить їх уразливими до атак ззовні та всередині і наражає на небезпеку не тільки інформацію користувача, але також і його здоров'я. Все це змінює парадигму мислення, в якій мовиться: «Мій дім - моя фортеця»[2].

Вже зараз існують різні розробки, створені для вирішення проблеми безпеки систем «розумного будинку». Наприклад, стандарт Thread, або розробка CherryHome, проте ці рішення носять суто містцевий характер, і не вирішують проблему забезпечення кібербезпеки[3].

Актуальність роботи полягає у розробці системи моніторингу розумного будинку, яка б дозволяла виявляти не лише фізичні загрози, а й атаки, спрямовані безпосередньо на інфраструктуру розумного будинку.

Метою магістерської кваліфікаційної роботи є покращення системи безпеки “розумного будинку” шляхом розробки системи моніторингу, яка б дозволяла відстежувати активність пристроїв всередині екосистеми розумного будинку. Удосконалення існуючих систем моніторингу “розумного будинку” за рахунок врахування моделі загроз, що дозволяє покращити захищенність мережі, а також використання малоресурсної

криптографії для автентифікації пристроїв “розумного будинку”, що дозволяє виявити атаку та підміну. Для досягнення мети необхідно розв’язати такі задачі:

– проаналізувати предметну область;

– розробити структуру системи моніторингу «розумного будинку»

– обґрунтувати методи автентифікації пристроїв у системі «розумний будинок»;

– провести тестування розробленого засобу.

Новизна отриманих результатів полягає у використанні методів мало ресурсної криптографії для моніторингу розумних пристроїв у мережі.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз безпеки системи “розумний будинок”

З розвитком розумних пристроїв та інфраструктури однією з найбільш перспективних та бажаних технологій є система «розумний будинок». Згідно з розрахунками Strategy Analytics [4] (рис. 1), в світі з кожним роком прогнозується збільшення обсягу витрачених коштів на розробку систем “розумний будинок”. Все більше і більше коштів витрачаються на її побудову та поліпшення. Отже, відбувається поступовий перехід користувачів від декількох автоматичних процесів у будинку до тотальної автоматизації всіх приладів. Однак на фоні актуалізації динаміки розвитку систем «розумний будинок» мало уваги надається питанню кібербезпеки.

Рисунок 1.1 – Темпи росту витрачених коштів на системи типу “розумний будинок”

Аналіз використання технології «розумний будинок» необхідно починати з вивчення роботи периферійних пристроїв, програмних середовищ моніторингу, а також «розумних» мікропроцесорних систем управління технологічними процесами. Дана технологія значно спростила життя

користувачам та відкрила можливості, недоступні при використанні звичайного, не «розумного» будинку. Проте, далеко не всі користувачі знають, скільки небезпек приховують сучасні, розумні технології [5].

Компанія HP провела дослідження ринку інтелектуальних систем, в ході якого з'ясувала, що практично всі системи мають проблеми з безпекою. Перша проблема — недостатньо надійна перевірка справжності. Системи захисту, незважаючи на те, що володіли ресурсами хмарних технологій та мобільними інтерфейсами, не вимагали установки паролів достатньої довжини і складності. Також жодна з систем не блокувала обліковий запис після певного числа невдалих спроб введення пароля — виходить, що захист від перебору відсутній.

Ще одна проблема пов'язана з конфіденційністю. Всі системи збирали будь-які види персональної інформації: імена, адреси, номери телефонів і кредитних карт. Це викликає певне занепокоєння, оскільки створює загрозу крадіжки облікових даних. Варто також відзначити, що ключовою особливістю багатьох домашніх систем безпеки є використання відео, перегляд якого доступний через різні інтерфейси. Конфіденційність такої інформації також знаходиться під питанням.

Ще один ризик, якому піддаються всі без винятку власники «розумних будинків» — повне відключення системи при припиненні подачі електроенергії. Розумний будинок енергозалежний і інших варіантів його функціонування немає. Ситуація може бути досить небезпечною, якщо відключення сталося у відсутності господаря, коли в будинку знаходяться діти або люди похилого віку. Є тільки один варіант вирішення проблеми — монтаж додаткового джерела живлення. Мова йде про монтаж міні-електростанції будь-якого типу. Кращим варіантом буде замість генератора запустити електростанцію альтернативного типу, що працює на сонячній або вітровій енергетиці.

Нарешті, останньою проблемою експерти назвали відсутність шифрування при передачі даних. Хоча у всіх системах реалізовані механізми

шифрування на транспортному рівні, такі як SSL / TLS, багато хмарних підключень залишаються вразливими для атак. А це дуже важливий момент: щоб усунути можливість несанкціонованого втручання в роботу пристрою, обмін між контролером і сервером повинен йти у зашифрованому за допомогою ключа вигляді.

Поставивши собі ці питання, компанії Google, Samsung Electronics, Silicon Labs і деякі інші об'єдналися з метою розробити новий бездротовий мережевий стандарт спеціально для розумних будинків. Він отримав назву Thread[6]. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а основною його перевагює є саме забезпечення механізмів безпеки.

Одночасно в мережі можуть знаходитися до 250 пристроїв, які захищаються шифруванням рівня банківської системи. Ще одна особливість Thread ─ це прозорість. Користувач бачить список всіх підключених пристроїв, завдяки якому йому легко визначити, що з чим пов'язано. Проте, така система вимагає значних ресурсів від усіх елементів “розумного будинку”.

1.2 Аналіз технології «Розумний будинок»

«Розумний будинок» ─ житловий будинок сучасного типу, організований для проживання людей за допомогою автоматизації і високотехнологічних пристроїв. Під «розумним будинком» слід розуміти систему, яка забезпечує безпеку, комфорт і ресурсозбереження для всіх користувачів [7].

Сьогодні виділяється три варіанти побудови системи «розумний дім» [8]:

—Системи централізованого управління системи «розумний дім».

—Системи децентралізованого управління системи «розумний дім».

—Системи, що працюють по радіоканалу в силовій проводці

— (X-10).

Щоб зрозуміти ризики, пов'язані з системами «розумного будинку», необхідно розглянути архітектуру такої системи. Як приклад візьмемо найбільш загальний варіант домашньої автоматизації. Уразливі місця системи показані на рисунку 1.2.

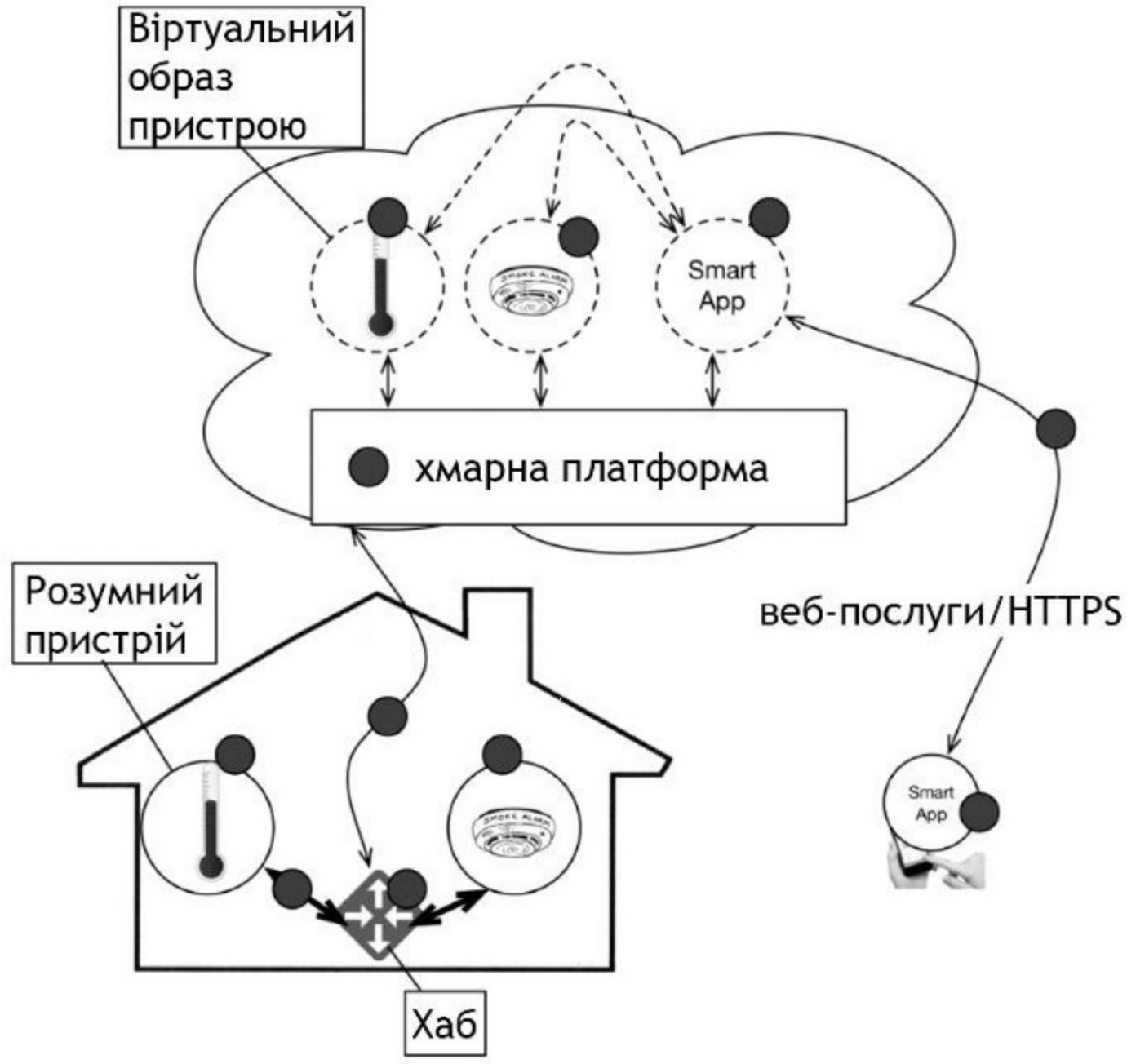


Рисунок 1.2 – Вразливі місця “розумного будинку”

Компонентів системи, як правило, багато і всі вони різноманітні. Наприклад, «розумний» пристрій. Пристрої значно розрізняються як за своєю функціональністю, так і за доступними ресурсами — від спеціалізованого комп'ютера до мініатюрного сенсора або контролера. Перша категорія пристроїв є найбільш привабливою для рекрутерів ботнетів. Широко відомі випадки використання «розумних» холодильників для розсилки спаму або медіаресивера для створення потужної атаки відмови в обслуговуванні. Для другої категорії використовуються спеціалізовані ОС. Скомпрометовані

пристрої цієї категорії можуть використовуватися для атаки на самого власника (збір даних, заміна функціональності), а також для атаки на інші пристрої мережі.

Комунікаційні протоколи. Всі пристрої системи можуть бути підключені до Інтернету. При цьому має сенс виділити бездротовий зв'язок в якості окремого компонента.

Бездротовий зв'язок. WiFi може бути уразливим місцем, коли атакуючий знаходиться на невеликій відстані від пристроїв. Це може бути і атака відмови в обслуговуванні шляхом глушіння сигналу або атака посередника, якщо атакуючому вдається підключитися до бездротової мережі.

Протоколи верхніх рівнів. Недостатній захист на цьому рівні, наприклад, відсутність надійної автентифікації і захисту даних, може бути використана для атаки «людина всередині» з усіма наслідками, що випливають.

Шлюз або хаб. Шлюз забезпечує обмін даними між пристроями, що використовують різні протоколи. Також шлюз зазвичай забезпечує опосередковане підключення цих пристроїв до Інтернету і доступ до хмарних послуг. Проблеми, які перераховані для пристроїв з достатніми ресурсами, є актуальними і для шлюзів.

У деяких архітектурних рішеннях, як наприклад, HomeKit, шлюз бере на себе також розширені функції, що зазвичай надаються хмарними послугами ─ збір, аналіз і зберігання даних, програми автоматизації, а також забезпечує віддалений доступ до функцій системи «розумного будинку». Також шлюз часто забезпечує захист підключених до нього пристроїв, тому забезпечення безпеки для цього елемента надзвичайно важливо.

Хмарні послуги. Оскільки можливості більшості «розумних» об'єктів обмежені, обчислювальні ресурси для підтримки процесів автоматизації і управління пристроями, збору і зберігання даних, а також надання віддаленого доступу забезпечуються віддаленими серверами, найбільш

типово розміщеними в хмарі. Такий підхід дозволяє також управляти не ізольованими пристроями, а їх ансамблем ─ наприклад, координуючи роботу освітлювальної та опалювальної систем, системи безпеки, датчиків руху і т.д..

Програмне забезпечення платформи. Хмарна платформа забезпечує реєстрацію і управління пристроями. Після реєстрації пристрою платформа створює віртуальний образ фізичного об'єкта системи, забезпечуючи обчислювальні ресурси і пам'ять, необхідні для його роботи і автоматизації. Хмарна платформа є свого роду віртуальною операційною системою для додатків системи. Платформа відіграє критичну роль у забезпеченні безпеки, так само як мобільна ОС визначає рівень безпеки смартфона. Реєстрація пристрою і додатків, контроль доступу до різних функцій пристрою ─ від реалізації цих функцій залежить захищеність усієї системи.

1.3 Типові моделі побудови «Розумного будинку»

Системи централізованого управління складаються з центрального контролера, панелей управління і безлічі виконавчо-командних блоків.

Центральний контролер в даній системі автоматизації «розумний будинок» виконує функції мозку ─ до нього підключаються всі інші системи. Різні компоненти мають свої мікроконтролери, але програма взаємодії знаходиться в одному ─ головному.

Від головного контролера сигнали управління можуть йти до виконавців по різних каналах.

До особливостей даної системи можна віднести:

– опрацювання ядра і програмного забезпечення;

– можливість зібрати в єдиний комплекс всі системи і звести управління ними на єдиний пульт;

– можливість включати в якості виконавців пристрої від різних виробників «розумного будинку»;

– значна вартість для створення графічного інтерфейсу;

– продумана робота з аудіо- та відеотехнікою, мультирум-системами, живим відеосигналом;

– респектабельний дизайн і функціональність панелей управління, впізнаваність і престижність.

Проектування та інсталяція системи в даному випадку доступні тільки кваліфікованим фахівцям. При цьому монтаж можна здійснити в ході ремонту або спорудження будинку.

На противагу вказаному відзначається її велика вартість і обмежений вибір дизайнерських рішень зовнішнього вигляду і кольорів сенсорних і клавішних пультів управління.

Типова схема системи централізованого управління представлена на малюнку 1.3:

Рисунок 1.3 – Централізована схема розумного будинку

Децентралізоване управління здійснюється в межах пристроїв. Незалежно від того, являються вони передавачами чи приймачами, вони

пов'язані один з одним безпосередньо по загальному каналу — шині. Передача даних між пристроями здійснюється по протоколу шини.

Схема децентралізованого управління має просту структуру, яка продемонстрована на рисунку 1.4:

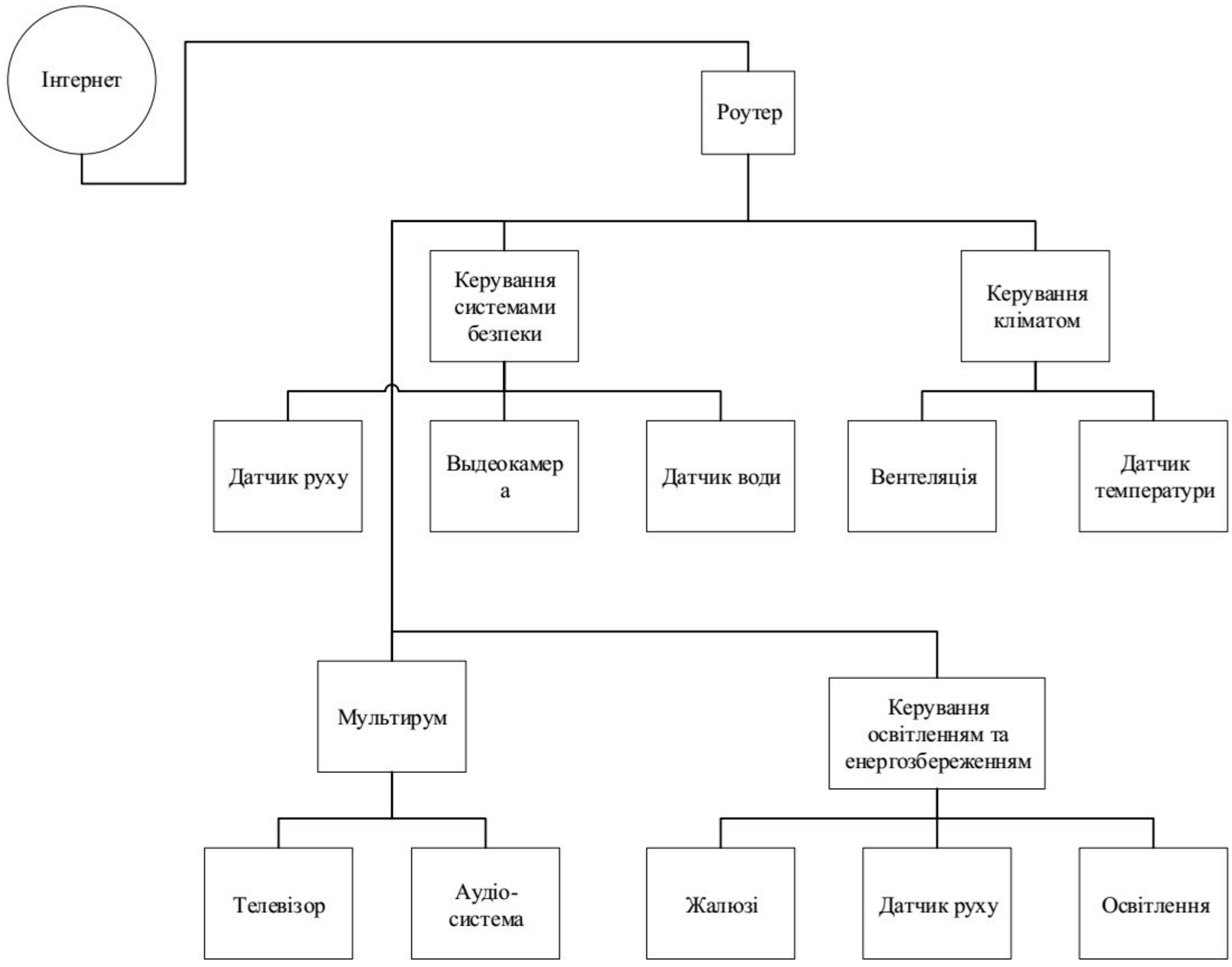


Рисунок 1.4 – Децентралізована схема розумного будинку

Дана схема повністю автономна і незалежна, надійна в роботі, багатофункціональна, вона дозволяє гнучко перепрограмувати систему під бажання користувача.

Децентралізована система має відмінне опрацювання програмно-апаратного забезпечення компонентів, величезні можливості розширення, хороші засоби створення графічного інтерфейсу. Однак система має досить високу ціну, невисоку швидкість передачі команди (близько 0,3 сек).

X10 — це метод і протокол передачі керуючих сигналів-команд по силовій електропроводці на електронні модулі, до яких підключені керовані електропобутові та освітлювальні прилади.

Рухаючись від пристрою по мережі X10, повідомлення містять два інформаційних поля ─ адреса пристрою, якому ця команда адресована, і саму команду. Підключені до електромережі пристрої X10 приймають передані повідомлення, декодують поле адреси одержувача і, якщо він збігається з їхньою власною адресою, виконують команду. Тобто кожен контролер системи «розумний дім» отримує сигнал незалежно від того, кому він призначався.

Типова схема, що працює по радіоканалу в силовій проводці, представлена на рисунок 1.5:

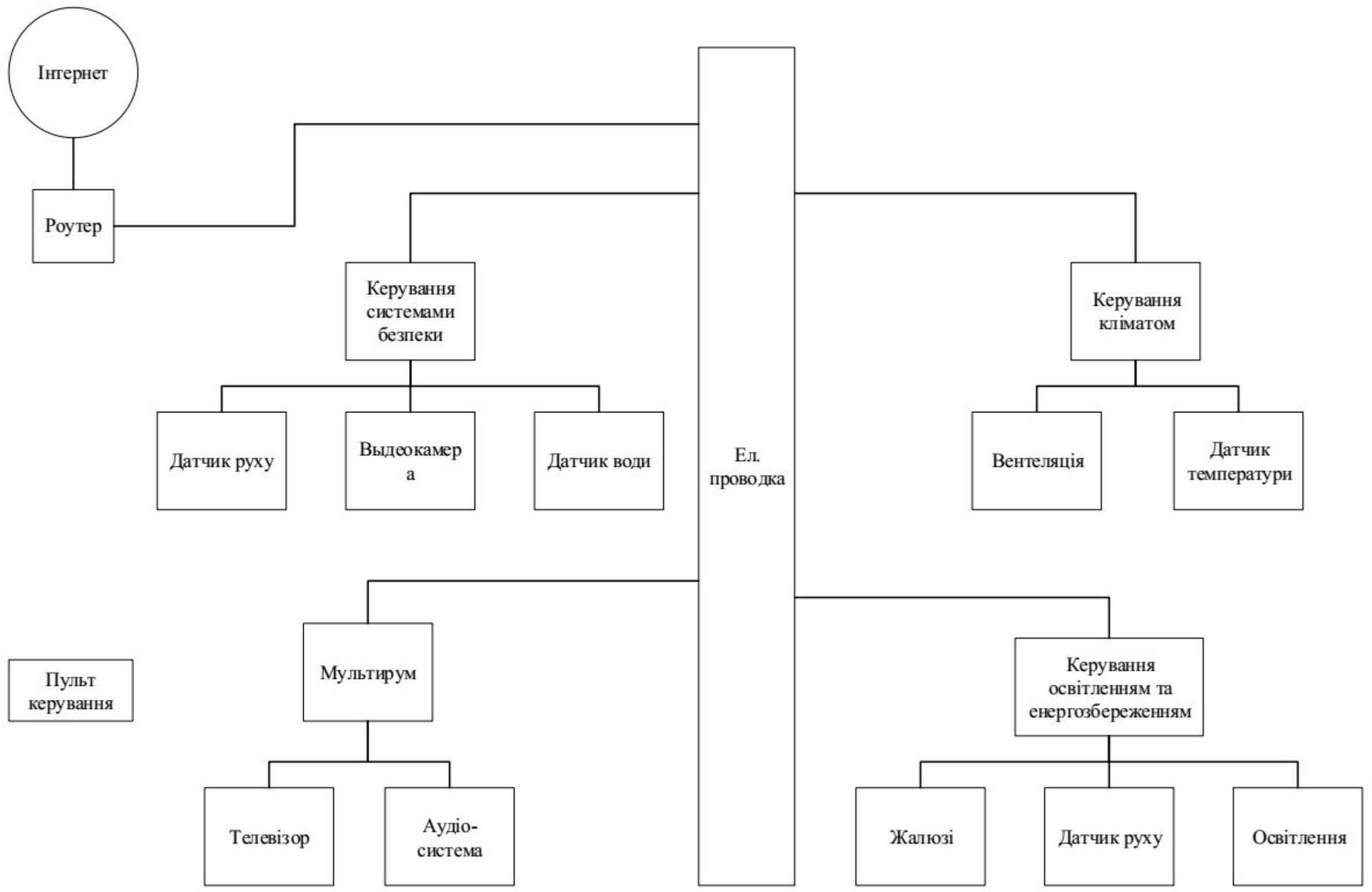


Рисунок 1.5 – Розумний будинок виконаний по стандарту X-10

Протокол X-10 має низьку ціну і легкий монтаж пристроїв ─ він сумісний з будь-якими пристроями від різних виробників, крім того, можлива легка інтеграція. Однак він має низьку швидкість передачі інформації, низьку захищеність, проблему помилкового спрацьовування, відсутність зворотного зв'язку приймача з передавачем, при цьому можливий несанкціонований доступ до пристроїв X-10 по електромережі.

1.4 Аналіз технології Wi-Fi

Одним з найбільш розповсюджених протоколів передачі даних у мережі “розумний будинок” є саме Wi-Fi. Аналіз використання технології Wi-Fi в розумному будинку необхідно починати з вивчення роботи Wi-Fi пристроїв та ноутбуків, персональних комп'ютерів, мобільних пристроїв і закінчуючи «розумними» мікропроцесорними системами управління технологічними процесами. Даний вид зв'язку значно спростив доступ до мережі користувачам і відкрив можливості, недоступні при використанні дротових видів зв'язку. Проте не всі на підприємствах знають, скільки небезпеки чекає кожного користувача під час використання Wi-Fi мережі [9].

Під час аналізу технології Wi-Fi треба починати з того, що бездротові мережі Wi-Fi діляться на два типи - відкриті і закриті. Мережі відкритого типу (OPEN), як правило, не використовують захист для підключення до самого пристрою або використовують віддалений захист доступу до мережі, коли аутентифікація користувача відбувається не на самому пристрої, а на віддаленому сервері. Однак жоден з вищеописаних способів не буде захищати користувачів, підключених до самої Wi-Fi мережі від атак типу MITM (людина посередині). Або коли зловмисник вже підключився до мережі. Це відбувається коли інформація в мережі проходить через зловмисника, що негативно позначається на надійності інформації, що передається у відкритій мережі підприємства. Такий вид мережі не рекомендується для використання з точки зору захисту інформації.

У випадку, коли є необхідність використання даного виду мережі для передачі конфіденційної інформації, то рекомендується використовувати VPN (віртуальна приватна мережа) для захисту самого каналу передачі даних. Також, досить важливе та актуальне використання розширеного протоколу HTTP що застосовує шифрування SSL для приховування запитів від клієнта до сервера підприємства [10].

Ця технологія дозволяє переглянути передані пакети даних при їх перехопленні, що підвищує надійність передачі інформації в мережі Wi-Fi.

Інший вид бездротової мережі - мережі закритого типу, як правило, використовують шифрування для захисту пакетів даних в каналі передачі інформації. Для них використовуються найбільш популярні технології захисту такі, як: Wired Equivalent Privacy (WEP - застаріла технологія для забезпечення безпеки бездротової Wi-Fi мережі), Wi-Fi Protected Access (WPA і WPA2 - являє собою оновлену технологію захист пристроїв бездротового зв'язку, і Wi-Fi Protected Setup / Quick Security Setup (WPS / QSS - захищена установка, що використовується в WPA / WPA2).

Треба відзначити, що у мережі закритого типу теж є вразливості, але при правильній конфігурації, ризики можна мінімізувати [11].

Технологія WEP одна з найперших технологій захисту. В даний час вкрай ненадійна і не рекомендується для використання. Проблема в тому, що потік даних шифрується тимчасовим ключем, частина якого є в кожному пакеті. Отже, якщо перехопити необхідне число пакетів, з'являється можливість отримати ключ будь-якої довжини. Тому, актуальність та важливість використання даної технології недоцільна, так як час перехоплення ключа залежить від обсягу інформації, що передається по бездротовій мережі, чим її більше передається, тим швидше у зловмисника з'являється можливість перехоплення ключа.

Технологія WPA, яка є сумою протоколів EAP, MIC, TKIT, 802.1X дозволяє її використовувати в комерційному секторі.

На відміну від WEP в WPA встановлення основного ключа неможливо, але є спосіб дізнатися ключ, який необхідний для перевірки цілісності потоку даних. Щоб реалізувати такі атаки зловмисникові необхідно знати MAC адресу клієнта, підключеного до Wi-Fi мережі. Для подальшої крадіжки цієї адреси і підміни на своєму пристрої вразливою є мережа Wi-Fi. Тому, мережа Wi-Fi повинна підтримувати сучасні технології WMM і QoS де зміна тимчасового ключа триває не більш ніж 3600 секунд.

Найпростіший захист від даного виду вразливості полягає в тому, щоб зменшити значення тимчасового ключа. Це надасть гарантію від другого виду злому - це стандартного брутфорсу, тобто, підбору всіх можливих комбінацій звичайним перебором. Захист від даного методу злому - це щомісячна зміна пароля.

Існує вид атаки під назвою «злий двійник», який може використовуватись на підприємствах. Мета атаки полягає в копіювання імені SSID бездротової мережі. На підставі цього створюється підроблена бездротова мережа з більш сильним сигналом випромінювання, ніж у справжньої бездротової мережі.

Тому, для зменшення ризику від даної атаки, рекомендується зменшити час зміни частоти радіоканалів, а також використовувати шифрування при передачі даних на підприємстві.

Технологія WPA2 - це досить актуальна та доповнена версія технології WPA. В ній усунена вразливість з розкраданням і підміною ключового потоку. Так само актуальним є доданий новий протокол AES / CCMP з новим алгоритмом шифрування заснованому на AES256 та додатковим захистом і перевіркою на цілісність. Дану технологію, можливо тільки зламати за допомогою брутфорса, захист від якого є щомісячна зміна ключа.

Протокол WPS / QSS розроблений для створення захищеної WPA2 мережі. В даному протоколі передбачено підключення по восьми значному PIN-коду. Вразливість даного протоколу полягає в наступному. Так як в PIN-коді використовується вісім цифр - підбір PIN-коду складається 108 варіантів. Остання цифра є контрольною сумою, яка вираховується за семи перших цифр. Проте в самому протоколі спочатку є вразливість, яка дозволяє розділити PIN-код на дві частини, 4 і 3, які підбираються окремо один від одного в такому випадки підбір PIN-коду 104 і 103 становить 11000 комбінацій. Даний протокол вкрай вразливий. Тому, після отримання PIN-коду відсилається інформація про ключі WPA2 клієнту, що робив запит на підключення, який згодом може бути використаний.

На початку 2018 року міжнародний альянс Wi-Fi Alliance анонсував новий протокол бездротової безпеки - WPA3. Основними доповненнями, що будуть реалізовані в цьому протоколі стануть:

- вбудований захист від брутфорс-атак;

- індивідуальне шифрування даних для посилення конфіденційності користувачів у відкритих Wi-Fi мережах;

- спрощене налаштування IoT-пристроїв ("розумний будинок");

- вдосконалений криптографічний стандарт для мереж Wi-Fi ("192-розрядний пакет безпеки").

Найбільш ефективним є використання блокування таймеру декількох невдалих спроб введення пароля. Тому, рекомендується відключати даний протокол в налаштуваннях мережі для запобігання крадіжки ключа WPA2 і несанкціонованого підключення до бездротової мережі підприємства [12]. Проте, для “розумного будинку” дана технологія не підходить, адже вона може завадити роботі авторизованого пристрою

1.5 Системи моніторингу

Моніторинг IoT пристроїв потрібен в першу чергу для забезпечення захисту мережі, а також безпосередньо пристроїв, які знаходяться всередині мережі. Захист забезпечується можливістю цілодобового слідкування за підключеними пристроями.

Моніторинг — це постійний збір і реєстрація інформації за наперед визначеним переліком показників (індикаторів). Запровадження системи моніторингу потребує витрат часу, коштів та інших ресурсів, але забезпечує, своєю чергою, належне виконання норм захисту та профілактики мережі.

Моніторинг буде проводитись за допомогою спеціалізованого ПЗ, моніторити необхідно цифровий підпис, в свою чергу моніторинг буде відбуватись у реальному часі на сервері.

Під дані критерії підпадають одразу декілька систем моніторингу, а саме:

– Ntopng;
– Zabbix;
– 10-страйк: Мониторинг сети;
– Network MACMonitor.

Система моніторингу Zabbix цікава в першу чергу тим, що надає можливість підключати власні модулі, наприклад UniFi Miner, яка надає змогу моніторити пристрої за заданими параметрами, а також пропонує широкий спектр додаткових графіків. Також, для зручності, додаток дає можливість підписати кожен з пристроїв і виводить статистику їх активності за певний час. Даний модуль використовує оперативні дані - показники і настройки, отримані від контролера UniFi через API, наданий компанією Ubiquiti. А також підтримує протокол Zabbix Low-level Discovery.

Ntopng - безкоштовне програмне забезпечення з відкритим вихідним кодом для моніторингу мережевого трафіку, яке надає веб-інтерфейс для моніторингу мережі в режимі реального часу. Дана система моніторингу використовує механізм RSPAN (Remote Switch Port Analyzer), працює він на канальному рівні моделі TCP / IP і дозволяє "віддзеркалювати" трафік. Тобто дана технологія дозволяє налаштувати комутатор так, щоб всі пакети, що приходять на один порт або групу портів комутатора, дублювалися на іншому, з метою їх подальшого аналізу і моніторингу.

Network MACMonitor - програма адміністрування комп'ютерних мереж, в якій зроблено акцент як на розташуванні пристроїв і користувачів в мережі, так і на обліку комутації елементів мережі. Головний її недолік заключається у тому, що Network MACMonitor не працює з бездротовими мережами. Працює даний додаток наступним чином, він опитує мережеві пристрої за допомогою протоколу SNMP і отримує ARP і MAC таблиці, які містять інформацію про IP і MAC адреси кінцевих пристроїв, а також опитує комп'ютери за допомогою протоколу WMI і отримує інформацію про дані

комп'ютери, яка включає в себе сесії користувачів, що працюють за комп'ютерами. До найбільшої переваги можливо віднести можливість вести облік комутації портів мережевих пристроїв, патч-кордів, патч-панелей, портів патч-панелей, ліній і мережевих розеток.

10-страйк: Мониторинг сети - програма для контролю серверів та мережевого обладнання. Програма реалізована у вигляді служби і може бути встановлена на сервері або робочої станції Windows для моніторингу пристроїв в мережі і видачі сповіщень в цілодобовому режимі 24/7 без необхідності входу з будь-якого облікового запису. Здійснюйте моніторинг різних перемінних в керованих комутаторах по протоколу SNMP.

Одним з найбільш універсальних засобів моніторингу є моніторинг за допомогою режима promiscuous[14]. У комп'ютерних мережах режим promiscuous - це особливий режим обладнання Ethernet, як правило мережевих інтерфейсних карт (NIC), який дозволяє карті отримувати весь трафік мережі, навіть якщо цей трафік не адресований конкретно даній карті. За замовчуванням NIC ігнорує повністю не адресований йому трафік шляхом порівняння адреси призначення Ethernet-пакета і апаратної адреси пристрою одержувача (MAC-адреси). Хоча така схема роботи цілком виправдана технічно, режим не-promiscuous істотно ускладнює роботу програм мережевого аналізу та моніторингу, що застосовуються для діагностики мережевих проблем і обліку трафіку. У більш широкому сенсі режим promiscuous також означає прозорість мережі з певної точки спостереження, але при цьому не передбачається обов'язкове переключення адаптерів в такий режим. У сучасному обладнанні і програмному забезпеченні часто реалізовані і інші способи моніторингу для досягнення повної видимості всіх мережевих процесів.

Моніторинг та аналіз мережі представляє собою важливі етапи контролю роботи мережі. Для виконання цих етапів вже давно розроблено ряд програм і засобів, що працюють автономно і тоді, коли їх втручанні необхідне. До складу автономних програмних засобів моніторингу і аналізу

входять засоби діагностики, аналізатори протоколів, експертні системи. До складу іншої групи входять безпосередньо системи моніторингу які спроможні вести діагностику 24/7.

1.6 Аналіз малоресурсної криптографії

Головною особливістю сучасного етапу розвитку Інтернету є дедалі зростаючу кількість найрізноманітніших інтелектуальних пристроїв, що мають доступ в Інтернет. В силу умов їх функціонування, а також жорстких цінових обмежень, які характерні для масового виробництва, ці пристрої характеризуються значними обмеженнями на використовувані ресурси пам'яті, обчислювальну потужність, джерела живлення і т.д. Звідси випливають обмеження на використовувані технології і технологічні рішення, що пред'являються до засобів малоресурсної криптографії[15].

Ефективність реалізації того чи іншого перетворення на програмному або апаратному рівні оцінюється по-різному. для порівняння програмних реалізацій прийнято розглядати вимоги до пам'яті та часу роботи, що вимірюється в тактах процесора. Для апаратної реалізації критерієм ефективності є перш за все розмір мікросхеми і час роботи в тактах процесора, хоча для дуже багатьох додатків важливим фактором є енергоспоживання пристрою.

Більшість вимог, що пред'являються до алгоритмів, призначеним для використання в малоресурсних умовах, були закріплені в рамках міжнародного стандарту ISO / IEC FDIS 29192 - Information technology - Security techniques - Lightweight cryptography[16], а саме:

- General Part
- Block ciphers Part
- Stream ciphers Part
- Mechanisms using asymmetric techniques

ISO / IEC 29192 є міжнародним стандартом, що визначає засоби нізкоресурсной криптографії для забезпечення секретності, автентичності, ідентефікаціі, неспростовності і ключового обміну (data confi dentiality, authentication, identifi cation, non-repudiation, and key exchange). Так як розроблюваний проект є програмним, надалі будуть розглядатись лише ті аспекти, які характерні для програмної частини.

Алгоритми малоресурсної криптографії розробляються спеціально для пристроїв з обмеженими обчислювальними ресурсами. Критерії, за якими можна сказати, що даний алгоритм можна віднести до категорії полегшеної криптографії є занадто розпливчасті і можуть відрізнятися в кожному конкретному випадку, вони залежать від використовуваної апаратної частини. Умовно прийнято вважати, що алгоритм відноситься до легковагої криптографії, якщо його можливо реалізувати на 1000 логічних елементах (GE) і менше. Типові обмеження для малоресурсної криптографії:

- розмір мікросхеми;
- споживана енергія;
- розмір програмного коду;
- розмір оперативної пам'яті;
- ширина смуги робочих частот каналу зв'язку;
- час, витрачений на виконання програми.

Криптографічні примітиви (cryptographic primitives) є основним криптографічним інструментарієм, який забезпечує виконання тих чи інших криптографічних сервісів. Зазвичай їх поділяють на примітиви з секретним ключем (симетричні примітиви), примітиви з відкритим ключем (асиметричні примітиви) і безключового примітиви (рис. 1.6)[17].

Рисунок 1.6 – Класифікація примітивів

Для примітивів з секретним ключем криптографічний стійкість забезпечується таємністю ключа, який повинен залишатися невідомим для всіх учасників інформаційного процесу, які не мають відповідних повноважень. У цей клас входять такі примітиви, як симетричні шифри (Які, в свою чергу, поділяються на блокові шифри і потокові шифри), ключові геш-функції, звані також кодами перевірки справжності повідомлення(Keyed hash function, Message Authentication Code - MAC) а також криптографічні генератори псевдовипадкових послідовностей.

Примітиви з відкритим ключем використовують пари ключів (e, d) - (ключ шифрування, ключ розшифрування) або (Відкритий ключ, секретний

ключ). Криптографічний стійкість забезпечується таємністю секретного ключа, який повинен залишатися невідомим для всіх учасників інформаційного процесу, які не мають відповідних повноважень. У цей клас входять такі примітиви, як протоколи вироблення та узгодження ключів, асиметричні шифри (шифри з відкритим ключем), схеми цифрового підпису та деякі інші.

У клас безключових примітивів входять примітиви, які не використовують ключів. Такі примітиви використовуються в таких криптографічних сервісах, як аутентифікація і забезпечення цілісності інформації. У цей клас входять такі примітиви, як односпрямовані підстановки (One-way permutation), хеш-функції, безключові хеш-функції або коди виявлення модифікації інформації (unkeyed hash function, Modifi cation Detection Code - MDC), генератори випадкових послідовностей та інші.

1.7 Формалізація вимог та постановка задачі

Проаналізувавши вищевикладені дані можна зробити висновок, що існуючі системи моніторингу безпеки розумного будинку роблять наголос на захисті фізичного майна, це різноманітні системи відеоспостереження, моніторингу стану повітря, температури та ін. В той же час майже не звертаючи уваги на кіберзлочинців, які можуть перехопити дані безпосередньо з самої системи розумного будинку. Практика показала, що дані можливо зчитати майже з будь якого ”Розумного” пристрою, починаючи з телевізору, який прослуховує кімнату 24/7 і закінчуючи холодильником з виходом у інтернет.

Процес створення системи моніторингу розумного будинку буде розділено на декілька етапів:

– аналіз актуальних загроз для розумних будинків;
– вибір малоресурсної криптографії;

– вибір актуального програмного та апаратного забезпечення для реалізації моніторингу захисту;
– тестування дозволить визначити помилки у роботі тестової системи моніторингу, а також визначить її придатність для практичного застосування.

В результаті виконання задачі отримано засіб для моніторингу захисту систем розумних будинків, яка дозволить виявляти певні типи зловмисних дій, такі як під’єднання несанкціонованого пристрою у мережу розумного будинку.

2 ОБГРУНТУВАННЯ МЕТОДІВ ВИБОРУ РІШЕНЬ ОСНОВНОЇ ЗАДАЧІ

2.1 Розробка моделі загроз

Ключовим моментом створення системи захисту інформації системи «розумний дім» є побудова моделі загроз. При цьому можливе складання загроз за різними схемами. Наприклад, можна визначитися зі списком актуальних загроз відповідно до класифікатора. Так, ISO 17799 дозволяє визначити повний набір можливих загрози (альтернативою може бути Британський стандарт BS 7799, Російський стандарт ГОСТ Р 51275-2006 та інші). Або список актуальних загроз визначається відповідно до статистики (прикладами ресурсів зі статистиками можуть бути Касперський, infowatch та інші).

При розробці дерева загроз системи «розумний дім» необхідно враховувати технічні побудови системи, так як склад обладнання впливає на визначення можливих загроз.

Модель загроз - фізичне, математичне, описове уявлення властивостей або характеристик загроз безпеки інформації. Формою представлення моделі загроз - є дерево загроз. Для визначення структури дерева і можливих загроз виділяються ключові модулі:

- Хмарне управління системою «розумний дім».
- Пульт дистанційного керування.
- Wi-Fi.
- Мережа електроживлення.
- Оптоволоконні і коаксіальні кабелі.
- Устаткування (датчики руху, відеокамери і т.д.).
- Програмне забезпечення.

Для кожного модуля визначається набір загроз. На рисунку 2.1 представлено дерево загроз. Відповідність загрози схемою побудови системи «розумний дім» визначається візуальним індикатором.

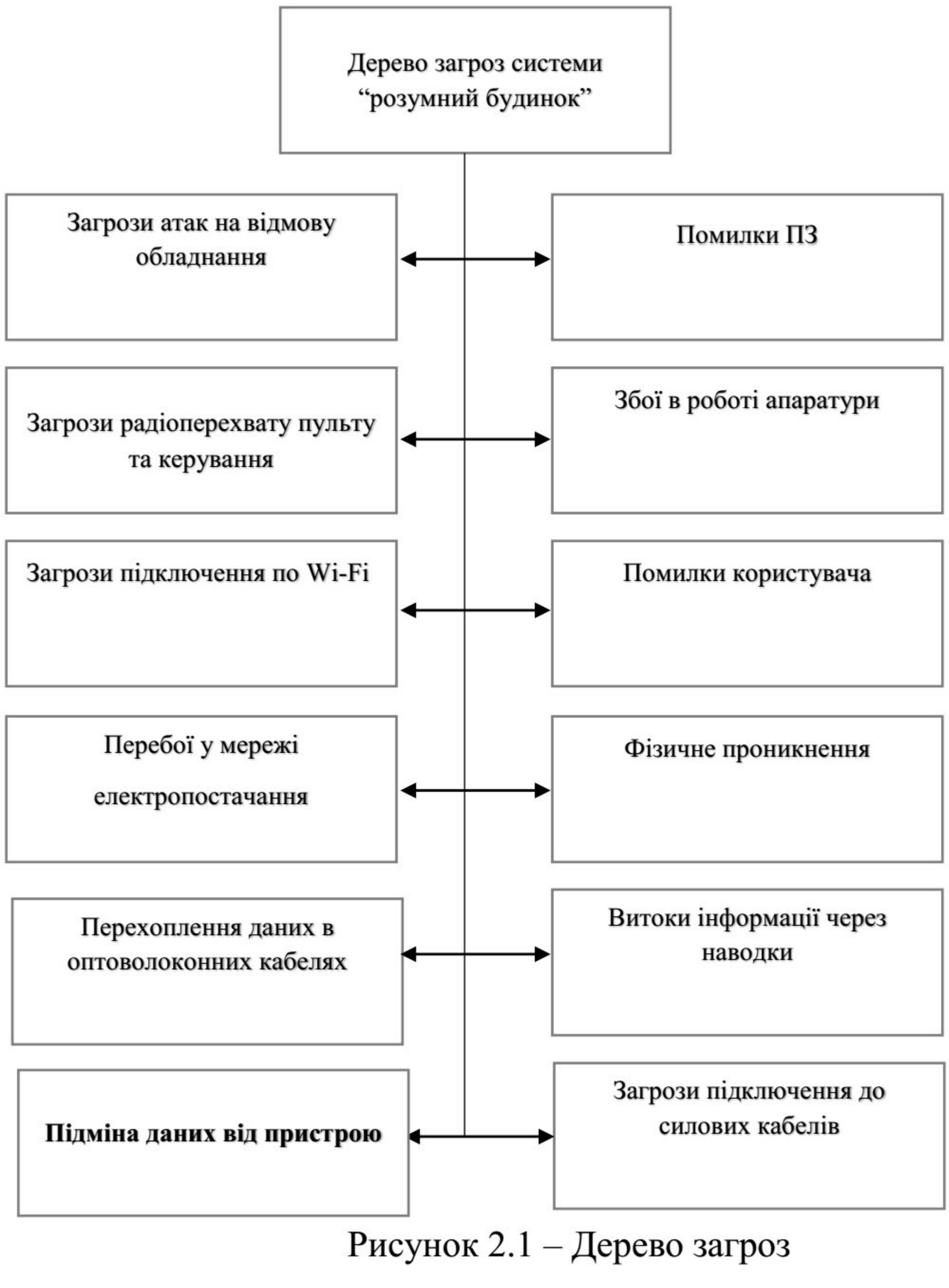


Рисунок 2.1 – Дерево загроз

Формалізоване представлення моделі загроз системи захисту інформації системи «Розумний дім» має вигляд:

$$F_u = \{F_1, F_2, F_3\}$$

$$F_1 = \mu_1(\{K_i\})$$

де і - множина загроз в централізованій системі «розумного будинку», і = 1; 11

$$F_2 = \mu_2(\{N_i\})$$

де j - множина загроз в централізованій системі «розумного будинку», i = 1; 11

$$F_3 = \mu_3(\{U_l\})$$

де l - множина загроз в централізованій системі «розумного будинку», i = 1; 11

Логічна форма представлення моделі загроз в системі «розумний будинок»:

$$F_u = F_1 V F_2 V F_3$$

де Ki - загрози централізованого управління системи «розумний дім»; Nj - загрози децентралізованого управління системи «розумний дім»; Ul - загрози системи «розумний дім», що працює по радіоканалу в силовій проводці.

F1 - функція системи централізованого управління системи «розумний дім», F2 - функція системи децентралізованого управління системи «розумний дім», F3 - функція системи, яка працює по радіоканалу в силовій проводці.

Представлена модель дозволить формалізувати процес системи захисту «розумний будинок» і таким чином вийти на новий рівень ефективності функціонування всієї системи в цілому.

В результаті проаналізованого матеріалу було прийнято рішення, що одним, з найбільш вразливих ланок в захисті являється саме бездротова мережа, яка використовується майже у всіх децентралізованих системах “розумний будинок”.

2.2 Аналіз захисту мережі Wi-Fi

Існують багато відомих методів та заходів безпеки Wi-Fi мереж які забезпечуються різними стандартами протоколів (табл. 2.1).

Таблиця 2.1 - Порівняльна характеристика поширених протоколів захисту у Wi-Fi мережах

Властивість протоколів	Протокол WPA	Протокол WPA2
Рівень захисту (стійкість до зламу)	середній	високий
Авторизація	шифровані ключі: WPA-Personal, WPA-Enterprise	шифровані ключі: WPA-Personal, WPA-Enterprise, підтримка шифрування AES CCMP
Довжина ключа (у бітах)	128, 192 і 256	128, 192 і 256
Вимоги щодо налаштування статичного ключа	не існують	не існують

Насамперед, самий перший з них - стандарт протоколу IEEE 802.11 передбачає забезпечення безпеки бездротових мереж за допомогою використання механізмів WPA2 (Wi-Fi Protected Access 2).

Проблема безпеки з самого моменту появи мережі Wi-Fi являється однією з найскладніших. Справа в тому, що в прототипах Wi-Fi це питання, як таке, практично не стояло. У розробників стандарту 802.11b (який зараз найбільш популярний і власне представляє торгову марку Wi-Fi) головним завданням була сумісність обладнання з спрощенням процедур доступу. З іншого боку, при використанні бездротової комп'ютерної мережі, зрозуміло, що для зловмисника вона є більш вразливою, ніж звичайна дротова мережа, так як питання фізичного доступу до трафіку вирішується наявністю недорогого радіообладнання.

Технологія WEP одна з найперших технологій захисту. В даний час вкрай ненадійна і не рекомендується для використання. Проблема в тому, що потік даних шифрується тимчасовим ключем, частина якого є в кожному пакеті. Отже, якщо перехопити необхідне число пакетів, з'являється

можливість отримати ключ будь-якої довжини. Тому, актуальність та важливість використання даної технології недоцільна, так як час перехоплення ключа залежить від обсягу інформації, що передається по бездротовій мережі, ніж її більше передається, тим швидше у зловмисника з'являється можливість перехоплення ключа.

Технологія WPA, яка є сумою протоколів EAP, MIC, TKIT, 802.1X дозволяє її використовувати в комерційному секторі.

На відміну від WEP в WPA відновлення основного ключа неможливо, але є спосіб дізнатися ключ, який необхідний для перевірки цілісності потоку даних. Щоб реалізувати такі атаки зловмисникові необхідно знати MAC адреса клієнта, підключеного до Wi-Fi мережі. Для подальшої крадіжки цієї адреси і підміни на своєму пристрої вразливою є мережа Wi-Fi. Тому, мережа Wi-Fi повинна підтримувати сучасні технології WMM і QoS де зміна тимчасового ключа триває не менше ніж 3600 секунд [5].

Найпростіший захист від даного виду вразливості полягає в тому, щоб зменшити значення тимчасового ключа. Це надає гарантію від другого виду злому - це стандартний метод грубої сили, тобто, підбір всіх можливих комбінацій звичайним перебором. Захист від даного методу зламу - це щомісячна зміна пароля.

Існує вид атаки під назвою «злий двійник», який може використовуватись на підприємствах. Мета атаки полягає в копіювання імені SSID бездротової мережі. На підставі цього створюється підроблена бездротова мережа з більш сильним сигналом випромінювання, ніж у справжньої бездротової мережі.

Тому, для зменшення ризику від даної атаки, рекомендується зменшити час зміни частоти радіоканалів, а також використовувати шифрування при передачі даних на підприємстві.

Технологія WPA2 - це досить актуальна та доповнена версія технології WPA. В ній усунена вразливість з розкраданням і підміною ключового потоку. Так само актуальним є доданий новий протокол AES / CCMP з новим

алгоритмом шифрування заснованому на AES256 та додатковим захистом і перевіркою на цілісність. Дану технологію, можливо зламати за допомогою методу грубої сили, захист від якого є щомісячна зміна ключа.

Тому, WPA2 на сьогоднішній день є самим надійним методом захисту бездротових мереж Wi-Fi. Протокол WPS розроблений для створення захищеної WPA2 мережі. В даному протоколі передбачено підключення по восьми значному PIN-коду. Вразливість даного протоколу полягає в наступному. Так як в PIN-коді використовується вісім цифр - підбір PIN-коду складається 108 варіантів. Остання цифра є контрольною сумою, яка вираховується за семи перших цифр. Отже, підбір PIN-коду становить 107. Проте в самому протоколі спочатку є вразливість, яка дозволяє розділити PIN-код на дві частини, 4 і 3, які підбираються окремо один від одного в такому випадки підбір PIN-коду 104 і 103 становить 11000 комбінацій. Даний протокол вкрай вразливий. Тому, після отримання PIN-коду відсилається інформація про ключі WPA2 клієнту, що робив запит на підключення, який згодом може бути використаний.

2.3 Розробка системи моніторингу

При виконанні магістерської дипломної роботи пропонується вирішити проблему автентифікації “розумних” пристроїв за допомогою цифрового підпису з використанням малоресурсної криптографії. В такому випадку дані з систем моніторингу будуть актуальними і в разі підміни MAC-адреси буде зрозуміло, що зловмисник намагається проникнути до захищеної мережі. Саме система моніторингу допоможе відслідкувати такі випадки та оперативно усунути проблему.

Отже, система моніторингу захисту розумного будинку повинна відповідати таким вимогам:

– забезпечити взаємодію обладнання мереж і систем, в тому числі з діючими системами управління обладнанням;

– моніторинг повинен проводитися шляхом детального контролю за розумними пристроями (шляхом знімання інформації з існуючих систем управління мережами, обладнанням);

– система повинна створюватися з урахуванням сучасного досвіду розвитку засобів моніторингу та малоресурсної криптографії (наприклад, за допомогою цифрового ключа з використанням малоресурсного шифру) для вирішення поточних завдань користувача по контролю мережі, а також з урахуванням необхідності слідкувати за пристроями різних виробників.

Системи повинна включати наступні підсистеми, які входять в комплексне рішення:

– засоби взаємодії - забезпечують сполучення з різнорідним обладнанням різних виробників і діючими системами управління для вирішення завдання моніторингу;

– контроль справжньості - являє собою систему моніторингу з реєстрацією нових пристроїв у мережі. Підсистема забезпечує визначення несправжнього обладнання на основі цифрового підпису;

– облік мережевих ресурсів - відповідає за облік фізичних пристроїв в мережі і забезпечує користувача всією необхідною інформацією для прийняття більш зважених і вивірених рішень в обстановці, що складається при вирішенні завдань захисту мережі.

Отже, до системи моніторингу висуваються наступні вимоги: можливість віддаленого підключення до системи моніторингу, можливість автинтифікувати нові пристрої, можливість прибрати пристрої зі списку довірених.

2.4 Алгоритм автентифікації за допомогою ЕЦП

Електронний підпис – це дані в електронній формі, які приєднуються до інших електронних даних або логічно з ними пов'язані, і призначені для ідентифікації передплатника цих даних [18]. Підпис показано на рисунку 2.2.

Рисунок 2.2 – Схема підписання даних

Електронний цифровий підпис (ЕЦП) – вид електронного підпису, отриманий в результаті криптографічного перетворення набору електронних даних, який приєднується до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати особу підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [19].

Електронний цифровий підпис може використовуватися як засіб автентифікації для перевірки справжності користувача.

ЕЦП володіє всіма основними властивостями власноручного підпису:

- засвідчує те, що отриманий документ надійшов від його підписала особи;

- гарантує цілісність і захист від спотворення / виправлень підписаного документа;
- не дає можливості особі, яка підписала документ, відмовитися від зобов'язань, що виникли в результаті підписання цього електронного документа.

Для створення цифрового підпису у магістерській роботі використовується малоресурсна криптографія, а саме гешування даних та їх шифрування шифром Trivium. Верифікація даного підпису зображена на рисунку 2.3:

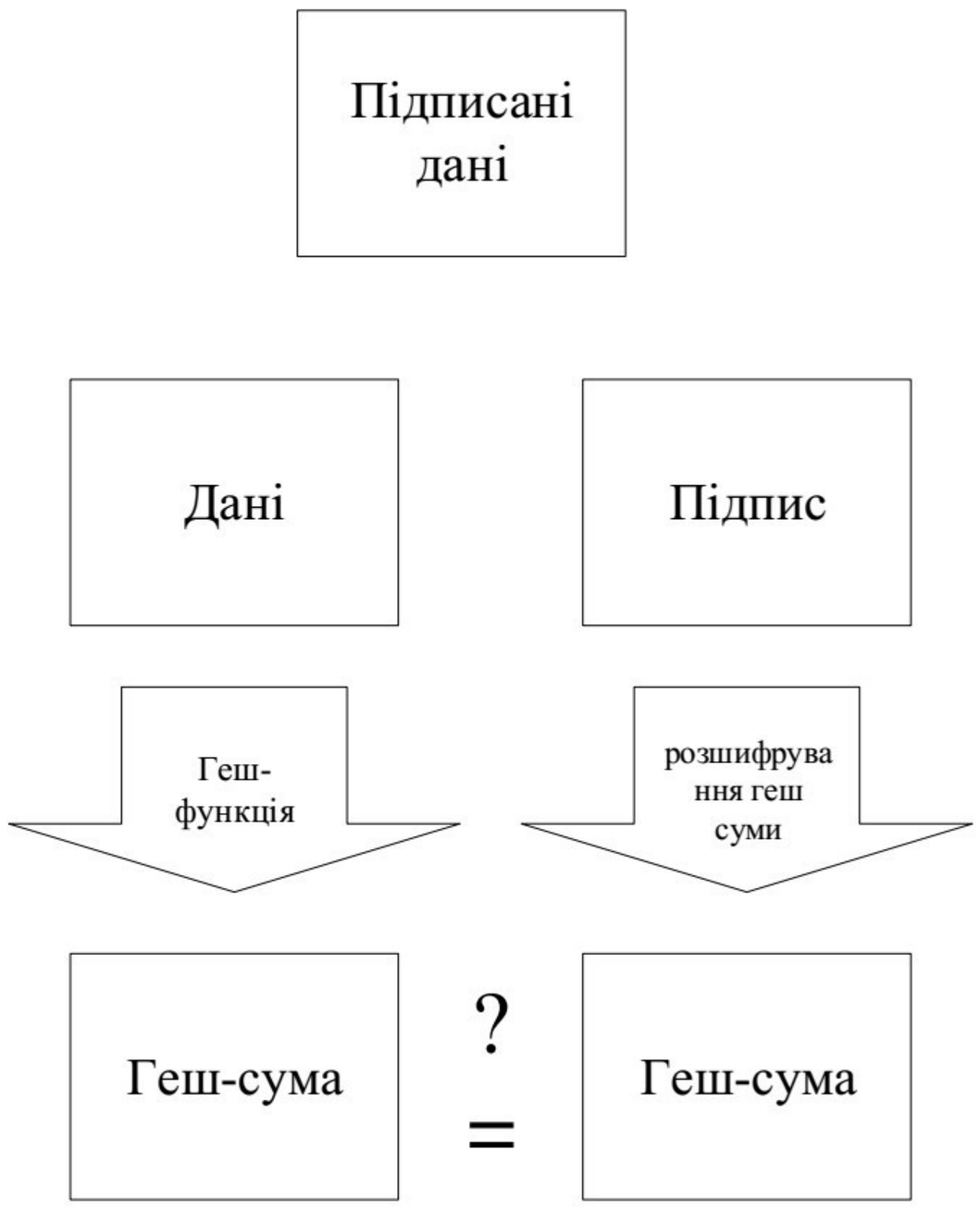


Рисунок 2.3 – Верифікація цифрового підпису

Якщо значення геш сум однакові, то дані не зазнали змін під час передачі.

2.5 Шифр Trivium

Trivium являє собою три зсувних регістра загальною довжиною 288 біт з нелінійної комбінацією прямого і зворотного зв'язку, які спільно формують

псевдовипадкову послідовність (біжить ключ) довжиною до $N \leq 2^{64}$ біт. Перший регістр алгоритму Trivium має довжину 93 біта, другий - 84 біта, третій - 111 біт[20].

При кожному такті виконання алгоритму відбувається зрушення вправо на один біт в кожному з бітових регістрів, а на виході генерується один біт біжить ключа. Шифрування повідомлення проводиться шляхом виконання операції XOR бітів повідомлення з відповідними бітами біжить ключа. розшифрування - шляхом виконання операції XOR бітів шифру повідомлення з відповідними битами біжить ключа.

На малюнку 2.4 зображено загальний вигляд алгоритму Trivium. Числами показана позиція біту в регістрах. Операція $\otimes$ означає множення, а операція $\oplus$ складання по модулю два.

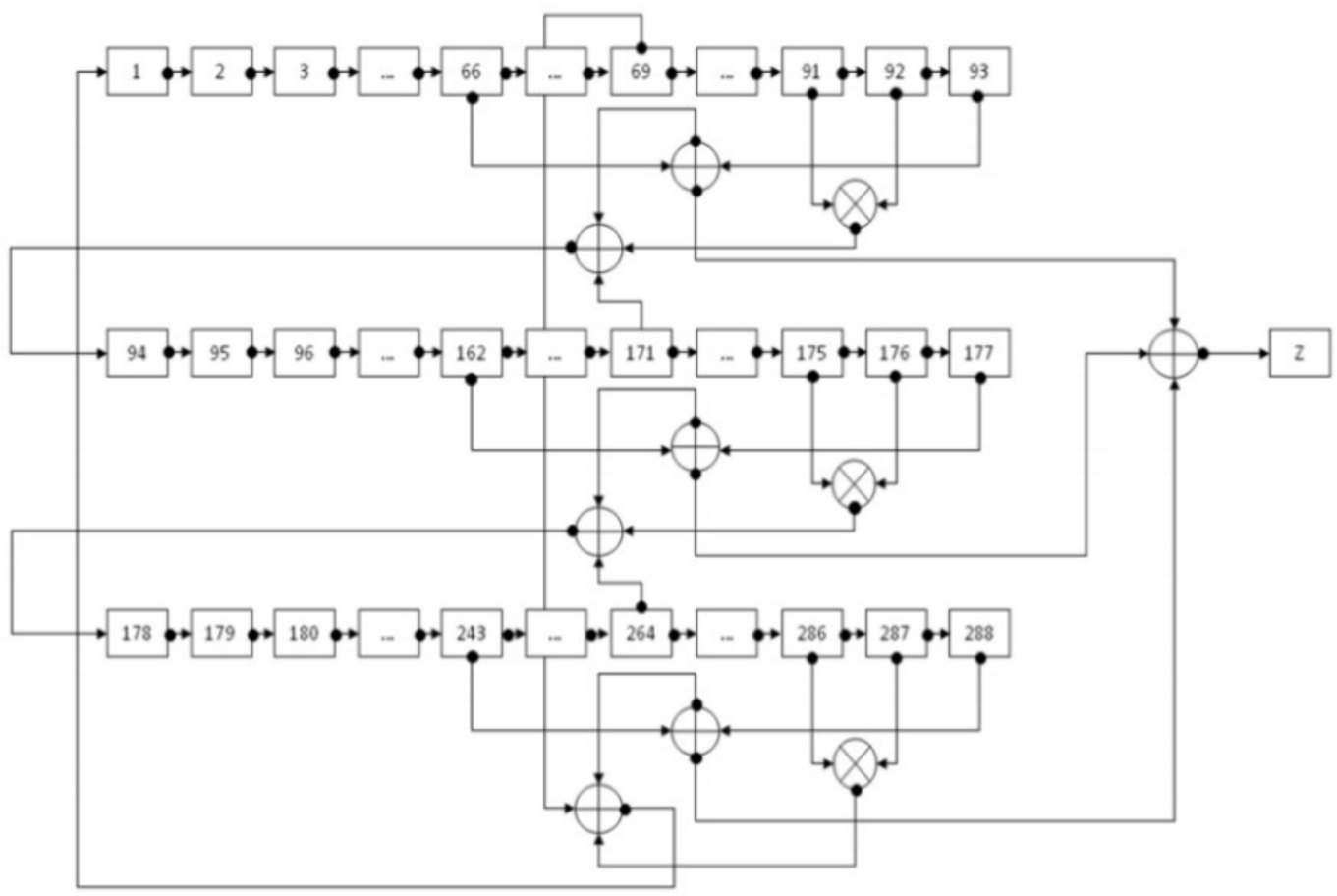


Рисунок 2.4 – Загальний вигляд алгоритму Trivium

Для початкового заповнення регістрів Trivium використовуються два джерела: секретний ключ K, а також ініціалізуючий вектор IV. Розміри ключа та ініціалізующого ветору становлять 80 біт.

Робота алгоритму Trivium полягає в наступному. Перед генерацією псевдослучайной послідовності Z, необхідно провести процедуру ініціалізації, яка полягає в тому, що на початку регістри Trivium заповнюються битами з секретного ключа K і не започатковано вектора IV.

Після цієї процедури відбувається виконання циклу довжиною в 288 * 4 раз алгорітмаTrivium, без генерації Z. Остання процедура необхідна для того, щоб кожен біт початкового стану регістрів залежав від кожного біта IV і К. Це досягається при виконанні двох повних циклів (288 * 2 раз), інші два циклу необхідні для ускладнення взаємозв'язків бітів регістра. На рисунку 2.5 наочно зображена блок-схема процедури ініціалізації початкового стану регістрів алгоритму Trivium.

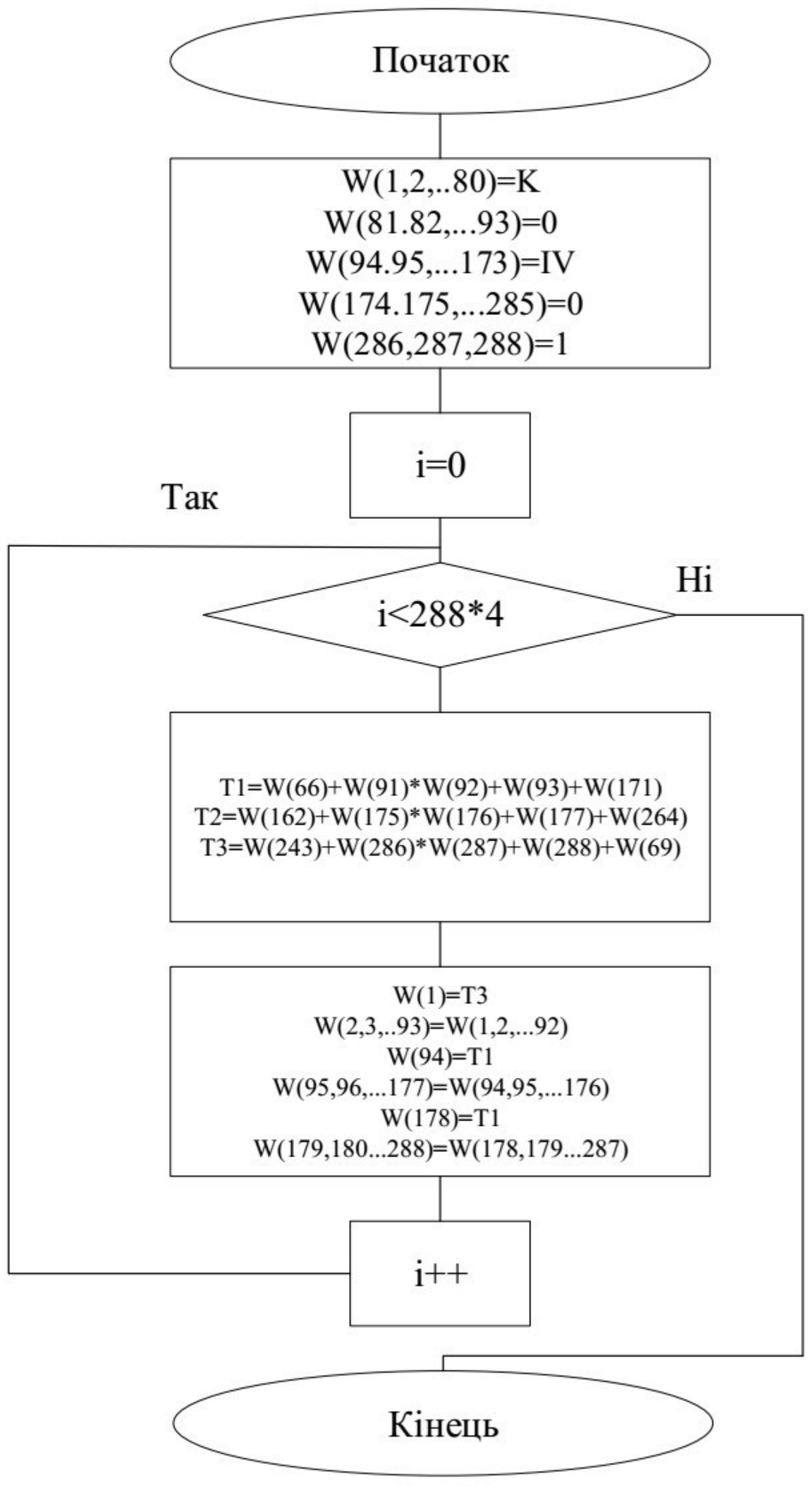


Рисунок 2.5 – Ініціалізація початкового стану

У ролі W виступають біти регістрів. Як видно зі схеми, зміна станів регістрів відбувається шляхом зсуву інформації на один біт вправо в кожному з регістрів. Останні біти в регістрах використовуються в сумі по модулю два з деякими іншими битами для генерації бітів, які переміщаються в початок регістрів. Цими битами на блок-схемі є біти T1, T2 і T3. Після

проведення операції ініціалізації схема Trivium готова приступити до своє головне завдання - створення послідовності Z. На рисунку 2.6 зображена блок-схема, що показує генерацію послідовності.

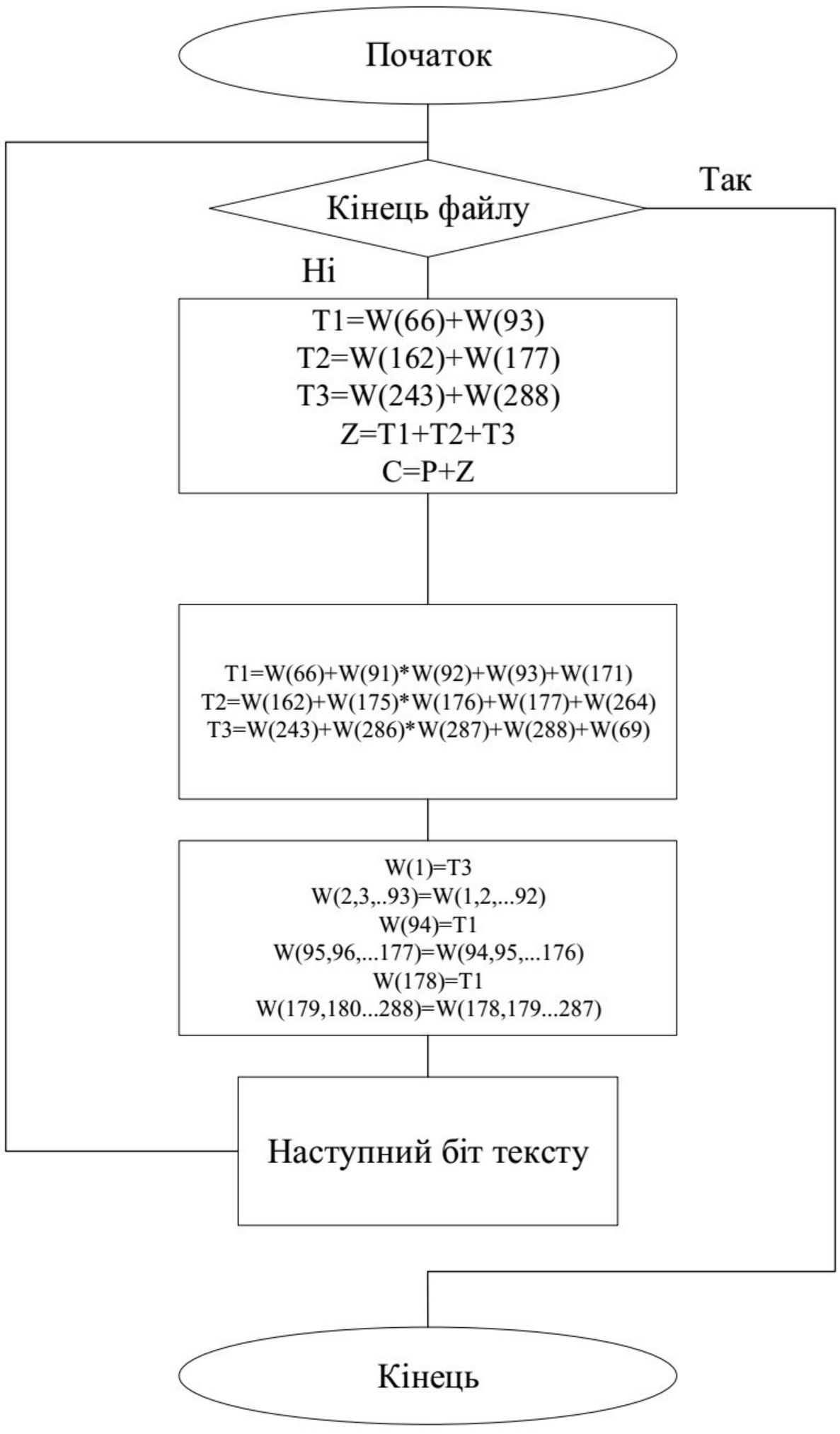


Рисунок 2.6 – Генерація послідовності Z

Хід роботи Trivium не надто змінюється по відношенню до процесу ініціалізації. Єдиною відмінністю є те, що на кожному такті виконання алгоритму генерується один біт послідовності Z, який являє собою суму по модулю два шести бітів регістрів (по два з кожного регістру). Номери бітів беруть участь в генерації Z, - 66, 93, 162, 177, 243, 288. На блок-схемі біти відкритого тексту позначаються P, а зашифрованного - C.

2.6 QUARK гешування

Для реалізації програмного засобу у магістерській кваліфікаційній роботі обрано алгоритм гешування QUARK, оскільки даний алгоритм гешування є надійним і стійким до зламу, а популярні алгоритми SHA-2 та MD5 мають проблеми з надійністю та не являються малоресурсними. Принципе роботи алгоритму QUARK зображено на рисунку 2.7:

Рисунок 2.7 – Принцип роботи алгоритму QUARK

QUARK - це гешування з апаратно орієнтованою перестановкою, яка була зроблена під впливом легких блокових шифрів KTANTAN і KATAN, та апаратно-орієнтованим потоковим шифром Grain. Найменша версія, довжиною 136 біт називається U-QUARK, середня, довжиною 176 біт - D-QUARK, а найдовша, довжино 256 біт - S-QUARK.

Функція оновлення відображає елемент від $\{0,1\}^b$ to $\{0,1\}^b$, який завантажує кожну половину у виразний NSFR довжиною b/2, а потім тактує це 4xb рази. NSFR з'єднані один з одним і невеликим журналом LFSR довжини (4b), (див. Малюнок збоку). Функції f, g і h - булеві функції, обрані через їх нелінійність, стійкість, алгебраїчну ступінь та щільність. f і g однакові для всіх версій і запозичені з Grain-v1, а h залежить від екземпляра.

Серед переваг даного методу хешування можливо виділити:

— Повідомлення коду аутентифікації (MAC);
— псевдовипадковий генератор;
— потоковий шифр;
— шифр потоку випадкового доступу;
— ключова функція виведення.

Крім того, екземпляри Quark можуть бути легко модифіковані для роботи в дуплексній конструкції, щоб дозволити реалізацію функцій як аутентифікованого шифрування або повторно завантажуваних генераторів.

2.7 Формування структури захисту

За результатами здійсненого аналізу інформаційних джерел можна зробити висновок, що одним з недоліків Wi-Fi є те, що в мережу можливо проникнути відносно легко. Основними аспектами таких проблеми є:

– неможливість керування мережею;
– відсутність контролю за користувачами в мережі;
– відносна простота взламу мережі;

Для доступу користувачів до мережі необхідна процедура однозначної ідентифікації. З оглядом на вищезазначені факти, структура системи моніторингу, яка реалізується у магістерській роботі, буде мати наступний вигляд(рис. 2.8):

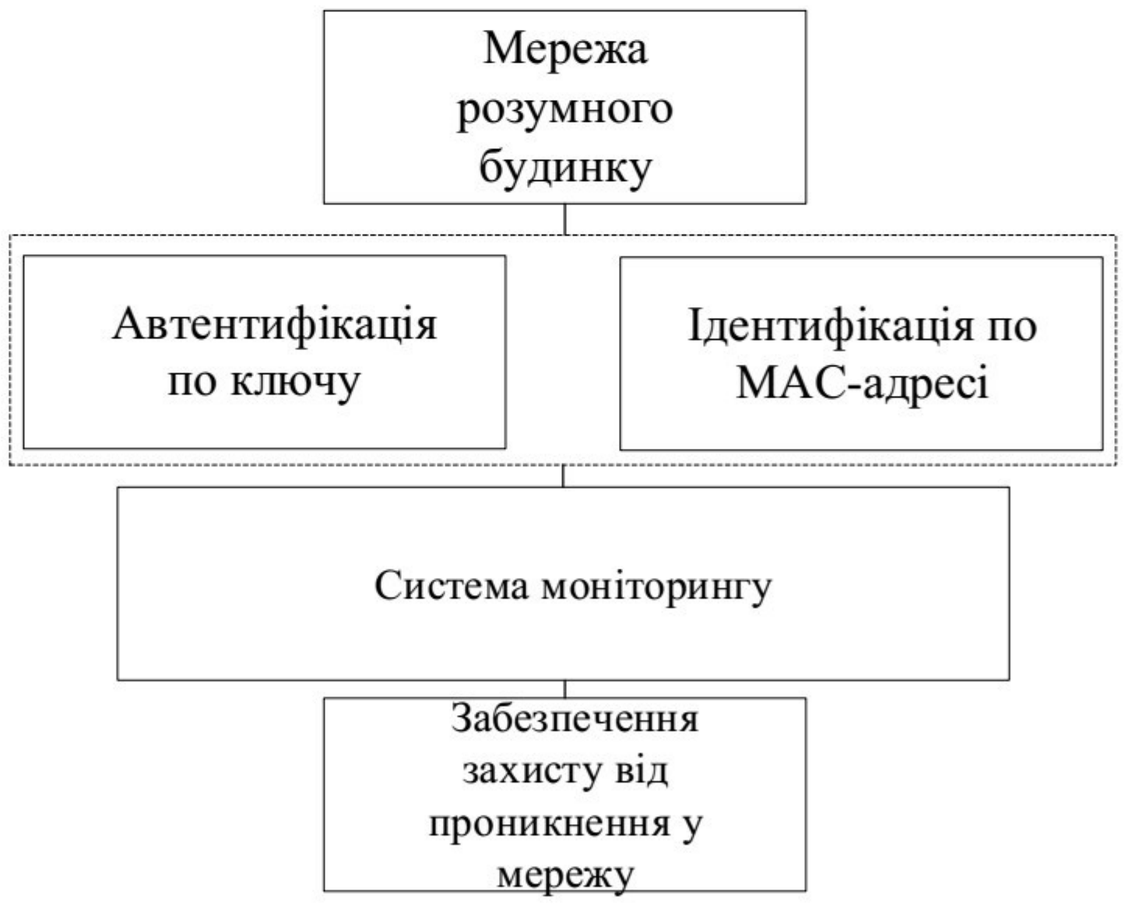


Рисунок 2.2 – Складові розроблюваної системи моніторингу

Для забезпечення захисту в системі моніторингу використовується потоковий шифр Trivium. Серед переваг не можна не зазначити гнучку рівновагу між швидкістю роботи і кількістю елементів, а також можливість досить ефективної програмної реалізації.

3 ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

3.1 Налаштування середовища для запуску системи моніторингу

Система моніторингу буде розроблена для використання у домашніх мережах, а саме для мереж на основі яких будується “розумний будинок”. За операційну систему для серверу було обрано Ubuntu. Дана ОС налічує кілька редакцій: серверна версія, десктопна версія, версія для хмарних інфраструктур. У версій для робочого столу є свої редакції в залежності від оточення. Залежно від релізу є версії з короткостроковій або довгостроковій підтримкою.

Ubuntu Server встановлюється без графічного інтерфейсу. Для інсталіції можна скористатися тільки можливостями клавіатури без використання мишки. Обидві версії і серверна і десктопна починаючи з Ubuntu 12.04 використовують одне ядро Linux. Завдяки цьому користувачі можуть ставити необхідні пакети в будь-яку з редакцій системи і налаштовувати її під будь-які завдання. Наприклад, якщо у встановлена Ubuntu Server і користувачу важко працювати з командним рядком, можливо встановити графічний інтерфейс. Також, відомо, що є певні терміни підтримки релізів Ubuntu. Ubuntu 18.04 буде підтримуватися протягом 10 років.

Було обрану серверну редакцію, тому що у роботі з віддаленими пристроями перш за все потрібна швидкість та стабільність роботи. Якщо користувачу буде не зручно працювати з командним рядком, завжди є можливість встановити графічну оболочку.

На рисунку 3.1 зображено загальний вигляд ОС

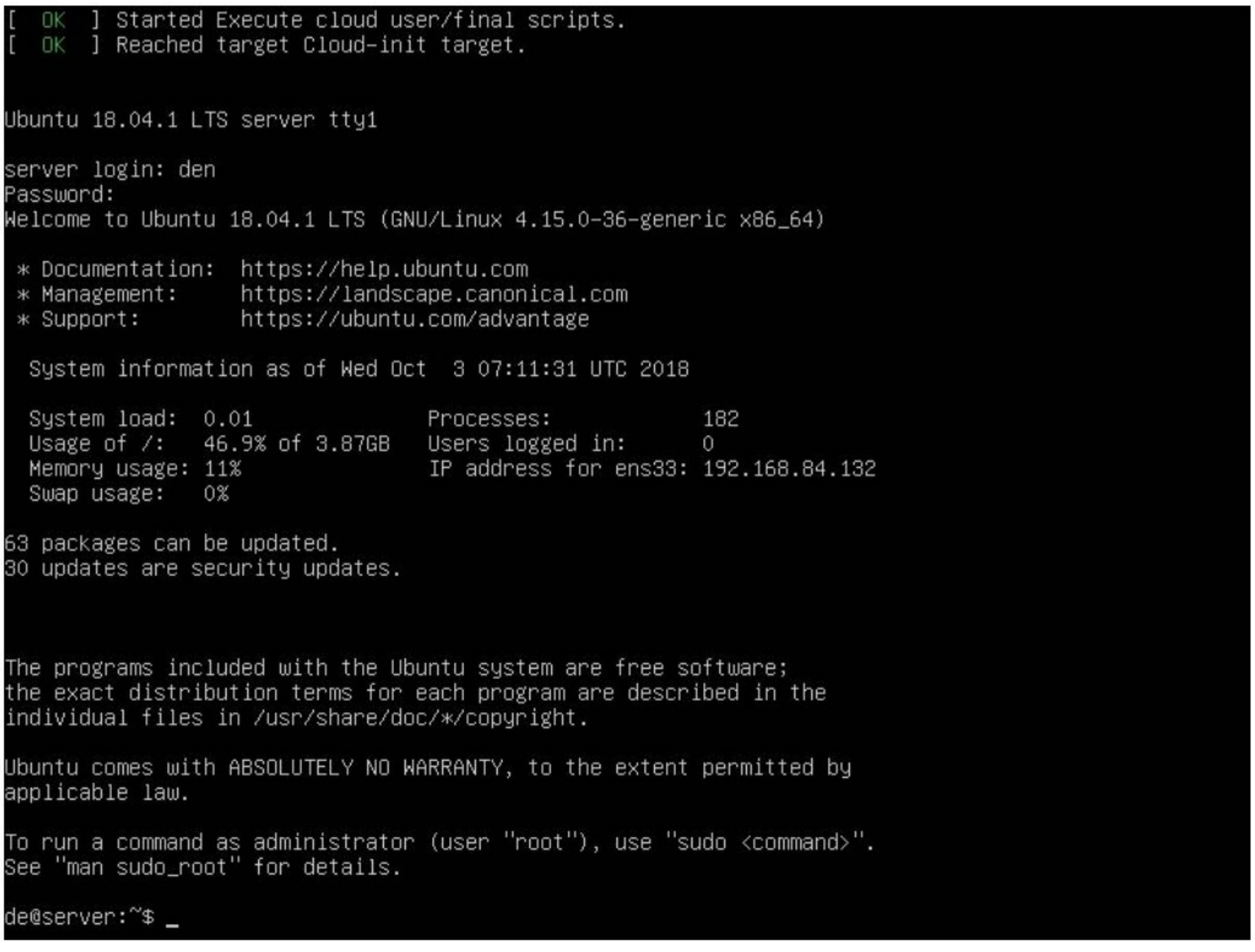


Рисунок 3.1 – Загальний вигляд ОС

Безпосередньо в ОС встановлюється система моніторингу, а також додаток, який надає новим пристроям електронний цифровий підпис. Системою моніторингу було обрано Zabbix. Серед переваг цієї системи моніторингу є те, що можливо використовувати, а також створювати власні агенти, які будуть збирати та опрацьовувати необхідну інформацію. Zabbix агенти встановлюються на цілях для активного моніторингу локальних ресурсів цих цілей, а також різноманітних додатків. Агент локально збирає оперативну інформацію і відправляє дані на сервер Zabbix для її подальшої обробки.

Також, на сервері використовується додаток, який видає електронний цифровий підпис для розумних пристроїв. Реалізація цифрового підпису відбувається за допомогою малоресурсної криптографії, а саме: гешування та малоресурсного шифру Trivium.

Для реалізації серверної частини потрібно мати пристрій, який буде у цілодобовому режимі мати доступ до мережі розумного будинку. При виконанні магістерської кваліфікаційної роботи сервером було обрано

ноутбук на базі операційної системи Ubuntu Server 18.04. Дослідження відбувались на прикладі точки доступу UniFi .

3.2 Розробка системи моніторингу

Розроблена система моніторингу заснована на взаємодії клієнта з сервером. Так як сервер має значно більшу обчислювальну потужність, на нього можливо перенести усі розрахунки пов’язані з присвоєнням Електронного цифрового підпису. Тобто, при підключені нового пристрою сервер автоматично генерує ЕЦП та надає його вищезазначеному пристрою, а також роутеру. Розділення на модулі дозволяє ефективніше використовувати ресурси системи моніторингу. На рисунку 3.2 наведено складові які використовуються на стороні серверу та роутеру.

Рисунок 3.2 – Складові на стороні серверу та роутеру.

Безпосередньо в засобі для моніторингу використовуються наступні модулі(рис 3.3):

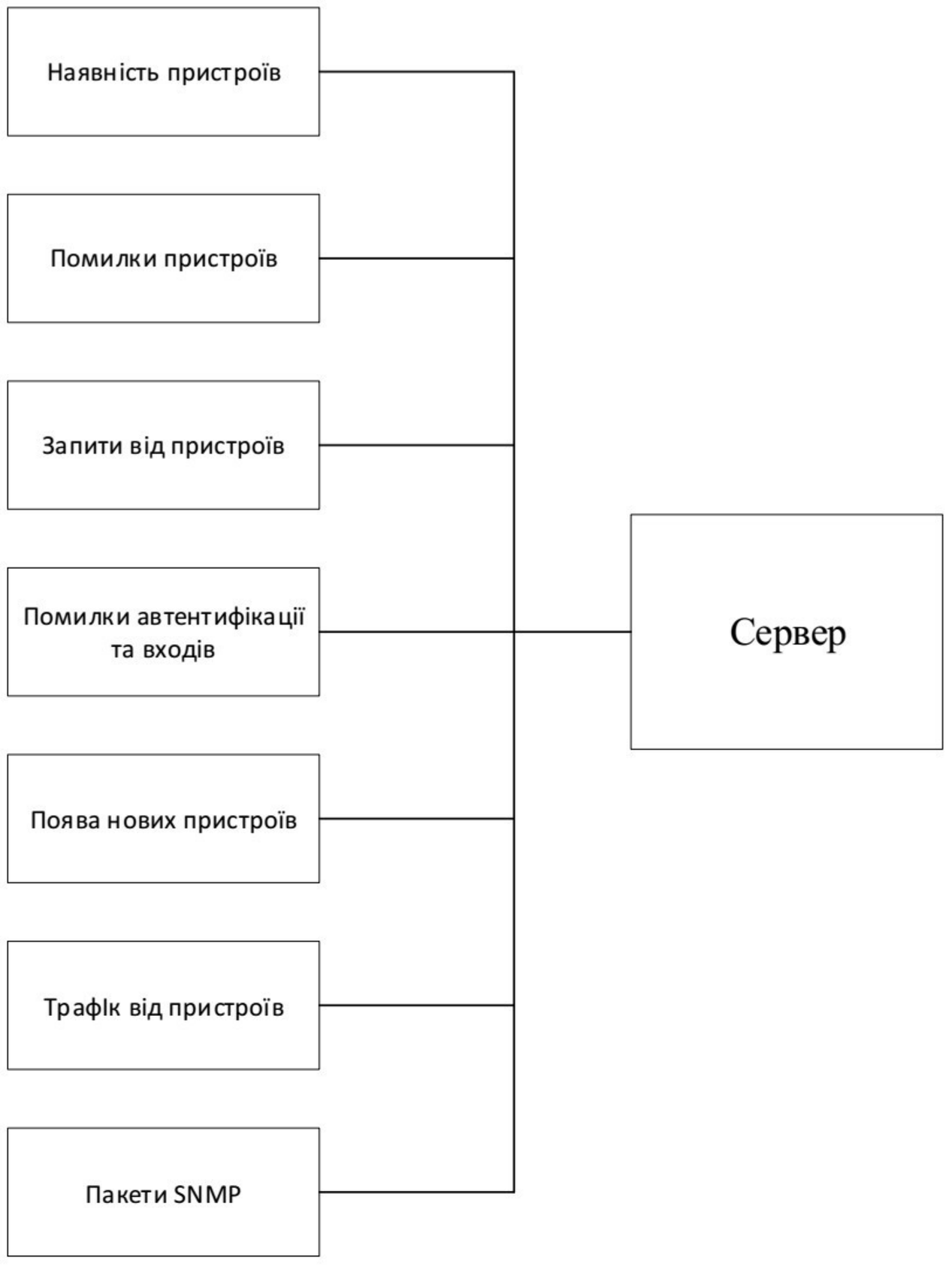


Рисунок 3.3 – Модулі системи моніторингу

Модуль наявності пристроїв перевіряє, чи підключені всі автентифіковані пристрої; модуль помилок веде логування помилок на стороні пристроїв; модуль запитів перевіряє аномальні дії з боку пристроїв; модуль помилки та автентифікації відображує кількість невдалих спроб автентифікації від пристрою; модуль появи нових пристроїв перевіряє мережу на підключення нових пристроїв; модуль трафіку перевіряє кількість пакетів надісланих та прийнятих пристроєм; модуль SNMP використовується для керування мережевими пристроями.

Роботу системи моніторингу показано на рисунку 3.4:

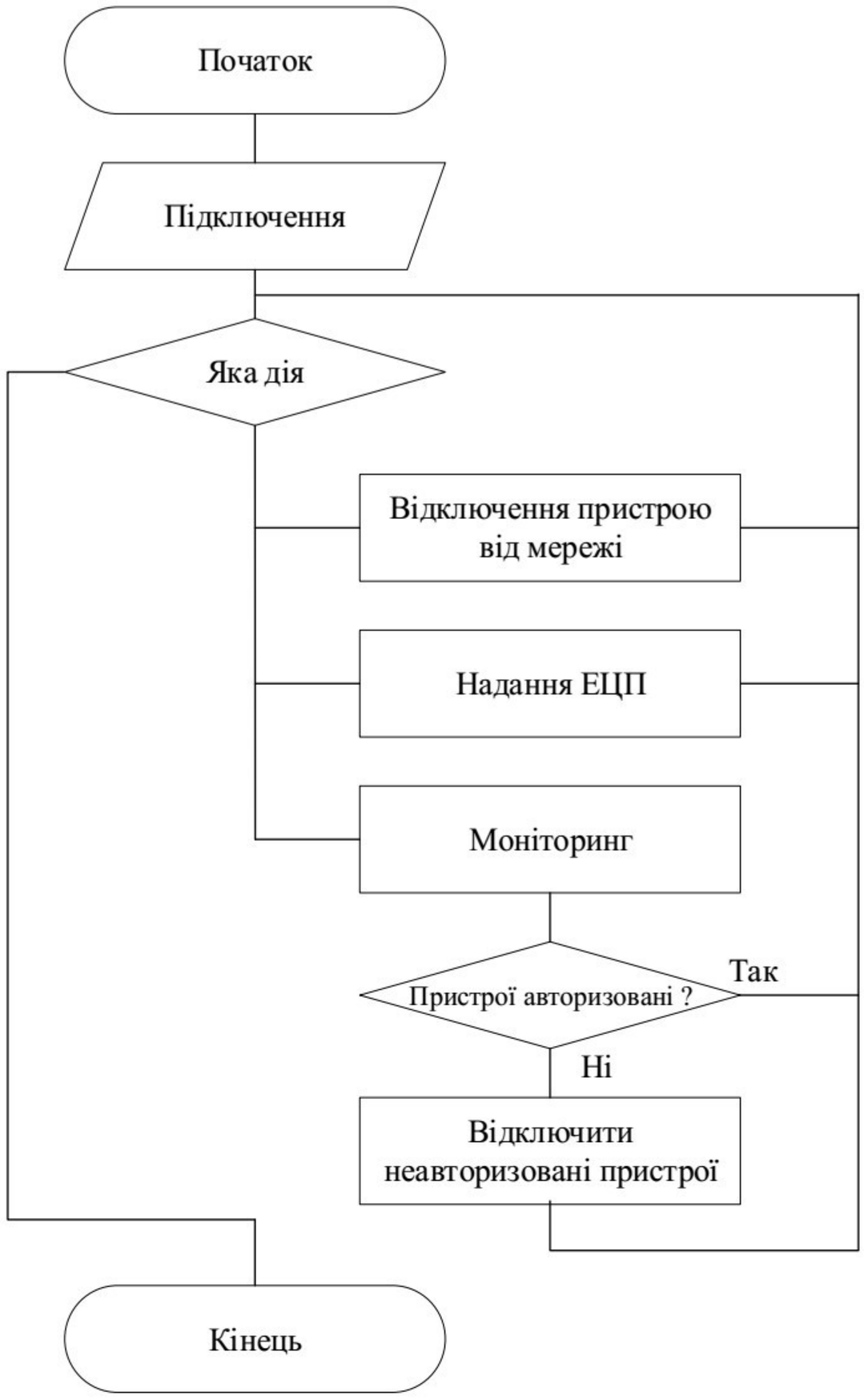


Рисунок 3.4 – Загальна схема роботи системи моніторингу

Після запуску системи моніторингу користувачу потрібно автентифікувати себе. Після автентифікації він переходить до меню, в якому у нього є можливість обрати одну з наступних дій: надати ЕЦП новому пристрою, відключити існуючи пристрої від мережі, або ж перейти в меню моніторингу, де можливо переглянути усі авторизовані прострої які перебувають у мережі. Якщо будуть виявлені пристрої, які перебувають у мережі але вони не є автентифікованими, або їх автентифікація відбулася з помилкою, їх можливо відключити.

3.3 Реалізація електронного цифрового підпису

Електронний цифровий підпис підтверджує достовірність і цілісність документа. Якщо в документ в процесі пересилки були внесені які-небудь зміни, нехай навіть зовсім незначні, то підміна виявиться. Сертифікат відкритого ключа містить персональну інформацію про власника, що дозволяє однозначно ідентифікувати автора документу. Модуль надання ЕЦП в системі моніторингу зображено на рисунку 3.5:

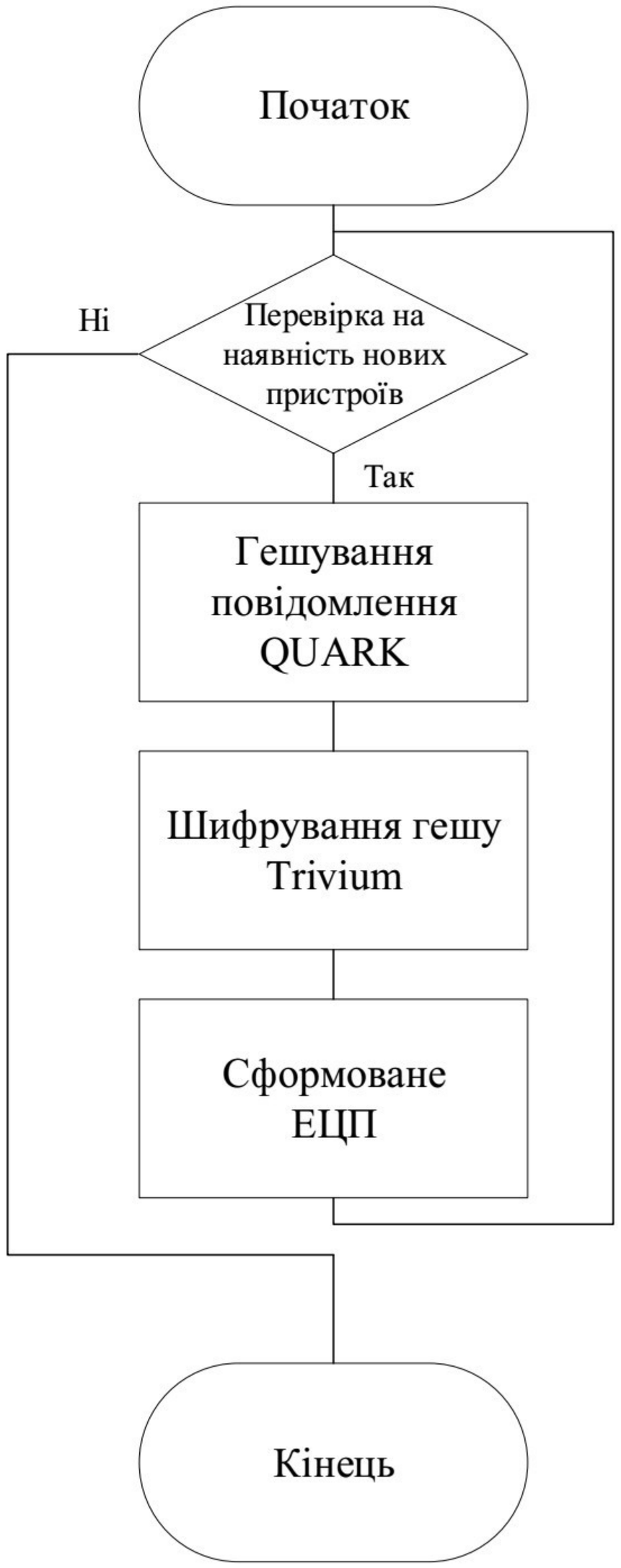


Рисунок 3.5 – Схема роботи модулю присвоєння ЕЦП

Модуль створює токен, який гешується за допомогою мало ресурсного алгоритму QUARK, після чого відбувається шифрування гешованого повідомлення мало ресурсним шифром Trivium. Сформоване ЕЦП додаємо до пакету. Таким чином відбувається автентифікація в системі моніторингу.

Отже розроблено алгоритми які мають змогу вровадити автентифікацію пристрою, а також провести перевірку автентифікації у мережі “розумний будинок”.

4 ЕКОНОМІЧНА ЧАСТИНА

В магістерській кваліфікаційній роботі розробляються методи моніторингу захисту розумного будинку та засіб, який реалізує ці запропоновані методи.

В економічній частині магістерської кваліфікаційної роботи буде виконано такі етапи робіт:

– оцінювання комерційного потенціалу розробки;

– прогнозування витрат на виконання наукової роботи та впровадження її результатів;

– прогнозування комерційних ефектів від реалізації результатів розробки;

– розрахунок ефективності вкладених інвестицій та період їх окупності.

4.1 Оцінювання комерційного потенціалу розробки

Об’єктом дослідження магістерської кваліфікаційної роботи є метод моніторингу безпеки розумного будинку.

Для проведення технологічного аудиту було залучено трьох незалежних експертів: Войтович Олеся Петрівна, Каплун Валентина Аполінаріївна, Куперштейн Леонід Михайлович. Войтович О.П .- к.т.н. ст. вик. кафедри ЗІ, Каплун В.А. – ст. вик. Кафедри ЗІ, Куперштейн Л.М. – к.т.н., доц. кафедри ЗІ. Кожен з експертів повинен ознайомитися з запропонованою розробкою, та заповнити таблицю, яка визначає рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можливу оцінку в балах. Після виконання цього, підраховується середньоарифметична сума балів та визначається який рівень комерційного потенціалу має нова розробка.

Здійснюємо оцінювання комерційного потенціалу розробки за 12-ю критеріями, наведеними в табл 4.1

Таблиця 4.1 – Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає

Продовження таблиці 4.1

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років.Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки пові-домлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання комерційного потенціалу розробки наведено в табл 4.2.

Таблиця 4.2 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали експерта		
	Войтович О.П.	Каплун В.А.	Куперштейн Л.М.
	Бали, виставлені експертами:		
1	3	4	4
2	2	2	2
3	3	4	3
4	2	3	3
5	3	3	2
6	1	1	2
7	3	2	3
8	4	4	4
9	4	4	4
10	4	4	3
11	4	4	4
12	4	4	4
Сума балів	$СБ_1$=37	$СБ_2$=39	$СБ_3$=38
Середньоарифметична сума балів СБ́	$СБ = \frac{\sum_1^i СБ_i}{i} = \frac{37+39+38}{3} = 38$		

Отже, з отриманих даних таблиці 4.2 видно, що середньоарифметична сума балів дорівнює 38, тобто нова розробка має рівень комерційного потенціалу вище середнього.

На ринку майже не існує засобів для розподілу секретної візуальної інформації. Тому є гостра необхідність в розробці нових методів та засобів для розподілу секретного вмісту зображень. Також існуючі методи мають недоліки пов’язані з неповним відновленням інформації і складними математичними обрахунками в ході роботи. А за результатами проведеного дослідження розроблений метод і засіб позбавлений цих недоліків.

4.2 Прогнозування витрат на виконання науково-дослідної роботи та конструкторсько-технологічної роботи

Для розробки нового програмного продукту необхідні такі витрати [21]:

– основна заробітна плата для розробника продукту;
– розрахунок загальних витрат на виконання даного продукту.

Основна заробітна плата для розробників визначається за формулою :

$$З_о = \frac{M}{T_р}\ t, \qquad (4.1)$$

де M – місячний посадовий оклад конкретного розробника;

$T_р$ – кількість робочих днів у місяці, $T_р = 21$ день;

t – число днів роботи розробника.

Розрахунки заробітних плат для керівника і програміста наведені в таблиці 4.1.

Таблиця 4.1 – Розрахунки основної заробітної плати

Працівник	Оклад М, грн.	Оплата за робочий день, грн.	Число днів роботи, t	Витрати на оплату праці, грн.
Науковий керівник	10000	476	7	3332
Інженер-програміст	5000	238	20	4760
Всього:				8092

Розрахуємо витрати на основну заробітну плату. Витрати на основну заробітну плату операторів розраховуються за формулою:

$$З_р = \sum_{i=1}^{n} t_i \cdot C_i\,, \qquad (4.2)$$

де n – число робіт по видах та розрядах;

t_i – норма часу (трудомісткість) на виконання конкретної роботи, годин;

C_i – погодинна тарифна ставка робітника відповідного розряду, який виконує дану роботу, яка визначається за формулою:

$$C_i = \frac{M_m \cdot K_i}{T_p \cdot T_{зм}}, \quad (4.3)$$

де M_m – мінімальна місячна оплата праці. M_m = 4173 грн.;

K_i – тарифний коефіцієнт робітника першого розряду. K_i = 1,0;

T_p – число робочих днів в місяці; приблизно T_p = 21 день;

$T_{зм}$ – тривалість зміни ($T_{зм}$ = 8 год.).

Отже, значення ставки:

$$C_i = (4173 \cdot 1{,}0) / (21 \cdot 8) = 24{,}83 \text{ (грн./год.)}.$$

В таблиці 4.2 наведено розрахунок витрат на основну зарплату.

Таблиця 4.2 – Розрахунок витрат на основну зарплату

Робітники	Трудомісткість год.	Розряд роботи	Погодинна ставка, грн..	Величина оплати, грн.
Оператор з підготовки носіїв	0,07	1	24,83	0,6

Додаткова заробітна плата $З_д$ операторів і розробників розраховується як 10…12% від основної заробітної плати операторів і розробників, а саме:

$$З_д = (0{,}12+8092) \cdot 0{,}1 = 809{,}2 \text{ (грн.)}.$$

Нарахування на заробітну плату $Н_{зп}$ розраховується як 22% від суми основної та додаткової заробітної плати:

$$H_{зп} = (З_о + З_р + З_д)\frac{\beta}{100}, \quad (4.4)$$

Значення нарахування дорівнює [12]

$$H_{зп} = (0{,}6 + 8092 + 809{,}2)8901 \cdot 22/100 = 3337{,}87 \text{ (грн.)}.$$

Розрахунок амортизаційних витрат для комп'ютера, вартість якого становить 10000 грн, а термін використання 1 місяць. Амортизаційні відрахування для комп'ютера розраховуються за такою формулою:

$$A = \frac{Ц}{T} \cdot \frac{T_в}{12}, \quad (4.5)$$

де $Ц$ – балансова вартість обладнання, грн;

T – термін використання (T = 1 міс.).

$T_в$ – корисний час використання ($T_в$ для комп'ютера становить 2 роки).

Отже, розрахуємо амортизаційні відрахування:

$$A = \frac{10000}{1} \cdot \frac{2}{12} = 1666{,}66 \text{ (грн.)}.$$

Витрати на матеріали розраховуються за формулою:

$$M = \sum_{i=1}^{n} H_i Ц_i К_i - \sum_{i=1}^{n} B_i Ц_в, \quad (4.6)$$

де H_i – витрати матеріалу i-го найменування, кг;

$Ц_i$ – вартість матеріалу i-го найменування, грн./кг.;

$К_i$ – коефіцієнт транспортних витрат, $К_i$ = (1,1…1,15);

B_i – маса відходів матеріалу i-го найменування, кг;

$Ц_в$ – ціна відходів матеріалу i-го найменування, грн/кг;

n – кількість видів матеріалів.

Витрати на матеріали, описані у розділі 2, зведені до таблиці 4.3.

Таблиця 4.3 – Витрати на матеріали, що були використані для розробки системи захисту.

Найменування матеріалу	Одиниці виміру	Ціна, грн.	Витрачено	Вартість витрачених матеріалів, грн.
Пачка паперу	Уп	50	1	50
Фарба для принтера	шт	200	1	200
Ручка	Шт	20	1	20
Всього				257

$$М = 257 \cdot 1,1 = 282,7 \text{ (грн.)}.$$

Розрахуємо витрати на комплектуючі.

Витрати на комплектуючі розрахуємо за формулою [12]:

$$K = \sum_{i=1}^{n} H_i \cdot Ц_i \cdot K_i, \qquad (4.7)$$

де n – кількість комплектуючих;

H_i – кількість комплектуючих i-го виду;

$Ц_i$ – покупна ціна комплектуючих i-го виду, грн;

K_i – коефіцієнт транспортних витрат ($K_i = 1,1$).

В таблиці 4.4 проведено розрахунок витрат на комплектуючі.

Таблиця 4.4 – Розрахунок витрат на комплектуючі

Найменування	Кількість	Ціна за шт., грн.	Сума, грн.
Диск CD-RW	3	10	30
Конверт для диску	3	1	3
Всього	33		

Таким чином, витрати на комплектуючі становлять:

$$K = 33 \cdot 1,1 = 36.3 \text{ (грн)}.$$

Витрати на силову електроенергію розраховуються за формулою:

$$B_e = B \cdot П \cdot Ф \cdot K_n, \quad (4.8)$$

де B – вартість 1кВт-години електроенергії (B = 2,44 грн/кВт);

$П$ – установлена потужність комп'ютера ($П$ = 0,3кВт);

$Ф$ – фактична кількість годин роботи комп'ютера ($Ф$ = 0,4 год.);

K_n – коефіцієнт використання потужності ($K_n < 1$, $K_n = 0,8$).

Потужність комп'ютера складає 230Вт/год = 0,23кВт/год + потужність на освітлення, тоді $П$ = 0,3кВт/год

$$B_e = 2.44 \cdot 0,3 \cdot 0,4 \cdot 0,8 = 0,23 \text{ (грн.)}.$$

Розрахуємо інші витрати $B_{ін}$.

Інші витрати можна прийняти як (100…300)% від суми основної заробітної плати розробників та робітників, які були виконували дану роботу, тобто [12]:

$$B_{ін} = (1..3) \cdot (З_o + З_p), \quad (4.9)$$

Отже, розрахуємо інші витрати:

$$B_{ін} = 2 \cdot (0,6+8092) = 16185,2 \text{ (грн)}.$$

Усі витрати складають

В = 8092+0,6+809,2+3337,87+1666+282,7+36,3+0,23+16185,2=30410,76 грн.

Розрахуємо загальну вартість наукової роботи $B_{заг}$ за формулою:

$$B_{заг} = \frac{B}{\alpha}, \quad (4.10)$$

Де α – частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відносних одиницях; $\alpha = 1$.

$$B_{заг} = 30410{,}76 \text{ грн.}$$

Прогнозування загальних витрат *ЗВ* на виконання та впровадження результатів виконаної наукової роботи здійснюється за формулою :

$$ЗВ = \frac{B_{заг}}{\beta}, \qquad (4.11)$$

Де β – коефіцієнт, який характеризує етап (стадію) виконання даної роботи.

Отже, розрахуємо загальні витрати

:

$$ЗВ = 30410{,}76/0{,}7 = 43443{,}94$$

Отже, загальна кількість витрат на розробку дорівнює 43443,94 грн.

4.3 Прогнозування комерційних ефектів від реалізації результатів розробки

В економічній частині магістерської кваліфікаційної обґрунтовується економічна доцільність розробки методів проведення моніторингу захисту розумного будинку. Для того щоб виконати дану розробку потрібно 74 робочих днів.

Оцінка зростання чистого прибутку підприємства від впровадження результатів наукової розробки. У цьому випадку збільшення чистого прибутку підприємства $\Delta \Pi_i$ для кожного із років, протягом яких очікується отримання позитивних результатів від впровадження розробки, розраховується за формулою:

$$\Delta П_i = \sum_{i=1}^{n} (\Delta П_я \cdot N + П_я \cdot \Delta N)_i, \qquad (4.12)$$

де $\Delta П_я$ – покращення основного якісного показника від впровадження результатів розробки у даному році;

N – основний кількісний показник, який визначає діяльність підприємства у даному році до впровадження результатів наукової розробки;

ΔN – покращення основного кількісного показника діяльності підприємства від впровадження результатів розробки;

$П_я$ – основний якісний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки;

n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки.

В результаті впровадження результатів наукової розробки витрати матеріалів на розробку алгоритму зменшаться на 200 грн (що автоматично спричинить збільшення чистого прибутку підприємства на 200 грн), а кількість користувачів збільшиться: протягом першого року – на 90 користувачів, протягом другого року – на 100 користувачів, протягом третього року – на 80 користувачів.

Реалізація продукції до впровадження результатів наукової розробки складала 400 шт., а прибуток, що його отримувало підприємство (організація) на одиницю продукції до впровадження результатів наукової розробки – 350 грн.

Спрогнозуємо збільшення чистого прибутку від впровадження результатів наукової розробки у кожному році відносно базового.

Отже, збільшення чистого продукту $\Delta П_1$ протягом першого року складатиме:

$$\Delta П_1 = 200 \times 400 + (350 + 200) \times 90 = 80000 + 550 \times 90 = 129500 \text{ (грн)}$$

Протягом другого року:

$$\Delta П_2 = 200 \times 400 + (350 + 200) \times (90 + 100) = 80000 + 550 \times 190 = 184500 \text{ (грн)}$$

Протягом третього року:

$$\Delta П_3 = 200 \times 400 + (350 + 200) \times (90 + 100 + 80) = 80000 + 550 \times 270 = 228500 \text{ (грн)}$$

Тепер можна обрахувати ефективність інвестування та її окупність.

4.4 Розрахунок ефективності вкладених інвестицій та період їх окупності

Розрахунок ефективності вкладених інвестицій передбачає проведення таких робіт:

1-й крок. Розрахуємо теперішню вартість інвестицій PV, що вкладаються в наукову розробку. Такою вартістю ми можемо вважати прогнозовану величину загальних витрат ЗВ на виконання та впровадження результатів НДДКР, розраховану раніше, тобто будемо вважати, що ЗВ = PV= 43443,94 грн.

2-й крок. Розрахуємо очікуване збільшення прибутку $\Delta П_i$, що його отримає підприємство (організація) від впровадження результатів наукової розробки, для кожного із років, починаючи з першого року впровадження. Таке збільшення прибутку також було розраховане нами раніше та становить:

$\Delta П_1 = 129500$ грн, $\Delta П_2 = 184500$ грн, $\Delta П_3 = 228500$ грн.

3-й крок. Для спрощення подальших розрахунків необхідно побудувати вісь часу, на яку наносять всі платежі (інвестиції та прибутки), що мають місце під час виконання науково-дослідної роботи та впровадження її результатів.

Якщо загальні витрати ЗВ на виконання та впровадження результатів НДДКР (або теперішня вартість інвестицій PV) дорівнюють 43443,94 грн., а результати вкладених у наукову розробку інвестицій почнуть виявлятися вже вкінці другого року впровадження. То ці результати виявляться у тому, що у першому році підприємство отримає збільшення чистого прибутку на 129500 грн. відносно базового року, у другому році – збільшення чистого прибутку на 184500 грн (відносно базового року), у третьому році – збільшення чистого прибутку на 228500 грн (відносно базового року).

Тоді рисунок, що характеризує рух платежів (інвестицій та додаткових прибутків) буде мати вигляд, наведений на рис. 4.1.

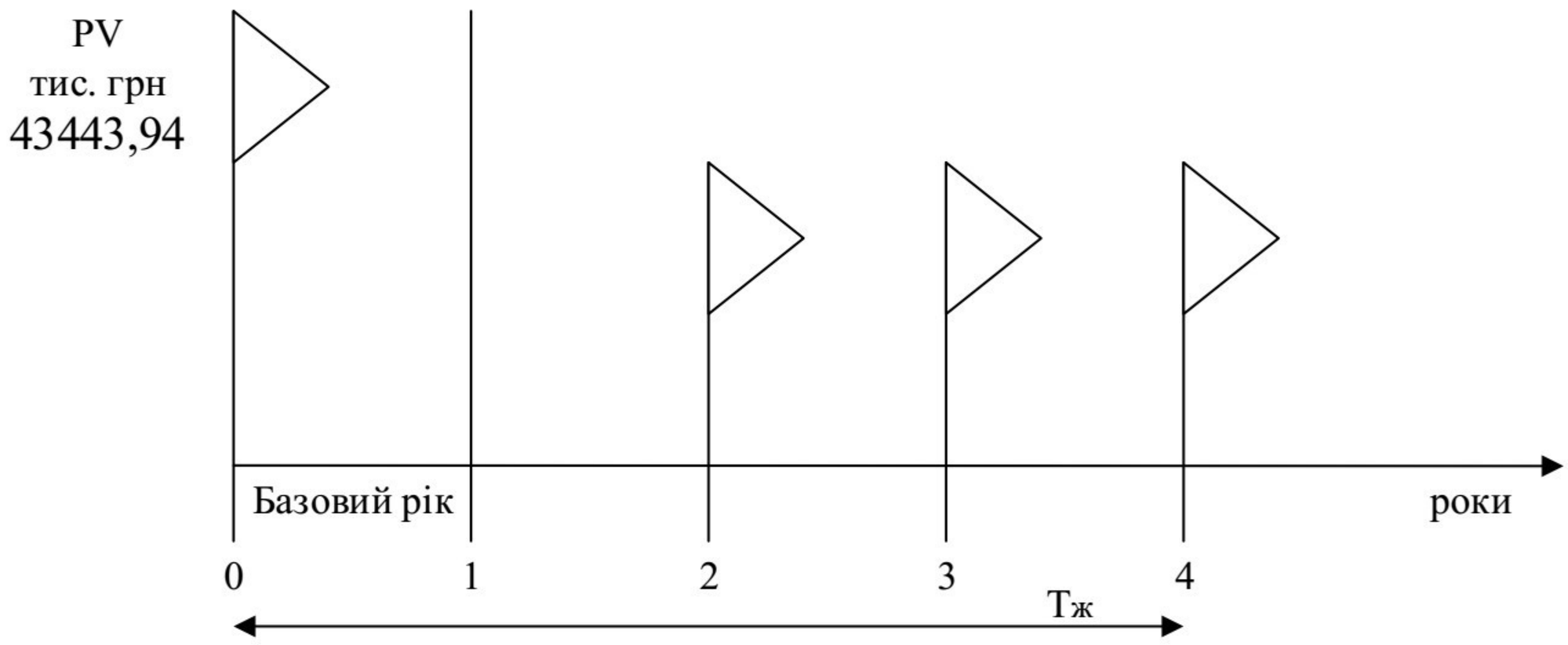


Рисунок 4.1 – Вісь часу з фіксацією платежів, що мають місце під час розробки та впровадження результатів НДДК

4-й крок. Розрахуємо абсолютну ефективність вкладених інвестицій Еабс.

Для цього скористаємося формулою:

$$Еабс = (ПП – PV),$$

де ПП – приведена вартість всіх чистих прибутків, що їх отримає підприємство (організація) від реалізації результатів наукової розробки, грн.; PV – теперішня вартість інвестицій PV = ЗВ= 43443,94 грн.

У свою чергу, приведена вартість всіх чистих прибутків ПП розраховується за формулою:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)}$$

де $\Delta П_i$– збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої НДДКР, грн;

т – період часу, протягом якого виявляються результати впровадженої НДДКР, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні; для України цей показник знаходиться на рівні 0,1;

t – період часу (в роках) від моменту отримання чистого прибутку до точки „0”.

$$ПП=\frac{129500}{(1+0,1)^2}+\frac{184500}{(1+0,1)^3}+\frac{228500}{(1+0,1)^4}=\frac{129500}{1,21}+\frac{184500}{1,331}+\frac{228500}{1,4641}=$$

$$107024,79 + 138617,58 + 156068,57 = 401710,94(грн)$$

Еабс =401710,94 – 43443,94 = 358267,81 (грн)

Оскільки Еабс > 0, то вкладання коштів на виконання та впровадження результатів НДДКР може бути доцільним.

5-й крок. Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій Ев. Для цього використаємо формулу:

$$E_в = \sqrt[Т_ж]{1+\frac{E_{абс}}{PV}-1},$$

де Еабс – абсолютна ефективність вкладених інвестицій, грн; PV – теперішня вартість інвестицій PV = ЗВ, грн; Тж – життєвий цикл наукової розробки, роки.

Далі, розрахована величина Ев порівнюється з мінімальною (бар'єрною) ставкою дисконтування $\tau_{мін}$, яка визначає ту мінімальну дохідність, нижче за яку інвестиції вкладатися не будуть. У загальному

вигляді мінімальна (бар'єрна) ставка дисконтування $\tau_{\text{мін}}$ визначається за формулою:

$$\tau = \text{d} + \text{f}$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2019 році в Україні d = (0,14...0,2); f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,1), але може бути і значно більше.

Якщо величина Ев > $\tau_{\text{мін}}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки. В іншому випадку фінансування наукової розробки здійснюватися не буде.

Спочатку спрогнозуємо величину $\tau_{\text{мін}}$. Припустимо, що за даних умов

τ мін = 0,15 + 0,05 = 0,2.

Тоді відносна (щорічна) ефективність вкладних інвестицій в проведення наукових досліджень та впровадження їх результатів складе:

$$\text{E}_\text{в} = \sqrt[4]{1 + \frac{358267,81}{160000,13}} - 1 = \sqrt[4]{1 + 1,51} - 1 = \sqrt[4]{2,51} - 1 = 1,26 - 1 =$$

0,26 або 26%.

Оскільки Ев = 26% > $\tau_{\text{мін}}$= 0,2 = 20%, то інвестор буде зацікавлений вкладати гроші в дану наукову розробку.

6-й крок. Розраховують термін окупності вкладених у реалізацію наукового проекту інвестицій. Термін окупності вкладених у реалізацію наукового проекту інвестицій Ток можна розрахувати за формулою:

$$\text{T}_\text{ок} = \frac{1}{\text{E}_\text{в}}.$$

Якщо Ток < 3…5-ти років, то фінансування даної наукової розробки в принципі є доцільним. В інших випадках потрібні додаткові розрахунки та обґрунтування.

$$\text{T}_\text{ок} = \frac{1}{0,26} = 3,8 \text{ року}$$

Ток < 5 років, що свідчить про доцільність фінансування даної наукової розробки.

Обрахувавши термін окупності даної наукової розробки (0,9 років), можна зробити висновок, що фінансування даної наукової розробки буде доцільним.

Рівень комерційного потенціалу засобу моніторингу розумного будинку є вище середнього. Загальні витрати на створення нового програмного продукту склали 43443,94 грн. Вартість чистого прибутку від впровадження даної розробки за 3 років складиме . Показники ефективності показують, що даний метод є доцільним і буде цікавий для інвестора.

.

ВИСНОВОК

У магістерській кваліфікаційній роботі проведено науково-досліджене обґрунтування необхідності моніторингу захисту розумного будинку.

Отже, досліджено проблеми безпеки мережі розумного будинку, в яких показано наявну проблему в забезпеченні безпеки. Проаналізовано такі методи захисту як: фізичний та програмний захист розумного будинку, в результаті чого, було виявлено, що захисту на рівні мережі майже не відбувається. Здійснено огляд етапів та методів впровадження захисту.

Проаналізовано відомі схеми “розумного будинку” досліджено методи їх побудови та аналізу. Для впровадження захисту було обрано децентралізовану схему мережі “розумного будинку”.

Розглянуто сучасні методи моніторингу, а також додатки, які впроваджують дані методи. Як метод захисту в бездротовій мережі було прийнято рішення використовувати Електронний Цифровий Підпис на базі малоресурсного шифрування.

Проведено економічний розрахунок витрат, необхідних на розробку програмних засобів, що реалізують запропоновані методи впровадження моніторингу. Проведено розрахунок необхідних інвестицій та визначено термін їх окупності. Визначено, що така розробка доцільна та приверне увагу інвесторів.

Таким чином, усі задачі магістерської кваліфікаційної роботи розв’язані і досягнуто сформульованої мети дослідження.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Умные и опасные ? [Електроний ресурс] – Режим доступу: http://internetinside.ru/umnye-i-opasnye-voprosy-bezopasnosti-i/ – Назва з екрану

2. Сложности и риски умного дома [Електроний ресурс] – Режим доступу: https://tech-house.su/slozhnosti-i-riski-umnogo-doma/. – Назва з екрану

3. Cherryhome [Електроний ресурс] – Режим доступу: https://cherryhome.ai/technology – Назва з екрану

4. IoT: Вопросы безопасности умного дома [Електроний ресурс] – Режим доступу https://habr.com/ru/company/gsgroup/blog/394343/ – Назва з екрану

5. What is thread? [Електроний ресурс] – Режим доступу: https://www.threadgroup.org/What-is-Thread/Overview – Назва з екрану

6. Умный дом. Послушный дом [Електроний ресурс] – Режим доступу: https://www.apple.com/ru/ios/home/– Назва з екрану

7. Safer, smarter homes start with Z-Wave [Електроний ресурс] – Режим доступу: https://www.z-wave.com/ – Назва з екрану

8. Z-Wave [Електроний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Z-Wave – Назва з екрану

9. J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang. "SAVE: Source address validity enforcement protocol." In proceeding of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002), vol. 3, pp. 1557 – 1566, 2002.

10. Дональд Э. Кнут. Глава 3. Случайные числа // Искусство программирования = The Art of Computer Programming. — 3-е изд. — М.: Вильямс, 2000. — Т. 2. Получисленные алгоритмы. — 832 с.

11. Кельтон В., Лоу А. Имитационное моделирование. Классика CS. — 3-е изд. — СПб.: Питер, 2014. — С. 465, 466. — 487 с.

12. L'Ecuyer. Pierre Random Number Generation // Springer Handbooks of Computational Statistics : Глава. — 2007. — С. 93 - 137. — DOI:10.1002/9780470172445.ch4

13. Why you need a monitoring system [Електроний ресурс] – Режим доступу: https://pandorafms.com/blog/why-you-need-a-monitoring-system/– Назва з екрану

14. Promiscuous mode monitoring [Електроний ресурс] – Режим доступу: https://searchsecurity.techtarget.com/definition/promiscuous-mode– Назва з екрану

15. Малоресурсная криптография [Електроний ресурс] – https://studme.org/190620/informatika/maloresursnaya_kriptografiya– Назва з екрану

16. ISO / IEC FDIS 29192 [Електроний ресурс] – https://www.iso.org/standard/56552.html– Назва з екрану

17. Основы криптографии (Криптографические примитивы) [Електроний ресурс]http://cryptowiki.net/index.php?title=Часть_I._Основы_криптографии_(Криптографические_примитивы) – Назва з екрану

18. Каплун В.А., Дудатьєв А.В., Семеренко В.П., Захист програмного забезпечення, частина 1 – Вінниця, ВНТУ, 2005 – 140 с.

19. Каплун В.А., Дмитришин О.В., Баришев Ю.В. Захист програмного забезпечення, частина 2 – Вінниця, ВНТУ, 2014 – 105 с

20. Алгоритм шифрования Trivium [Електроний ресурс] https://m.studme.org/190623/informatika/algoritm_shifrovaniya_trivium– Назва з екрану

21. Методичні вказівки до виконання студентами-магістрантами наукового напряму економічної частини магістерських кваліфікаційних робіт / Уклад. В. О. Козловський – Вінниця : ВНТУ, 2012. – 22 с.

ДОДАТКИ

Додаток А
Технічне завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ, д.т.н., проф.
_____ В. А. Лужецький
_____ 2019 року

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання науково-дослідної роботи

на тему: «Система моніторингу безпеки розумного будинку»
08-20.МКР.008.00.000 ТЗ

Керівник роботи

к.т.н., доц., доц. каф. ЗІ О. П. Войтович

Вінниця 2019

1 Підстави для проведення робіт

Робота проводиться на підставі наказу ВНТУ від 2 жовтня 2019 року № 254.

Дата початку роботи 1.09.19 р.

Дата закінчення роботи 14.12.19 р.

2 Мета та призначення НДР

Метою магістерської кваліфікаційної роботи є підвищення захищеності бездротової мережі розумного будинку.

Об'єктом дослідження є процес захисту інформації за допомогою системи моніторингу на базі мало ресурсної криптографії.

Актуальність теми. Інформація має важливе значення в життєдіяльності людства. При цьому вона стає все більш вразливою через зростаючі обсяги збережених даних. Тому все більшу важливість набуває проблема захисту інформації від несанкціонованого доступу під час передачі та зберіганні. Для захисту інформації всередині мережі розумного будинку одним з найкращих варіантів є саме моніторинг мережі. Є кілька варіантів підвищення надійності безпеки "розумного будинку", фізичні та програмні. Даний метод підвищує надійність при спробі програмного втручання, але робить "розумний будинок" залежним від серверної частини на якій відбувається моніторинг. Даний метод зменшує ймовірність підміни розумного пристрою.

3 Вихідні дані для проведення НДР

НДР проводиться вперше і вихідними даними для проведення НДР є:

1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.

2. Червяков Н. И. Алгебраические и практические аспекты реализации нейросетево й порогово й схемы раделения секрета / Н. И. Червяков [та ін..] // Наука. Инновации. Технологии. – 2014. - № 2(6) – С. 14-26.

3. Введение в криптографию / Под общ. ред. В. В. Ященко. 4-е изд., доп. М.: МЦНМО, 2012. 348 с.

4. Романова Е.А., Мелешко Е.А. Методы защиты информации с использованием визуальной криптографии. [Електроний ресурс] – URL: http://www.rusnauka.com/31_ONBG_2011/Informatica/4_96500.doc.htm – Назва з титул. екрана.

4 Виконавці НДР

Студент групи БС-18м Круговий Владислав Віталійович

5 Вимоги до виконання НДР

Для захищеності секретного вмісту зображень за рахунок розподілу секрету необхідно:

- проаналізувати відомі системи моніторингу;
- проаналізувати малоресурсну криптографію
- розробити власний метод моніторингу мережі;
- розробити програмний засіб для виконання даного методу.

6 Вимоги до супровідної документації

6.1 Графічна і текстова документація повинна відповідати діючим стандартам України.

7 Етапи НДР

Робота з теми виконується у 8 етапів.

Зміст етапу	Початок	Закінчення	Очікувані результати	Звітна
Аналіз завдання. Вступ	01.09.2019	04.09.2019	Вступ	Чернетка вступу
Розробка технічного завдання	16.09.2019	22.09.2019	Технічне завдання	Проект технічного завдання
Розробка техніко-економічного та науково-технічного обґрунтування доцільності досліджень	05.09.2019	15.09.2019	Аналіз існуючих аналогів. Вибір напрямку дослідження	Чернетка першого розділу
Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	23.09.2019	29.09.2019	Аналіз відомих методів. Постановка завдання	Чернетка другого розділу
Розробка методу моніторингу мережі	30.09.2019	12.10.2019	Запропоновано метод моніторингу.	Чернетка третього розділу
Експериментальні дослідження	13.10.2019	09.11.2019	Метод, який реалізує розроблювані методи	Чернетка четвертого розділу
Розробка економічного розділу	11.11.2019	17.11.2019	Економічні показники дослідження	Чернетка з економічного розділу
Оформлення пояснювальної записки	25.11.2019	30.11.2019	Пояснювальна записка	Пояснювальна записка

8 Очікувані результати та порядок реалізації НДР

Передбачається розробка методу моніторингу безпеки розумного будинку. Заплановане створення програмного засобу, який може бути використаний у навчальному процесі.

9 Матеріали які подаються після закінчення НДР

По завершенню роботи подається пояснювальна записка та ілюстративна частина.

10 Порядок приймання НДР та її етапів

Результати роботи будуть розглядатися на засіданні ДЕК із захисту магістерських кваліфікаційних робіт.

Попередній захист та доопрацювання МКР листопад 2019 р.

Представлення МКР до захисту грудень 2019.

Захист МКР 17.12.2019

11 Вимоги до розроблення документації

Документація буде виконуватись за допомогою комп'ютерного набору у відповідності вимог ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»

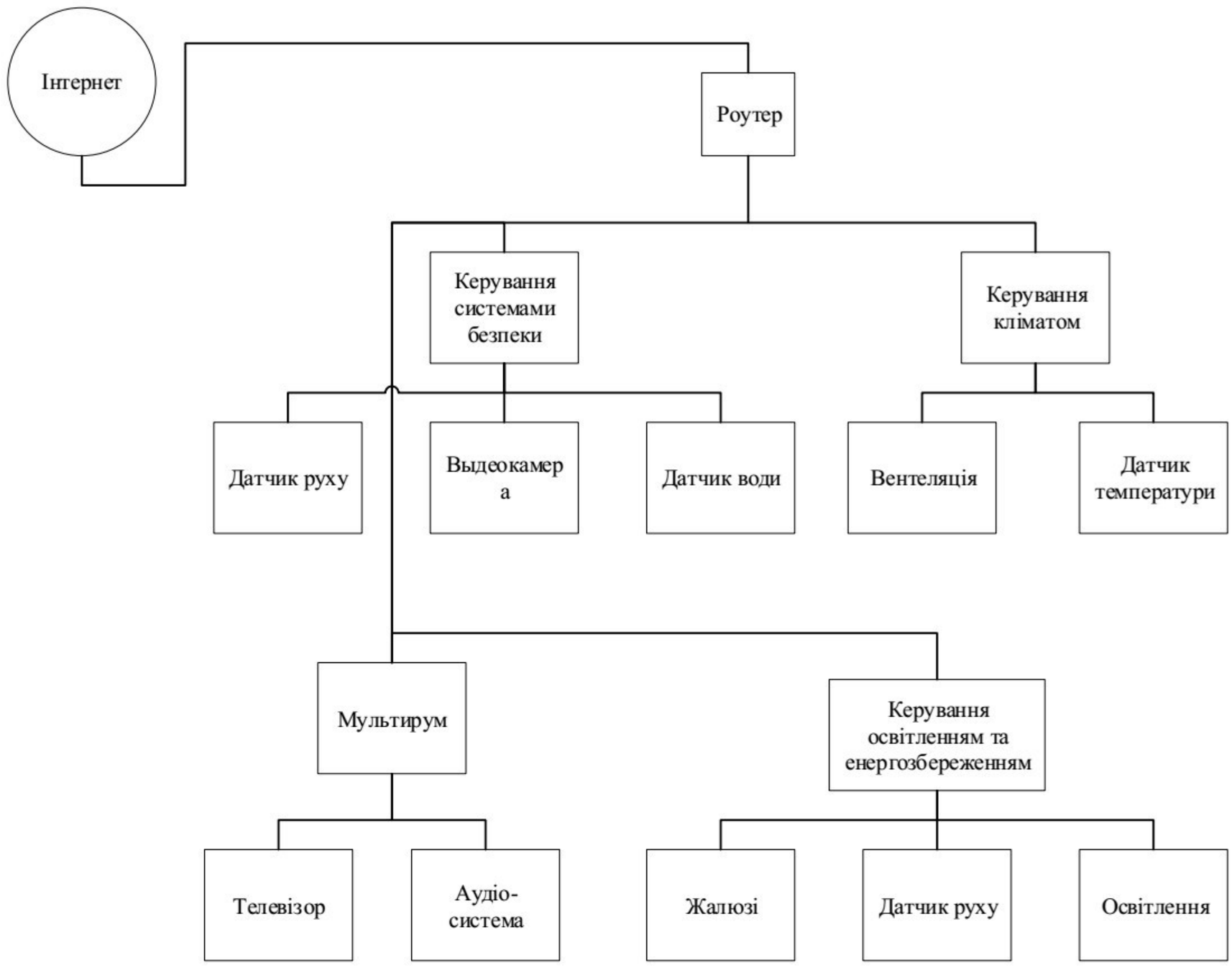
12 Вимоги щодо технічного захисту інформації з обмеженим доступом

У зв'язку з тим що дана робота не містить інформації, що потребує захисту у відповідності до законів України, заходи з її технічного захисту не передбачаються.

Розробив студент групи БС-18м _____ Круговий В. В.

ІЛЮСТРАТИВНА ЧАСТИНА

Загальна схема децентралізованої моделі розумного будинку

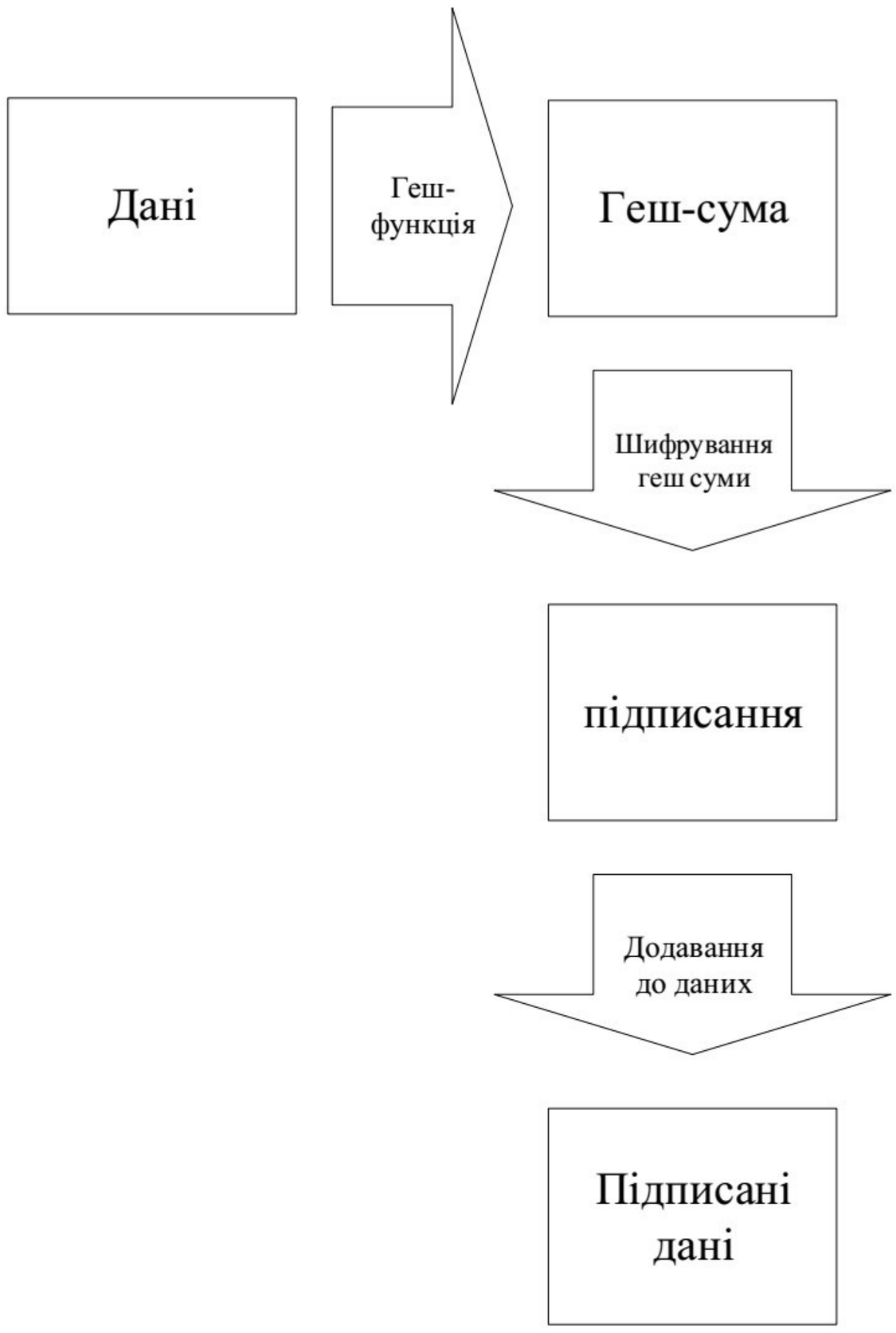


					08-20.МКР.008.00.000 ІЧ1
Змн	Арк.	№ докум.	Підпис	Дат	
Розроб.		Круговий В.В			Система моніторингу безпеки розумного будинку. Загальна схема децентралізованої моделі розумного будинку
Перевір.		Войт			
Реценз.		Крупельницький			
Н. Контр.		Войт			
Затверд.		Лужец			

Літ.	Маса	Масштаб

1 ВНТУ, ГР. БС-

Схема підписання даних



					08-20.МКР.008.00.000 ІЧ2
Змн	Арк.	№ докум.	Підпис	Дат	
Розроб.		Круговий В.В			Система моніторингу безпеки розумного будинку. Схема підписання даних.
Перевір.		Вой			
Реценз.		Крупельницький			
Н. Контр.		Вой			
Затверд.		Лужец			

Літ.	Маса	Масштаб

2 ВНТУ, ГР. БС-

Принцип роботи гешування

					08-20.МКР.008.00.000 ІЧЗ
Змн	Арк.	№ докум.	Підпис	Дат	
Розроб.		Круговий В.В			Система моніторингу безпеки розумного будинку. Принцип роботи гешування
Перевір.		Войт			
Реценз.		Крупельницький			
Н. Контр.		Войт			
Затверд.		Лужец			

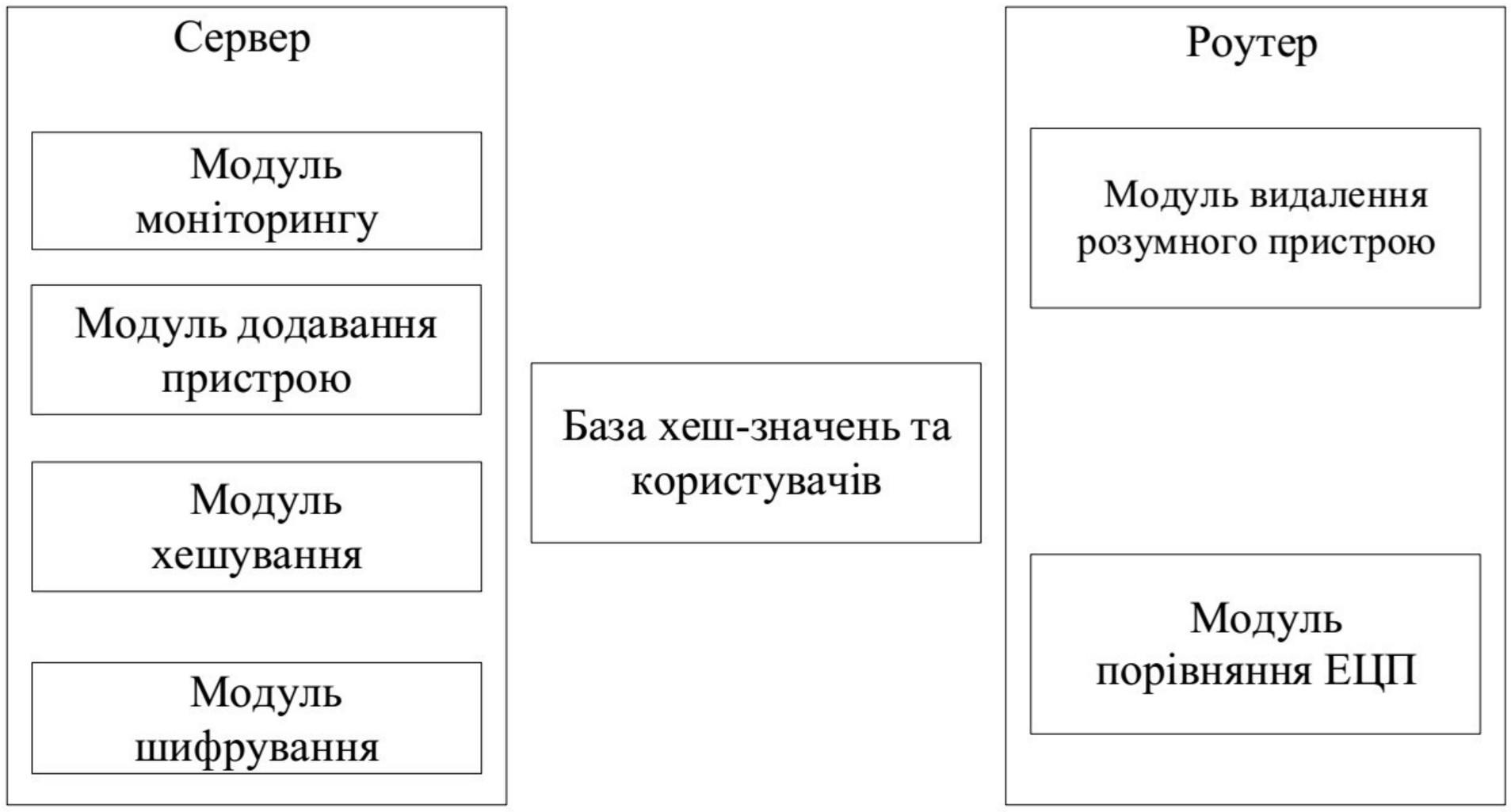
Літ.	Маса	Масштаб

3 ВНТУ, ГР. БС-

Складові системи моніторингу

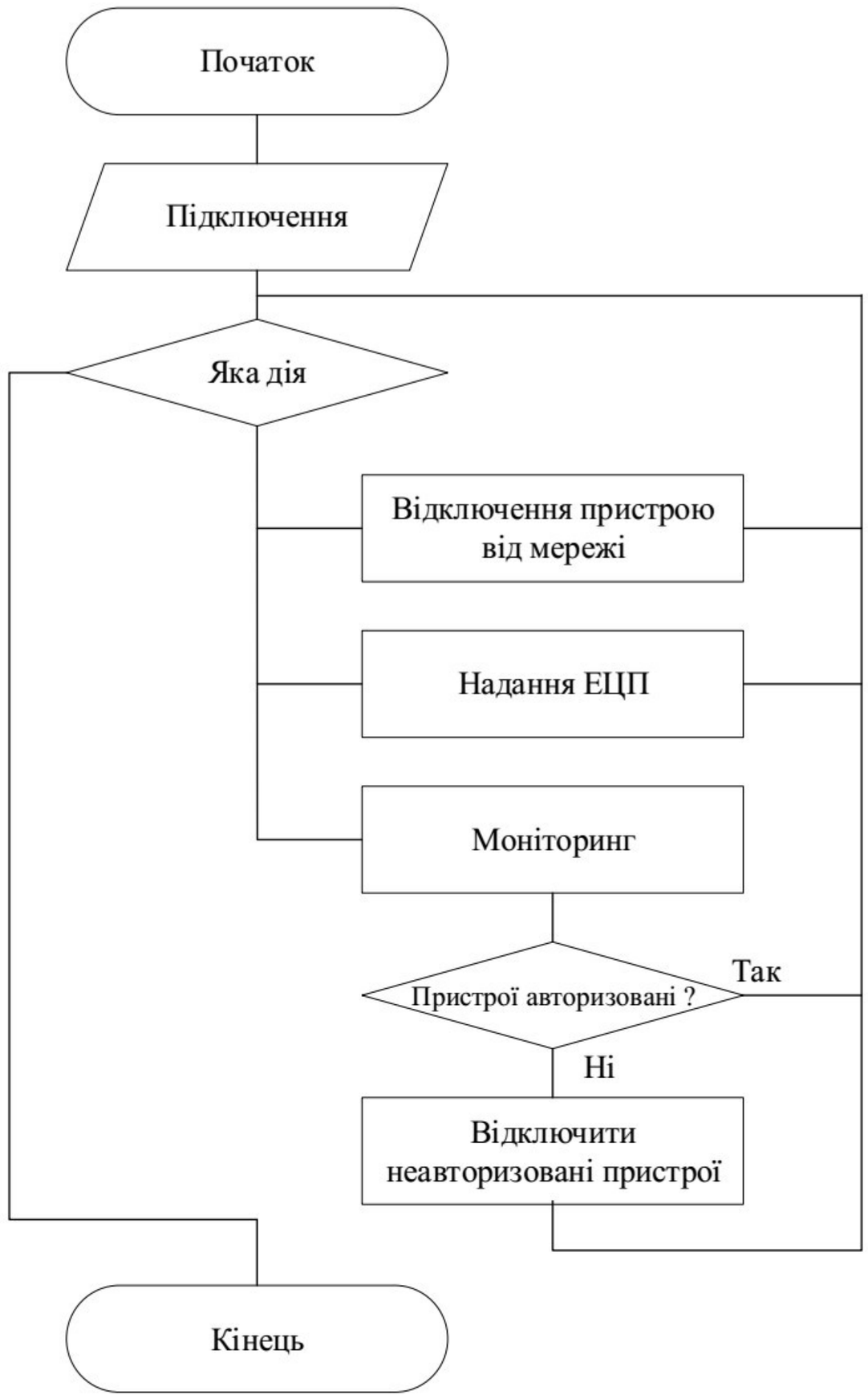
					08-20.МКР.008.00.000 ІЧ4		
Змн	Арк.	№ докум.	Підпис	Дат			
Розроб.		Круговий В.В			Система моніторингу безпеки розумного будинку. Складові системи моніторингу	Літ.	Маса / Масштаб
Перевір.		Вой					
Реценз.		Крупельницький				4 ВНТУ, ГР. БС-	
Н. Контр.		Вой					
Затверд.		Лужец					

Складові на стороні серверу та роутеру



					08-20.МКР.008.00.000 ІЧ5		
Змн	Арк.	№ докум.	Підпис	Дат			
Розроб.		Круговий В.В			Система моніторингу безпеки розумного будинку. Складові на стороні серверу та роутеру	Літ.	Маса / Масштаб
Перевір.		Войт					
Реценз.		Крупельницький				5 ВНТУ, ГР. БС-	
Н. Контр.		Войт					
Затверд.		Лужец					

Алгоритм роботи програми



					08-20.МКР.008.00.000 ІЧ6
Змн	Арк.	№ докум.	Підпис	Дат	
Розроб.		Круговий В.В			Система моніторингу безпеки розумного будинку. Алгоритм роботи програми.
Перевір.		Вой			
Реценз.		Крупельницький			
Н. Контр.		Вой			
Затверд.		Лужец			

Літ.	Маса	Масштаб

6 ВНТУ. ГР. БС-